THE FORUM

Welcome to The Forum

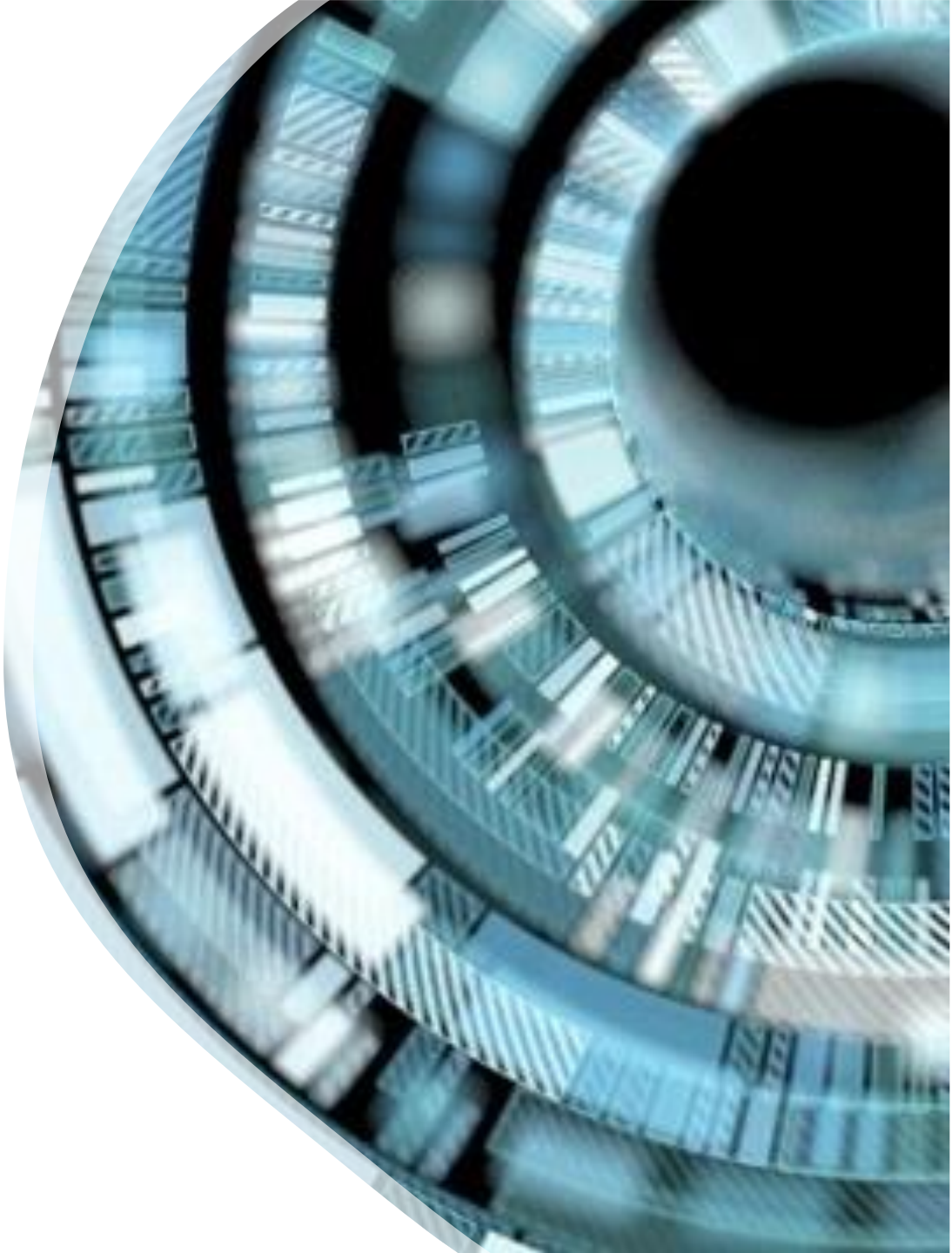
Exploring data protection in the context of cloud agreements, particularly SaaS

TRETHOWANS

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).



How can a cloud customer mitigate data protection risks?

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

Data protection law

- What is personal data?

"*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

- What is special category personal data?
    - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership.
    - Genetic data.
    - Biometric data (where used for identification purposes).
    - Data concerning health, a person's sex life or a person's sexual orientation.

Data protection law

- Criminal offence personal data
- Financial information
- Children's data

- What is “processing” of personal data?

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

Data protection law principles

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not then further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary given the purposes for which the personal data is processed
- Accurate and kept up to date
- Kept for no longer than is necessary for the purpose for which it was collected
- Kept secure using appropriate technical and organisational security measures
- Accountability

Controllers and processors

The UK GDPR defines a controller as:

> *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".*

The UK GDPR defines a processor as:

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

Considerations for SaaS

1. Does the contract involve the processing of personal data by the service provider?
2. What are the roles of the customer and the service provider?
    - Controller and Processor?
    - Controller and Processor (and sometimes also a Controller)?
    - Controller and Controller?
    - Processor and Processor?
3. Is the service provider a company registered in England and Wales or the EU?
4. Is the personal data being processed high risk?
5. Is the personal data processing high risk?

Due diligence

1. What are the controller's obligations?

Article 28(1) of the UK GDPR:

"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".

2. What should the controller's due diligence involve?

3. Recent EDPB guidance

- Identifying the whole sub-processor chain
- Verification and documentation of sufficient guarantees
- Verification of sub-processor contracts
- Onward transfers

Data processing agreements

Article 28 (UK GDPR) Requirements

a. Controller's processing instructions
b. Processing in accordance with documented instructions
c. Personnel confidentiality
d. Appropriate technical and organisational measures
e. Assistance with requests by data subjects to exercise their rights
f. Assistance with notifying personal data breaches, data protection impact assessments and consultation with supervisory authorities
g. Delete or return all personal data
h. Demonstrate compliance and audits
i. Use of sub-processors

Important considerations

- Sub-processors
- International transfers
- Indemnities
- Limitations of liability
- Is it still personal data?
    - Anonymised
    - Pseudonymised (or de-identified)
    - Aggregated
    - Encrypted
- AI


TRETHOWANS
Law. As it should be.
Q&A


THE FORUM
Thank you
Website: www.trethowans.com/the-forum
Password: the-forum
TRETHOWANS

Meet the Panel

Louise Thompson
Partner

louise.thompson@trethowans.com
02380 820 509

Sarah Wheadon
Partner

sarah.wheadon@trethowans.com
02380 820 485