



Image source: Microsoft 365 content library

# Data protection in practice



1



Image source: Microsoft 365 content library

## LEARNING OUTCOMES

- **Explain** the difference between processing, data sharing, joint controllership.
- **Identify** what clauses need to be included for any contract to be compliant with UK GDPR.
- **Understand** when sharing information would constitute an international transfer.
- **Apply** a pragmatic approach to compliance.



2



gdpr obligations

Image source: Microsoft 365 content library

# Contracts and clauses



3

## Processing

- Collection
- Recording
- Organisation
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure
- Alignment or combination
- Restriction
- Erasure or destruction
- Anonymisation and pseudonymisation



Image source: Microsoft 365 content library



4

## Processing



***“any operation performed on personal data or sets of personal data”***

You assume liability for supplier’s actions

Documented standard to assess and appoint a supplier

Clauses to cover Art. 28 requirements

- Act on your behalf i.e. only on your instruction
- Supplier’s staff must be bound by confidentiality
- Supplier must take all measures required to process data securely
- Supplier cannot engage another processor without your written authorisation
- Supplier must assist you in complying with your obligations relating to data subject rights and data protection impact assessments (DPIAs)
- Delete or return your data
- Permit you to audit them

## Data Sharing



***“the disclosure of personal data by transmission, dissemination or otherwise making it available”***

Clauses to comply with Data Sharing Code issued by ICO under s121 of DPA18

- purpose and legal reason for sharing
- what data items are being shared
- what happens to the data at each stage of the process
- where responsibilities of each party start and finish
- and what standards and governance need to be in place.

Data Sharing Inventory

Each party assumes liability for own actions

Each party are independently responsible for compliance

## Joint Controllership

***“two or more parties jointly determine the purposes and means of processing”***

Clauses to cover Art. 26 requirements

- Respective responsibilities

- Lead controller nominated to act as point of contact for data subjects

- Record keeping including maintenance of disclosure logs/sharing inventories

Must make essence of agreement available if a data subject requests it

Jointly liable – can agree how to split liability but ICO may overrule this



7

## Clauses and Ts&Cs

**Vague security clauses** e.g. “We take appropriate measures”

**Overly broad sub-processor rights** e.g. automatic approval or no visibility of who they use.

**Conflicting clauses** especially in “standard T&Cs” where marketing or analytics use conflicts with “only process on instructions.”

**Silence on deletion** i.e. no process or deadlines for data return/deletion.

**Liability caps that undermine GDPR** e.g. very low liability limits for breaches.

**Hidden independent controller language** i.e. terms that give them rights to use data for their own purposes.

**No mention of assistance** leaving you alone to handle requests.

**Jurisdiction risks** i.e. no controls on data transfers outside the UK, or reliance on invalid transfer mechanisms.

**Terminology** e.g. Personally Identifiable Information (PII), service provider, third party.



8

# International transfers

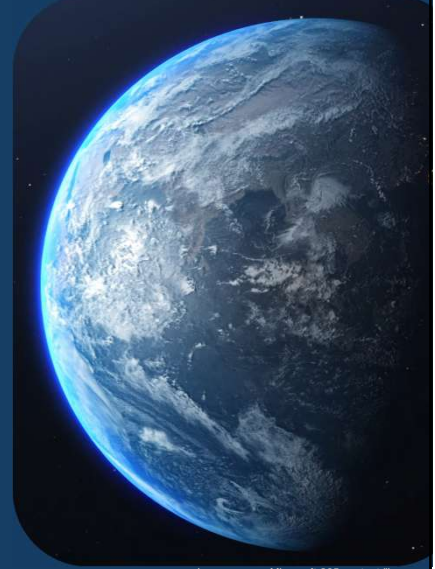


Image source: Microsoft 365 content library



9

## WHAT ARE THE RULES?

### 1. Adequacy

Is the country covered by adequacy regulations? If so, the transfer can take place.

### 2. Appropriate safeguards

If 1 doesn't apply, can the transfer be covered by appropriate safeguards? If so, the transfer can take place, provided a **Transfer Risk Assessment** is conducted by the exporting organisation.

### 3. Exceptions

If 1 and 2 don't apply, is the transfer covered by an exception? If so, the transfer can take place.

### 4. None of the above

If none of the above apply, then the transfer will not comply with data protection legislative requirements.



10

## PRACTICAL STEPS FOR DUE DILIGENCE



**Conduct risk assessments**



**Safeguard through contracts**



**Regular reviews**



**Embed good record keeping practices**

Image source: Microsoft 365 content library




# Example






Supplier	Use	Data	P/C
<b>QuickBooks by Intuit</b>	Bookkeeping and invoicing software	Invoice numbers Client names and contact details Service offering provided including dates and locations	Processor
<b>Microsoft</b>	Provides corporate services for day-to-day operations (Exchange Online for email, Onedrive for file storage, Office suite for document creation and storage, Teams for collaboration).	Names, contact details, activity logs, content of emails, signatures, video calls, transcriptions, video recordings etc	Processor
<b>Adobe</b>	Creative marketing and document management	location information of devices, IP addresses, history of web searches, browsing activity logs, social media profile information, ad campaign success rates etc.	Processor
<b>McAfee Ireland</b>	Antivirus	Internet Protocol (IP) address, user settings, MAC address, cookie identifiers, mobile carrier, mobile advertising and other unique identifiers, browser or device information, location information (including approximate location derived from IP address), and Internet service provider.	Controller
<b>ChatGPT</b>	Drafting and reporting support	Account creation detail (name, email address), prompt history, any attachments uploaded.	Processor



13

Section	What to Check	Tick if Present	Notes / Gaps
<b>Parties &amp; Roles</b>	Is the relationship defined?	<input type="checkbox"/>	
<b>Purpose &amp; Instructions</b>	Data processed only on documented instructions, for specified purposes.	<input type="checkbox"/>	
<b>Confidentiality</b>	Staff and sub-processors bound by confidentiality.	<input type="checkbox"/>	
<b>Security</b>	Specific or standards-based security commitments (e.g. ISO 27001, NCSC guidance).	<input type="checkbox"/>	
<b>Sub-processing</b>	Written authorisation required before sub-processor use; and process defined.	<input type="checkbox"/>	
<b>Data Subject Rights</b>	Supplier must assist with access, erasure, restriction, portability rights and other rights.	<input type="checkbox"/>	
<b>Assistance Duties</b>	Support with DPIAs, breach reporting, regulator engagement and any other duties.	<input type="checkbox"/>	
<b>End-of-Contract</b>	Clear return or deletion process; deadlines set, with workable practices.	<input type="checkbox"/>	
<b>Audit &amp; Info</b>	Your right to request compliance information or conduct audits.	<input type="checkbox"/>	
<b>International Transfers</b>	Lawful transfer mechanisms in place; specific clauses for non-UK destinations.	<input type="checkbox"/>	



14

Quickbooks		Microsoft	
<b>Only act on your documented instructions</b>	No – QuickBooks only recognises themselves as a Processor for QuickBooks Payroll Services and/or QB Time	<b>Only act on your documented instructions</b>	P9 of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Duty of confidentiality</b>	Clause 13.6 <a href="#">Terms of Service for QuickBooks Online - UK</a>	<b>Duty of confidentiality</b>	P10 of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Security measures</b>	Use MFA, encryption and threat scanning - <a href="#">Intuit Security Center</a>   <a href="#">Security Practices</a>	<b>Security measures</b>	P13 of Addendum (September 2025 version) <a href="#">Licensing Documents</a> and Appendix A
<b>Sub-processor approval</b>		<b>Sub-processor approval</b>	P19 of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Assist with rights requests</b>		<b>Assist with rights requests</b>	P36 (3e) of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Assist with compliance</b>		<b>Assist with compliance</b>	P36 (3f) of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Delete or return data</b>		<b>Delete or return data</b>	P18 of Addendum (September 2025 version) <a href="#">Licensing Documents</a>
<b>Make compliance info available</b>		<b>Make compliance info available</b>	P15 of Addendum (September 2025 version) <a href="#">Licensing Documents</a>

15

Supplier	Use	Data	P/C	ICO registered	Compliance	Risk
<b>QuickBooks by Intuit</b>	Bookkeeping and invoicing software	Invoice numbers, Client names and contact details, Service offering provided including dates and locations	Processor	ZA191666	QuickBooks recognise themselves as a Controller. This means they have not provided required information on sub-processor approval, assisting with rights requests, assisting with compliance or allowing provisions for auditing, or deleting /destroying data.	Medium/High
<b>Microsoft</b>	Provides corporate services for day-to-day operations (Exchange Online for email, Onedrive for file storage, Office suite for document creation and storage, Teams for collaboration).	Names, contact details, activity logs, content of emails, signatures, video calls, transcriptions, video recordings etc	Processor	Z6296785	Full – keep reviewing terms as versions change frequently (last reviewed 10/10/25)	Low
<b>Adobe</b>	Creative marketing and document management	location information of devices, IP addresses, history of web searches, browsing activity logs, social media profile information, ad campaign success rates etc.	Processor	(789022X	All requirements of Article 28 addressed: <a href="http://www.adobe.com/go/tou-dpa">www.adobe.com/go/tou-dpa</a>	Low
<b>McAfee Ireland</b>	Antivirus	Internet Protocol (IP) address, user settings, MAC address, cookie identifiers, mobile carrier, mobile advertising and other unique identifiers, browser or device information, location information (including approximate location derived from IP address), and Internet service provider.	Controller	ZA274735	Controller	Low
<b>ChatGPT</b>	Drafting and reporting support	Account creation detail (name, email address), prompt history, any attachments uploaded.	Processor	ZB625491	All requirements of Article 28 addressed in Data processing addendum (paid subscriptions only)	Low

16



# Data protection risks



17

## Risk Management

Be aware and **identify** risks

Plan and **evaluate** risks

Follow best practice to **address** risks

18

# Risk appetite vs. risk tolerance

If risk appetite represents the official speed limit of 70, risk tolerance is how much faster you can go before likely getting a ticket.



19

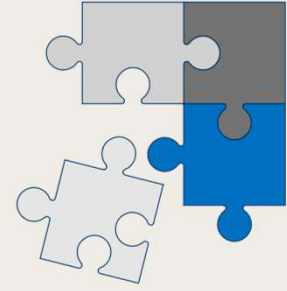
## Risk appetite levels

Rating	OPEN	FLEXIBLE	CAUTIOUS	MINIMALIST	AVERSE
<b>Philosophy</b>	Will take justified risks	Will take strongly justified risks	Preference for safe delivery	Extremely conservative	"Sacred" Avoidance of risk is a core objective
<b>Tolerance for uncertainty</b>	Fully anticipated	Expect some	Limited	Low	Extremely low
<b>Choice</b> when faced with multiple options	Will choose option with highest return; accept possibility of failure	Will choose to put at risk, but will manage impact	Will accept if limited, and heavily out-weighted by benefits	Will accept only if essential, and limited possibility/extent of failure	Will select the lowest risk option, always
<b>Trade-off</b> against achievement of other objectives	Willing	Willing under the right conditions	Prefer to avoid	With extreme reluctance	Never

Adapted from Rob Quail's article *Defining Your Taste for Risk* in Corporate Risk Canada (Spring 2012)

20

## CONCLUSION: PRAGMATIC COMPLIANCE



### **Understanding requirements**

Grasping the different requirements for different relationships is key to fulfilling your responsibilities effectively.

### **Robust contracts**

Robust contracts help establish clear data protection responsibilities and compliance.

### **Sustainable business practices**

Nothing about processing data, legally, is required to be risk-free, but you need to know where your risks are and what you've decided to do about them.



21

# What questions do you have?

Get in touch to take one of the 20 funded 1-to-1 slots!

[Malwina@privacyprotectgroup.com](mailto:Malwina@privacyprotectgroup.com)

07775 738 720



22