MASON HAYES & CURRAN

DATA & TECHNOLOGY

Commercial Contracts What's Market 2026?

Key takeaways

Dublin London New York San Francisco

MHC.ie

MASON HAYES & CURRAN

Commercial Contracts What's Market 2026?

Key takeaways

Our Data & Technology team recently hosted its seventh annual "What's Market?" webinar on commercial contracts.

The session brought together Partners, Wendy Hederman and Mark Fry along with Senior Associate, Caoimhe Ruane to discuss current market practice in business-to-business contract negotiations. The webinar focused on the clauses that most often drive difficult discussions, including liability caps, indemnities and much more.

The session drew from our own contract tracker, which captures agreed positions across a wide range of client agreements, and our annual in-house counsel survey. Survey respondents came from a broad range of sectors, including financial services, technology, energy, healthcare and life sciences (including pharmaceuticals) and professional services, as well as other sectors.

The central message was clear: knowing what is standard in the market can make contract negotiations faster and more focused, but market practice is only one part of the discussion.

Each position still needs to be tested against:

- The risk profile of the deal
- The bargaining strength of the parties
- The relevant regulatory framework, and
- The practical consequences if something goes wrong

"Knowing the market helps streamline negotiations. But it is equally important to understand why certain positions are accepted, and to be able to explain that rationale to the counterparty."

CONTENTS

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

01

“What’s market?” is not a fixed rule

Market practice matters because commercial contracts are rarely negotiated in a vacuum.

When parties negotiate a contract, they will usually ask whether a proposed position is reasonable. In addition, they consider whether it reflects industry practice and whether it is likely to be accepted by the counterparty. This is particularly true for clauses dealing with liability, indemnities, data protection, cybersecurity, subcontracting or termination.

However, “what’s market” is not a substitute for risk assessment. A position that is market standard in a low-risk services agreement may be inappropriate in a high-value outsourcing or a regulated financial services arrangement, for instance.

A good contracting position should take account of:

- The value of the contract
- The nature of the goods or services
- The likelihood of loss arising and its potential scale
- The regulatory obligations of each party
- The financial standing of the counterparty
- Whether risk can be passed through the supply chain
- The governing law and jurisdiction, and
- Whether the contract is based on supplier standard terms or a bespoke negotiated agreement.

In-house legal teams should therefore use market practice as a benchmark, not a ceiling or a floor. There will be cases where it is appropriate to accept a market position. There will also be cases where the commercial or regulatory risk justifies moving away from it.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

02

Regulation is now central to negotiations

Regulatory compliance is no longer confined to a generic *"comply with applicable laws"* clause near the end of a contract.

Over recent years, regulation has moved to the centre of contract negotiations. This is particularly clear in areas such as GDPR, cybersecurity, digital regulation, outsourcing, financial services, accessibility, consumer protection, AI and data governance.

Our in-house counsel survey found that 76% of respondents consider that regulatory demands are making contract negotiations more challenging. This reflects a wider trend. Businesses are now expected not only to comply with regulation themselves, but also to manage regulatory risk across their supply chains.

This has practical consequences for contracts.

Customers, particularly in regulated sectors, increasingly need to flow down specific obligations to suppliers. These may include:

- Audit rights
- Security standards
- Reporting obligations
- Incident notification requirements
- Subcontracting controls
- Data governance obligations
- Business continuity measures, and
- Exit planning.

Suppliers, meanwhile, are being asked to accept obligations that may go beyond their standard service model. They may also need to ensure that any obligations they accept can be passed down to their own subcontractors and technology providers.

The result is more detailed negotiation around:

- Who bears the compliance burden
- Who pays for additional compliance measures
- How audit rights are exercised
- Whether regulatory obligations apply directly or indirectly
- How much oversight a customer can exercise over the supplier's operations, and
- What happens if the regulatory position changes during the term of a contract.

For businesses, a practical takeaway is that regulatory clauses should be reviewed early. They are no longer boilerplate.

> *Regulatory compliance is no longer just a miscellaneous clause. It is now a core part of risk allocation in commercial contracts.*

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

03

Liability caps remain a major pressure point

Liability caps remain one of the most negotiated parts of commercial contracts.

Suppliers usually see the cap as a way to manage exposure and will often want liability linked to the fees they receive. Customers tend to look at the issue differently. They may be relying on the supplier's expertise, technology, service continuity, security controls, or regulatory compliance. If the supplier defaults, the loss may be far greater than the fees paid.

This explains why caps often create tension. The same clause is being viewed from different risk perspectives.

Our latest survey showed a notable shift on the supplier side, with more suppliers including caps that protect only their own liability rather than mutual caps that also protect the customer. This is an important feature to watch out for when reviewing supplier standard terms.

A limitation of liability clause may look detailed, but still only limit the supplier's exposure. In more complex contracts involving outsourcing, technology or managed services agreements, customers may also have significant obligations and will seek to have their own liability capped.

> The key question is *"whose liability is capped, for which claims and subject to which exceptions?"*

KEY THEMES FROM THE WEBINAR

04

Fee-based caps are becoming more common

Our in-house counsel survey revealed a continued move away from fixed monetary caps towards caps linked to contract value or fees.

On the supplier side, fewer respondents now use fixed monetary caps. Most supplier caps are instead linked to the fees payable under the contract, with an annual fee cap the most common approach. The approach adopted here reflects the familiar supplier position that liability should be proportionate to revenue.

For customers, the position is more nuanced. Many are prepared to accept fee-based caps, but often only where the cap is based on a multiple of fees or where key risks are dealt with separately. A customer may accept a general cap of one to two times annual fees, provided there is a higher cap for data protection or cybersecurity and uncapped liability for certain indemnities.

The right structure will depend on the contract. A low-value but business-critical arrangement may justify a higher cap than the fees alone suggest. The cap should be assessed against the real exposure, not just the commercial value of the deal.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

05

A lower general cap may be acceptable where the contract properly identifies the risks that need higher protection.

Lower general caps are often balanced by super caps and carve-outs

One of the clearest trends is the use of super caps, carve-outs and uncapped liability alongside a lower general liability cap.

Customers may be more willing to accept a lower general cap where key risks are dealt with separately. Doing so can make negotiations more realistic by focusing on the areas where loss is most likely to be significant.

Data protection remains a key issue. Some suppliers will accept uncapped liability for GDPR breaches, but many now push back strongly because of the scale of potential fines and claims. As a result, higher or "super" caps are increasingly common, particularly where the contract involves significant processing of personal data. We are also seeing some suppliers successfully negotiate additional fees to offset the cost of necessary cyber insurance.

Confidentiality is also shifting away from blanket uncapped liability, partly because suppliers are concerned that confidentiality clauses may be used as a backdoor for data-related claims. By contrast, third-party IP remains one of the clearest areas where uncapped liability is commonly expected.

The general liability cap should therefore be read alongside the carve-outs, super caps, indemnities and exclusions.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

06

Indemnities need precision

Indemnities remain one of the trickiest areas of contract negotiation.

Customers often seek broad indemnities to protect against key risks. Suppliers usually prefer narrower indemnities linked to clearly defined events, such as:

- Third-party claims
- IP infringement
- Data protection breaches, or
- Negligence or specific employment-related liabilities such as TUPE

The survey showed broad alignment on some indemnities, particularly third-party IP claims. They are usually the most accepted form of indemnity because the customer is relying on the supplier's right to provide the relevant technology, software, content or other IP.

The bigger gap is on data protection indemnities. While many customers routinely seek to include them, less than half of suppliers who responded to the survey are willing to offer them. Customers may seek cover for any breach of data protection obligations or the data processing agreement. Suppliers may resist this and look to limit the indemnity to specific claims, recoverable regulatory fines or losses caused by their own material breach.

The scope of the indemnity matters. A broad indemnity is harder to agree on an uncapped basis. A narrower indemnity for a specific third-party claim may be easier to accept.

Parties should also make sure the indemnity clause and limitation of liability clause work together. It should be clear whether the indemnity is capped, subject to a super cap or carved out altogether.

The practical advice is simple: indemnities should not be treated as standard wording. They should be tailored to the actual risk and cross-checked against the liability cap.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

07

Exclusion clauses are receiving closer scrutiny

Suppliers continue to expect exclusions for indirect and consequential loss. They will often also seek to exclude loss of profit and similar financial losses.

Customers are often prepared to accept some exclusions, particularly for indirect or consequential loss. However, exclusion clauses are now being scrutinised more closely. The key issue is whether the clause excludes only losses that are genuinely indirect, or whether it also excludes losses that may be direct and foreseeable.

A supplier may seek to exclude loss of profits, loss of revenue, loss of data or business interruption losses in broad terms. A customer may accept the exclusion of indirect loss of profit but resist wording that excludes direct loss where that loss is a foreseeable result of the breach.

This is why parties are spending more time negotiating what is excluded versus what is recoverable. Customers may seek to include a list of losses that are recoverable, subject to the agreed cap, to reduce uncertainty later.

Explicitly naming these losses makes it more difficult for a supplier to later argue that such losses were not "*within the contemplation of the parties*" at the outset, ensuring they remain safely recoverable subject to the liability cap.

> *Exclusion clauses should not be treated as boilerplate. A few words can materially change the commercial value of the contract.*

KEY THEMES FROM THE WEBINAR

08

Subcontracting risk is being viewed through different lenses

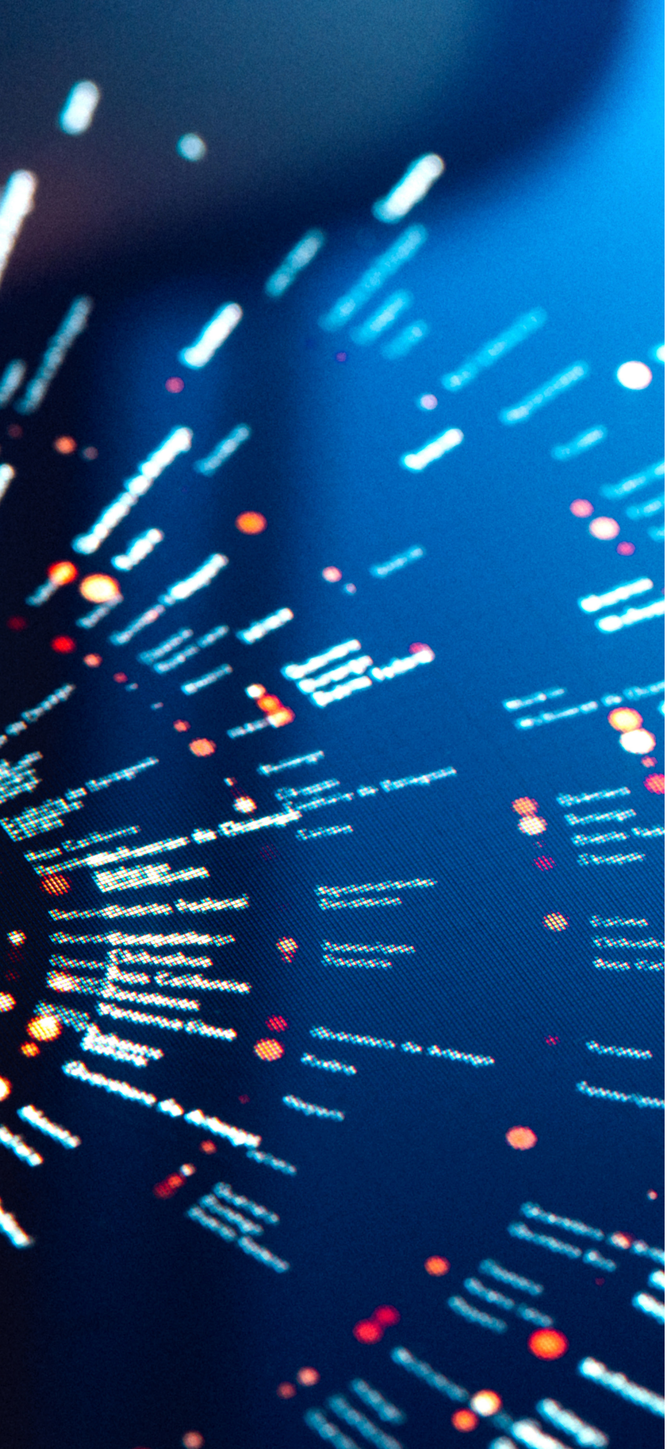
Subcontracting and supply chain risk are now major issues in commercial contracts, especially where services involve data or regulated activities.

Customers are focused on visibility. They want to know who is handling their data, who is delivering key parts of the service and whether the supplier has proper oversight of downstream providers. In regulated sectors, broad contractual rights may no longer be enough. Customers increasingly seek more specific controls, such as:

- Pre-approval rights for critical subcontractors
- Notice of changes in subcontracting arrangements
- Audit rights over subcontractors
- Regulator access rights
- Flow-down of key contractual obligations
- Supply chain mapping
- Information security commitments, and
- Exit and transition support.

Suppliers tend to be more focused on liability gaps. They may remain responsible to the customer for subcontractor failures, without being able to secure equivalent commitments from those subcontractors. This is especially difficult where they rely on large technology providers or cloud platforms with non-negotiable terms.

Subcontracting clauses should therefore go beyond consent. They should address which subcontractors matter, what information must be provided, what obligations must be flowed down and what happens if a key subcontractor changes or fails.



MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

09

AI is becoming part of ordinary contracting

AI clauses are moving from prohibition to governance. The focus is now disclosure, control, accountability and risk allocation.

Artificial intelligence (AI) is no longer a niche consideration in commercial contracts.

Our in-house counsel survey revealed a clear increase in organisations using AI and in-house legal teams advising on it. The bigger shift is that AI is moving from concern to expectation. Customers are increasingly comfortable with suppliers using AI to support service delivery, but they want transparency on how it is being used and what controls are being applied.

This matters especially where AI is used to process customer data or support regulated activities. The survey also highlighted a mismatch between customer expectations and supplier standard terms. Many customers now address supplier use of AI in their contracts, but fewer suppliers' terms do so. If AI is being used in service delivery, the contract should allow for it. Otherwise, customers may later argue that the use of AI was unauthorised.

For customers, the issue is not simply whether AI should be prohibited. The contract should specifically deal with issues like:

- Disclosure
- Customer data
- Ownership of outputs
- Accuracy and human oversight
- Liability for AI-generated outputs, and
- Compliance with internal policies.

AI contract wording will continue to develop as the EU AI Act is rolled out. AI is already being used in day-to-day operations, so contracts need to reflect that reality.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

10

The EU Data Act may have broader impact than many businesses realise

The EU Data Act is already in force and has important implications for business to business (B2B) contracts.

Much of the discussion has focused on connected products and cloud switching. Those areas matter, but our panellists highlighted another issue with potentially wider impact: unfair contractual terms imposed on another enterprise under Article 13 of the EU Data Act.

This regime can apply where contract terms relate to:

- Access to data
- Use of data, or
- Remedies for breach of data-related obligations.

It is not limited to contracts that mainly concern data processing. Clauses in wider commercial contracts may also be caught.

Businesses should therefore review standard terms and non-negotiated data clauses carefully. The EU Data Act includes controls similar to consumer protection rules, including terms that may be automatically unfair and unenforceable.

This could affect important provisions, including limitation of liability clauses. A standard severance clause may not preserve the position in the way the parties expect.

The Data Act should not be viewed as a narrow issue for connected devices or cloud services. It may require a broader review of B2B terms dealing with data access / use and data-related liability.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

11

Cybersecurity clauses are becoming active risk management tools

Cybersecurity regulation has changed the role of commercial contracts, turning them into active risk management instruments and regulatory compliance tools in themselves.

Contracts are increasingly being used to set security expectations and manage supply chain risk before cybersecurity incidents arise.

The Network and Information Systems Directive, or 'NIS2', is part of this shift. Many businesses are already assessing whether they are in scope and what contract updates may be needed.

For customers, this may mean adding more detailed cybersecurity obligations to supplier contracts, including minimum security standards, incident notification timelines, audit rights, flow-down requirements and clear processes for dealing with service disruption or vulnerabilities.

Suppliers may be affected directly if they are in scope, or indirectly where they provide services to customers that are. They may therefore be asked to accept more detailed obligations even where NIS2 does not apply to them directly.

Our survey also showed that many customers are including cybersecurity measures regardless of whether a specific regulation applies. This reflects a broader market expectation that suppliers should be able to give meaningful assurance on security controls.

A general requirement to maintain "appropriate security measures" may not be enough, but overly prescriptive obligations can be difficult to maintain over a long-term contract. The better approach is to match the security obligations to the services, the data involved and the supplier's operating model.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

12

DORA compliance is not just a regulatory exercise. It is a contract remediation, supplier management and operational resilience project.

DORA remains a live project for financial services contracts

The Digital Operational Resilience Act (DORA) remains a major contracting issue for financial services firms and ICT service providers.

While it applies primarily to financial entities, it also has a clear knock-on effect for suppliers providing ICT services to them. Contracts now need to deal more carefully with ICT risk, including service oversight, incident management, audit rights and the customer's ability to exit or transition the service if needed.

Although the DORA compliance deadline was 17 January 2025, many organisations are still working through contract updates. This is not surprising. Regulated entities may have hundreds of ICT suppliers, so reviewing and negotiating DORA contract amendments across that supplier base takes time.

Our panellists highlighted several practical challenges. Customers and suppliers are both experiencing pushback on DORA terms. Subcontracting also remains difficult, particularly where obligations need to be flowed down for critical ICT services. Classification can be contentious too, as suppliers may view their services as non-critical while customers may take a different view.

For financial services firms, DORA should be treated as an ongoing contract governance project. For suppliers, the key issue is whether their standard terms are equipped to deal with DORA-related requests.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

13

Dispute resolution clauses deserve more attention

Dispute resolution clauses are often left until the end of contract negotiations, but they can have real practical consequences.

The survey found that mediation followed by arbitration remains common for customers. By contrast, many suppliers prefer to go directly to the courts. This may reflect a concern that alternative dispute resolution (ADR) methods could delay debt recovery where a customer has failed to pay.

ADR can still be useful, however, particularly in longer-term commercial relationships, technology contracts, outsourcing arrangements and cross-border contracts. It can help preserve confidentiality, reduce costs and narrow the issues in dispute.

Where arbitration is used, ICC rules remain common, especially in cross-border contracts. However, arbitration clauses should be drafted carefully especially if you are not relying on the ICC template. For example the three-arbitrator panels may not be appropriate for every contract because of the additional cost.

Our speakers also considered *J. Burke and Associates Limited v O'Connell*, a recent Irish High Court decision on mediation. The Court indicated that parties could be directed to mediate where this was proportionate and where there was a reasonable prospect of resolving or at least narrowing the dispute.

The outcome of that case reinforces the need to think about the dispute resolution roadmap at the drafting stage, rather than treating it as an end-of-contract clause.

MASON HAYES & CURRAN

KEY THEMES FROM THE WEBINAR

14

Practical steps for in-house legal teams

01
Review liability positions in standard terms

Check whether your standard liability clause is still aligned with market practice and current business risk. Consider whether:

- Caps should be mutual
- Fee-based caps remain appropriate, and
- Key risks need separate treatment.

02
Map the relationship between caps, indemnities and exclusions

Uncertainty often arises because these clauses do not fit together. Make sure it is clear whether:

- Indemnities are capped
- Super caps apply, and
- Exclusions affect claims that should remain recoverable.

03
Refresh contracting playbooks

Playbooks should capture preferred positions and fallback positions. They should also reflect redlines and explain the rationale for each position so negotiators can respond more effectively to pushback.

04
Assess regulatory flow-down requirements

Regulated customers should identify which obligations need to be passed to suppliers. Suppliers should identify whether they can comply with those obligations and whether they can pass them down to subcontractors.

05
Update AI contract wording

Where AI is used in service delivery, contracts should address disclosure, customer data, outputs, human oversight, IP, liability and regulatory compliance.

06
Review data-related clauses for EU Data Act risk

Businesses using standard B2B terms should assess whether data access, data use, liability and remedy clauses could be affected by the Data Act unfair contract terms regime.

07
Strengthen cybersecurity provisions

Contracts should include practical and proportionate cybersecurity measures, including audit rights, security standards, incident notification obligations and subcontractor flow-down requirements where appropriate.

08
Treat DORA as ongoing contract governance

Financial services firms and ICT suppliers should expect DORA-related contract updates to continue as regulatory standards and guidance develop.

09
Do not overlook dispute resolution

The dispute resolution clause should reflect the commercial relationship, the likely types of dispute, the need for confidentiality and the practical importance of payment recovery or urgent relief.

MASON HAYES & CURRAN

Dublin London New York San Francisco

ABOUT US

As experts in complex, high-value commercial transactions, we advise blue-chip clients across a wide range of sectors on the contractual issues that go to the very core of their businesses. Our team advises on structuring, drafting and negotiation of all types of contracts.

Having one of the largest teams in Ireland in this area means we can offer a depth of resources and breadth of expertise that helps secure the best contractual outcomes for our clients. As trusted business advisers, we assist our clients in navigating the confusing array of regulations and obligations applying to their business.

We specialise in providing commercially focused advice to a wide range of public and private clients, applying our strategic knowledge and formulating innovative contractual structures. Our pragmatic drafting is based on a fundamental understanding of the underlying industry - we know what issues are important and how best to address them, resulting in more focused contracts, and more efficient negotiations.

MARKET RECOGNITION

"The firm is very strong in its information technology offering. There is a great level of knowledge of market standards, which enables pragmatic advice on which clauses are worth attempting to negotiate and which are unlikely to offer any prospect of success."

LEGAL 500, 2026

"The advice the firm provides is insightful and incredibly commercial."

CHAMBERS & PARTNERS, 2025

KEY CONTACTS

WENDY HEDERMAN
Partner, Data & Technology
whederman@mhc.ie
+353 86 046 4404

MARK FRY
Partner, Data & Technology
mfry@mhc.ie
+353 86 020 3549

CAOIMHE RUANE
Senior Associate, Data & Technology
cruane@mhc.ie
+353 86 102 0520

For more information and expert advice, visit:

MHC.ie/WhatsMarket2026

MHC.ie