


Welcome to The Forum

Navigating Cloud Software Contracts -
Essential Negotiation Points and
Common Challenges



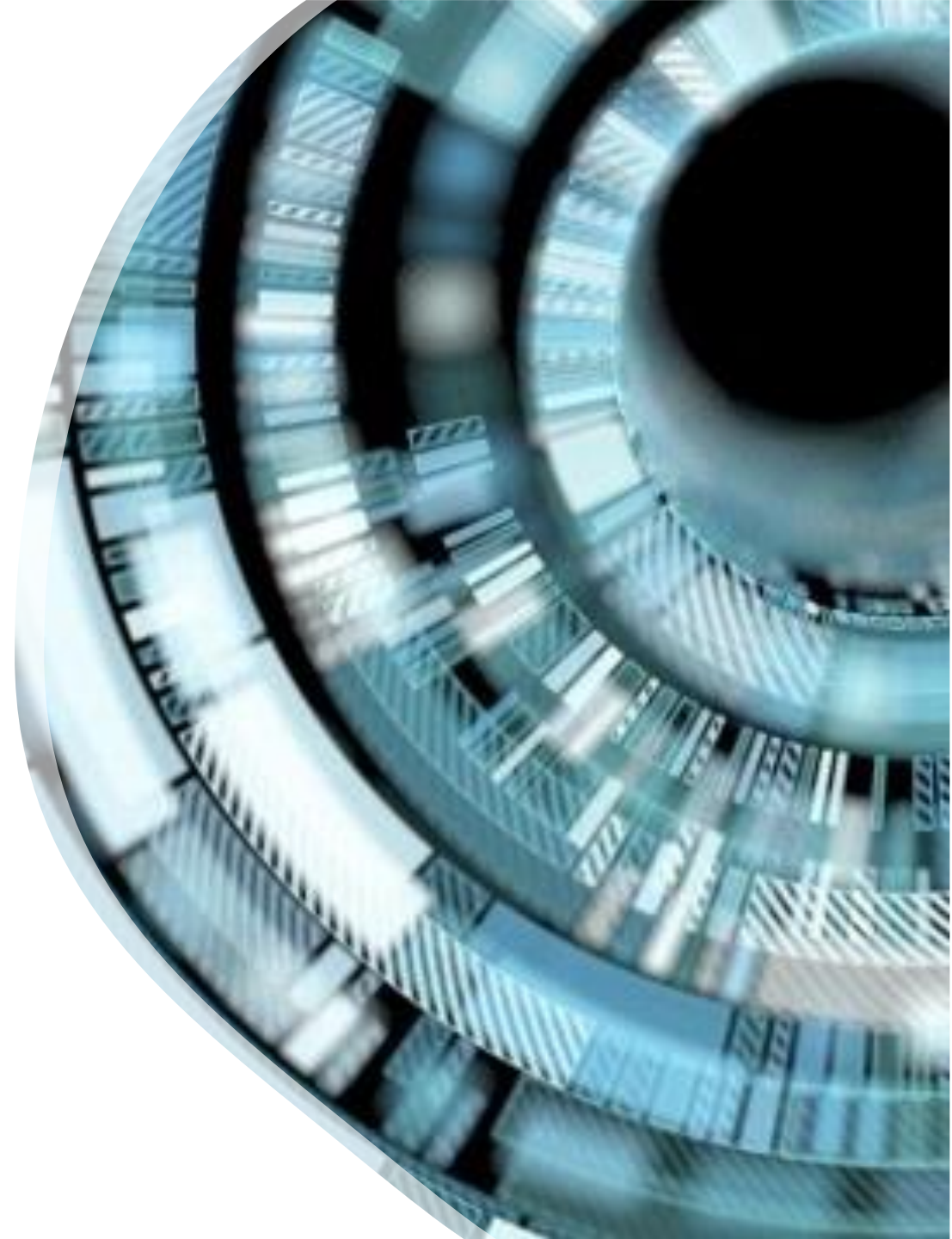
What are we going to talk about today?

We'll examine these topics from provider and customer perspectives, highlighting frequent pitfalls and essential data protection concerns.

What are cloud agreements?

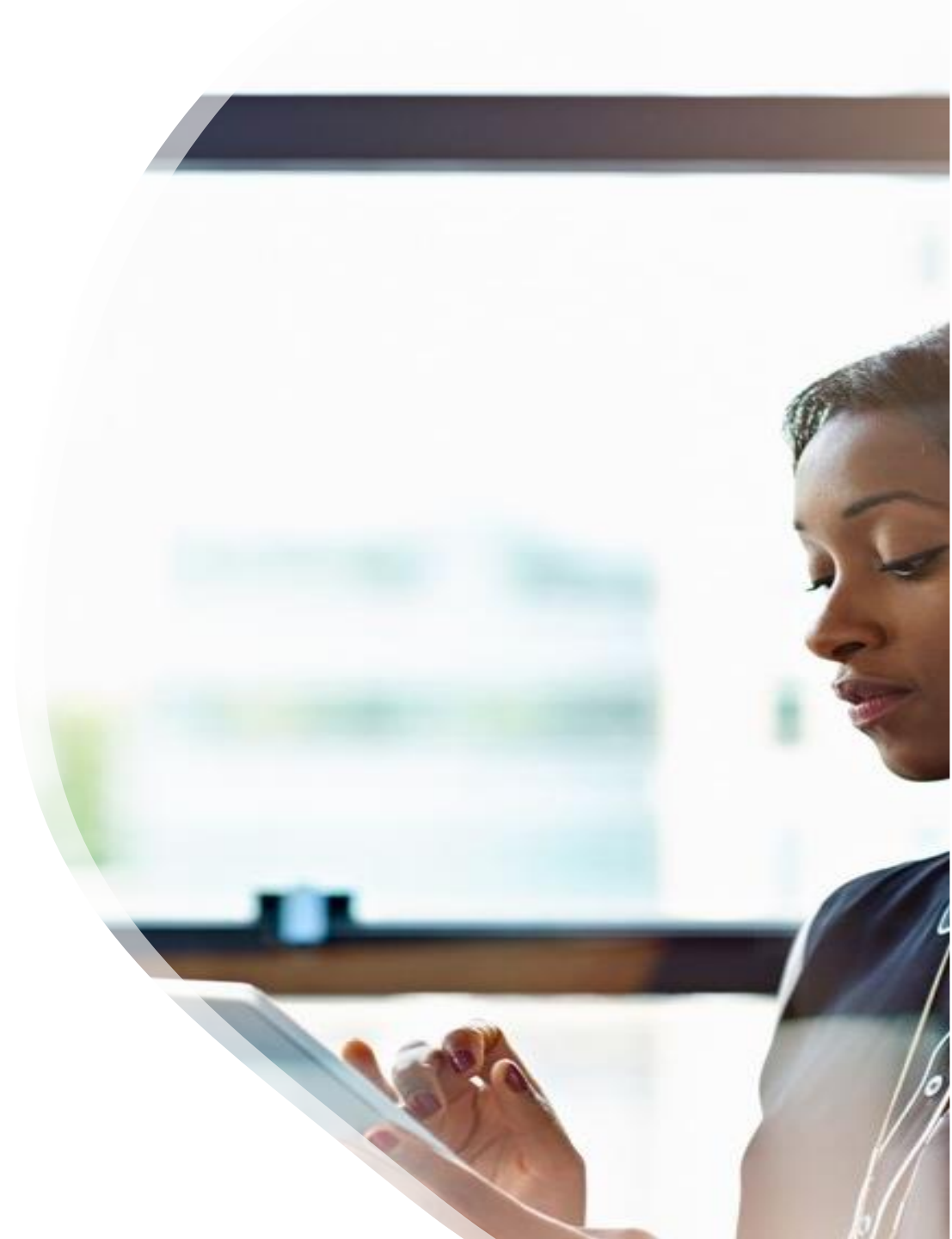
The term “cloud services” covers a multitude of different types of IT service, including:

- Single applications delivered as Software as a Service (SaaS)
- Hosted operating systems delivered as Platform as a Service (PaaS)
- Entire data centres being transitioned to the cloud using Infrastructure as a Service (IaaS).



What are the benefits of cloud services for customers?

1. Cost
2. More flexible and enables hybrid working
3. Scalable resource
4. Enhanced security and increased organisational resilience
5. Quick to deploy
6. Improved support and maintenance



What are the cloud customer's risks?

1. Losing control and lack of visibility
2. Cyber security / risk of data loss
3. Reliance on online connectivity
4. Poor service
5. Regulatory compliance
6. Integration complexity
7. Risk of technical or vendor lock-in
8. Unforeseen / unexpected costs
9. Untailored solutions



How can a customer mitigate these risks?

1. Select your provider carefully
2. Select your product carefully
3. Enter into a good contract



Focus on: SaaS Agreements

- What is SaaS?
- Are SaaS contracts negotiable?



Key considerations when drafting or reviewing SaaS contracts?

Key areas to consider:

- Parties
- Service description
- Term
- Use of the software
- Price
- Payment terms



Key considerations continued...

- Warranties / Supplier obligations
- Indemnities
- Limitation of liability clause
- Support and SLAs
- Termination and consequences of termination
- Audits



Other common clauses

- Dispute resolution
- TUPE
- Insurance
- Relationship management
- Confidentiality
- Sub-contractors
- Governing law and jurisdiction



Regulatory requirements and Due Diligence

- Data protection
- Business continuity / resilience and data security
- Sector specific requirements
- NIS Regulations
- EU regulations



Data protection

- What personal data will be processed and therefore what is the risk?
- Does the provider consider itself a DC or a DP or a mix of both?
- Sub-processors
- International transfers
- In what form does the provider use the personal data?
 - Anonymised
 - pseudonymised (or de-identified)
 - aggregated?
 - encrypted
- AI

Business continuity / resilience and data security

- Technical and organization security / cyber security
- Accreditation and certification standards
- ISO 27001 relating to information security
- ISO27018 relating to the protection of personally identifiable information
- PCI DSS an information security standard for card payments
- ISO 22301 relating to business continuity.
- SOC 2
- Disaster recovery
- Back-ups of data
- Restoration of data
- Portability of data to a new provider on contract expiry / termination



TRETHOWANS

Law. As it should be.

Q&A and Poll Results

Thank you

Website: www.trethowans.com/the-forum

Password: the-forum

Meet the Panel



Louise Thompson
Partner

louise.thompson@trethowans.com

07881 343 955



Julian Hamblin
Partner

julian.hamblin@trethowans.com

07779 799 048



Laura Trapnell
Partner

laura.trapnell@trethowans.com

07464 909 592