DPPC 2024

EMPOWERING YOU THROUGH INFORMATION

ico.
Information Commissioner's Office

#DPPC24

ico.org.uk/DPPC

Sky high: how to comply with UK GDPR when using cloud systems

ico.
Information Commissioner's Office

Agenda

1. Why use the cloud?

   Common use cases and data protection benefits

2. Cloud use and compliance

   5 key issues to consider

3. Q & A

Your presenters

Kitty Rosser Principal Lawyer (Data Privacy Advice)

Sonya Clarke Principal Lawyer (Contracts and Compliance)

Dalbir Singh Principal Policy Advisor, Anonymisation and Encryption (Technology and Innovation)

Iman El Mehdawy Group Manager (Information Management and Compliance Service)

Why use the cloud: common use cases

Types of cloud service

- Infrastructure as a Service (IaaS) - provision of computing resources
- Platform as a Service (PaaS) - used to develop apps on top
- Software as a Service (SaaS) - ready-made apps such as MS Teams, Slack, Workday, Salesforce, Shopify, etc

Operational drivers

- Lowers barriers to entry
- Scalable
- Cyber expertise/capacity
- New commercial opportunities (AI as a Service)
- Supports disaster recovery and business continuity

Why use the cloud: data protection benefits

Safeguards

- Specialised knowledge of cloud configuration
- Issuing security patches quickly
- Proactive monitoring
- Providing focused alerts
- Supporting the availability of data
- Access control

Accountability

- Records & logging
- Data mapping services
- Support in providing requisite info for DPIAs
- Support for response to data subject rights requests

Storage limitation

- Automating retention schedules

Cloud use and compliance

ico.org.uk/DPPC

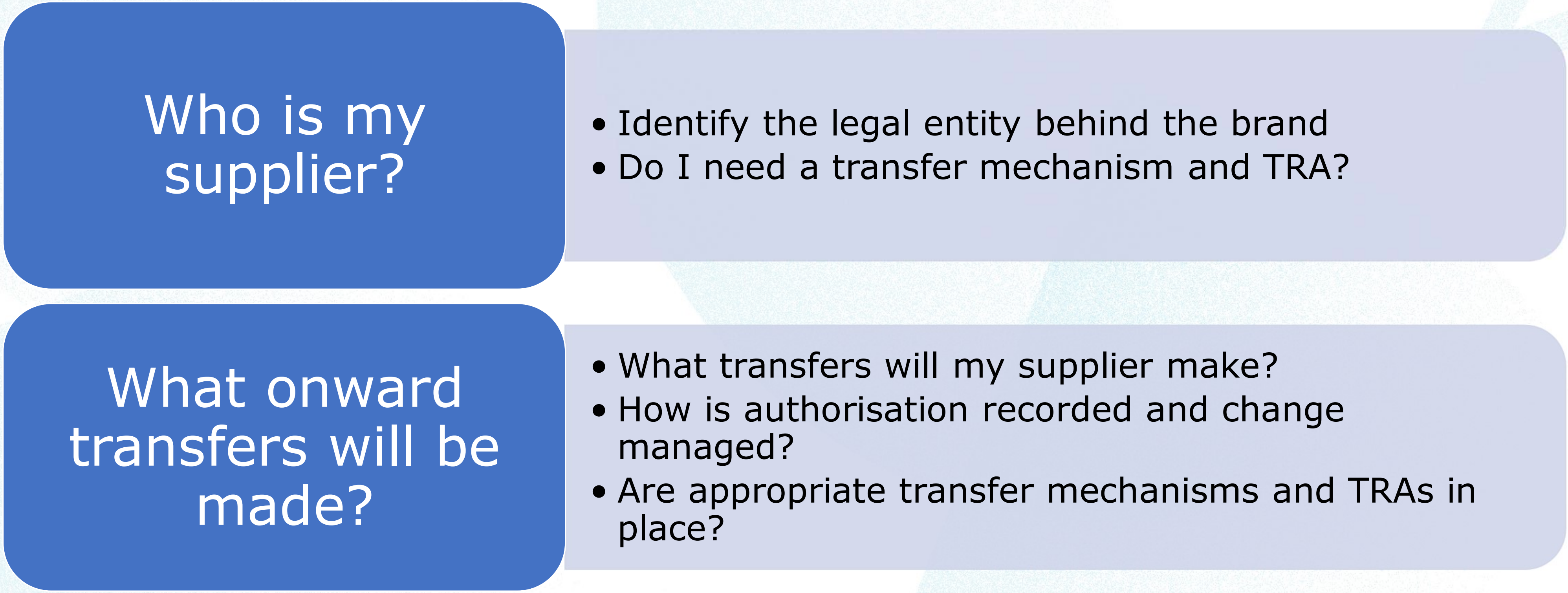
#DPPC24

Poll 1

We don’t need to think about international data transfers when using a cloud system if we are contracting with a UK supplier

- □ True
- □ False

Cloud use and compliance: mapping the cloud



Who is my supplier?

- Identify the legal entity behind the brand
- Do I need a transfer mechanism and TRA?

What onward transfers will be made?

- What transfers will my supplier make?
- How is authorisation recorded and change managed?
- Are appropriate transfer mechanisms and TRAs in place?

Poll 2

We should always consider whether we need to complete a DPIA before introducing a new cloud system

❑ True

❑ False

Cloud use and compliance: the DPIA

- A DPIA is a risk assessment
- Before introducing a new cloud system, you **must** always carry out a DPIA screening assessment to see if you need to complete a full DPIA
- The ICO provides a DPIA template you can use but you can also adapt this template or use your own
- On our website (www.ico.org.uk) you will find:
  - DPIA guidance
  - DPIA screening checklist
  - DPIA template

Cloud use and compliance: the DPIA

Your DPIA should describe…

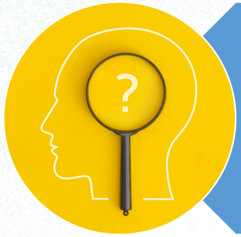
The nature, scope, context and purposes of the processing

An inventory of the personal data

Data life cycle (its journey from collection to disposal), relationships between controllers, processors, data subjects and systems

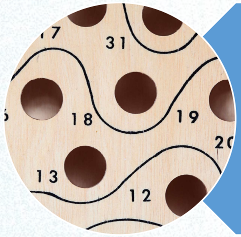
Cloud use and compliance: the DPIA

Your DPIA should also describe…



Who you’ve consulted with as part of your assessment

How you comply with the data protection principles and individual rights



What risks exist, how they are scored, what action you will take to mitigate those risks, and who is responsible for carrying out those actions.

Cloud use and compliance: the DPIA

Remember:

- A DPIA is a live document
- Consult with your supplier early
- You **must** consult with the ICO **before** you begin processing if your DPIA identifies any **unmitigated** high risks

Cloud use and compliance: due diligence

Importance of due diligence

- Standard supplier terms - limited scope to negotiate warranties and indemnities
- Identify and address key risks **before** agreeing contract and service commencement
- Use of topic-based DD questionnaires

Key risk areas

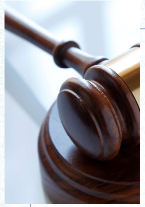
- Data protection and privacy and customer compliance
- Data security
- System security
- International transfers
- Sub-processors – storage and follow the sun support
- Business and service continuity
- Switching suppliers (vendor lock in)

Poll 3

Do you review the Ts & Cs when you take on a new supplier?

- ❑ Always – this is an essential part of the process
- ❑ Sometimes– it depends how important/expensive the service is
- ❑ Never – we can’t change them/understand them
- ❑ N/A – we always contract on our own Ts & Cs

Cloud use and compliance: supplier contracts



UK GDPR compliance

Article 28 terms

(**see ICO guidance**)

Service levels & KPIs/service credits/remedies

Security obligations & standards

Business continuity

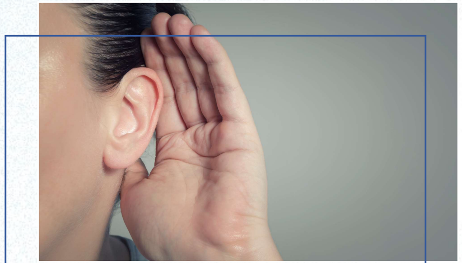
Caps on liability

(DP “supercap”)

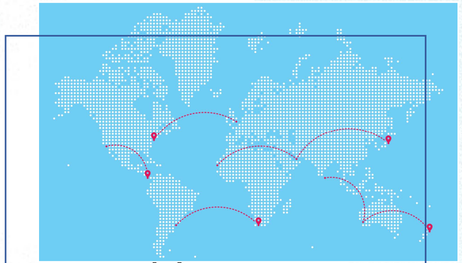
International transfers inc. SCCs/IDTAs

Exit management

Cloud use and compliance: transparency/accountability



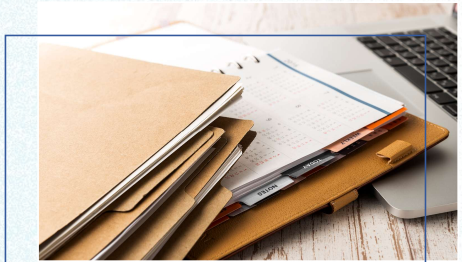
Privacy notices



ROPA/data maps

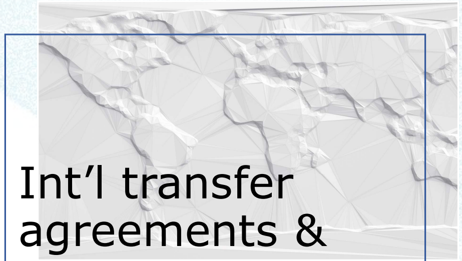
Retention

DPIA



Policies

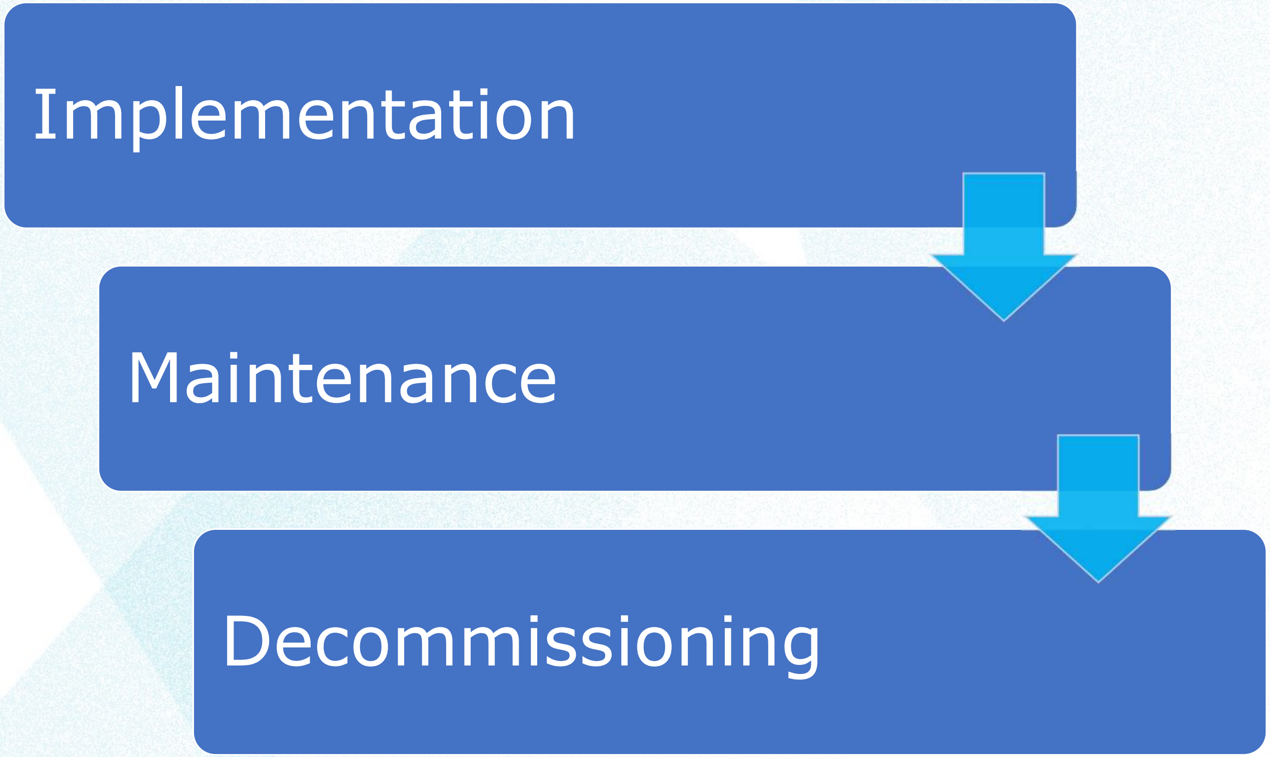
Contracts & DD



Int’l transfer agreements & TRAs

Lawful basis

Cloud use and compliance: beyond implementation


Implementation

Maintenance

Decommissioning

Questions?

ico.org.uk/DPPC

#DPPC24

Keep in touch

Subscribe to our e-newsletter at ico.org.uk or find us on...

#DPPC24

ico.org.uk/DPPC

DPPC 20 24

ico.

Information Commissioner's Office