Due diligence checklist: UK GDPR and DPA 2018

UK General Data Protection Regulation and Data Protection Act 2018. ICO, the United Kingdom.

Regime	UK GDPR and DPA 2018
Regulator	ICO
Country	the United Kingdom
Regulator's page	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/gb-ukgdpr

What it is

Personal data goes only to processors under Article 28 terms, with international transfers safeguarded.

Who it applies to

Applies to every financial institution in the United Kingdom.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Article 28 processor terms, including sub-processor approval	The vendor's standard contract terms on these points, marked against the regime, and its position on the institution's own schedule.	
2	Where data is hosted and processed, and the transfer mechanism for anything outside the UK	The hosting regions and a data flow description naming every country data is stored in or processed from, and the transfer mechanism for anything leaving the country.	
3	Breach notification to the institution without undue delay, so it can meet the 72-hour deadline	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.