How does Cyber Crucible support UK GDPR requirements?

Short answer: Cyber Crucible supports your UK GDPR obligations. UK GDPR and the Data Protection Act 2018 track EU GDPR closely, so the same mapping applies — minimal collection, processor role under a written DPA, strong technical safeguards, and deployment options that keep data in the UK or entirely on your premises.

What applies

Following the UK's departure from the EU, UK GDPR operates alongside the Data Protection Act 2018, supervised by the Information Commissioner's Office (ICO). The principles, lawful bases, and processor obligations closely mirror EU GDPR.

Where organizations should pay attention

- **International transfers** use the UK's own mechanisms — the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs, rather than EU SCCs alone.
- **Dual compliance** — organizations operating in both the UK and EU must satisfy both regimes, though the practical controls overlap almost entirely.

What specifically applies here

The assessment is the same as for EU GDPR, and the answers are the same:

- Keys, credentials, tokens, and file contents are never collected.
- Analysis occurs on the endpoint; protection does not require data to move.
- UK regional deployment, or air-gapped deployment that removes transfer entirely.
- Processor role under a written DPA with sub-processors bound to equivalent terms.

> For the appropriate transfer instrument for your circumstances, contact **dpo@cybercrucible.com**. Status at time of writing — confirm current ICO guidance with counsel.

Revision #3
Created 2026-07-21 19:00:17 UTC by Dennis Underwood
Updated 2026-11-24 04:23:21 UTC by Dennis Underwood