



5 CRITICAL DATA QUESTIONS EVERY IT PROFESSIONAL MUST ANSWER

EXPERT GDPR GUIDANCE FOR UK IT SERVICE PROVIDERS

BEANSECURE | HELLO@BEANSECURE.NET

Contents

Welcome	3
About BeanSecure & AXIS AI.....	4
MISSION	4
VISION	4
AXIS AI	4
Are our client data backups GDPR compliant?	5
72-Hour Breach Response: What Must We Do?.....	6
Cloud Services: Who's Responsible for What?	7
How Long Can We Keep Client Data?	8
Ransomware Attack: Our Legal Obligations	9
Ready for Instant GDPR Guidance?.....	10



WELCOME

As an IT professional, you're trusted with your clients' most sensitive data. But are you prepared for the complex web of UK GDPR compliance that comes with that responsibility?

A single compliance misstep can cost your business thousands in fines and irreparable damage to client relationships. Yet most IT companies lack dedicated legal teams to navigate these challenges.

This guide addresses the 5 most critical data protection questions we hear from IT professionals like you. Each answer is powered by AXIS AI - our specialized compliance assistant trained on UK data law.

Your expertise + our compliance guidance = unshakeable client confidence.

ABOUT BEANSECURE & AXIS AI

MISSION

BeanSecure simplifies UK GDPR compliance for businesses without overwhelming legal jargon or scare tactics.

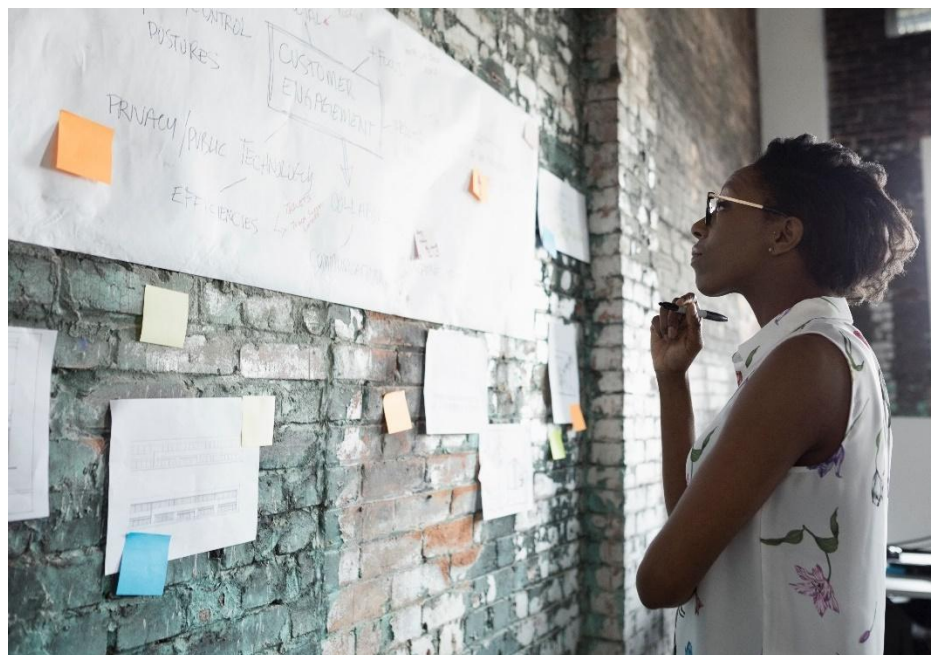
VISION

Every business should feel confident handling personal data, knowing they're protected and compliant.

AXIS AI

AXIS AI is our intelligent compliance assistant, trained specifically on UK data protection law. It provides instant, accurate guidance tailored to your industry and situation.

Trusted by 200+ UK businesses & individuals for GDPR compliance





Your clients define retention periods - you must follow their instructions and ensure secure cloud storage.

ARE OUR CLIENT DATA BACKUPS GDPR COMPLIANT?

Ensuring GDPR compliance for client data backups involves several key considerations.

Since you act as a data processor, your clients, as the data controllers, should define the retention period based on their business needs and legal obligations.

You must adhere to their instructions.

For backups in cloud services, you must ensure the provider offers adequate security measures like encryption and data location within the UK or EEA unless appropriate safeguards are in place for international transfers.

Do your contracts with clients clearly define these responsibilities and data retention policies?

This is crucial for demonstrating compliance.



Contain,
document,
evaluate, notify
client immediately
- they handle ICO
reporting.

72-HOUR BREACH RESPONSE: WHAT MUST WE DO?

The 72-hour clock starts ticking the moment you become aware of a potential breach.

First, contain the breach to prevent further data loss.

Then, document everything:

- the nature of the breach
- affected data
- potential impact
- and the measures taken

Evaluate if the breach is likely to result in a risk to individuals' rights and freedoms. If so, you **MUST** notify the ICO without undue delay.

Critically, inform your client (the data controller) immediately, providing them with all necessary information so they can decide if notification to affected individuals is required under GDPR Article 33.

Do you have a documented incident response plan that covers these steps?

It's essential for swift and compliant action.



You need DPAs with cloud providers and clear client contracts defining all responsibilities.

CLOUD SERVICES: WHO'S RESPONSIBLE FOR WHAT?

With cloud services like AWS or Azure, you remain responsible for processing client data lawfully, even if it's stored on their infrastructure.

You need a Data Processing Agreement (DPA) with the cloud provider (they are a sub-processor), setting out their data protection obligations.

This is legally mandatory.

Your contract with your client should also clearly define your responsibilities, data locations (UK, EEA, or elsewhere), and how you ensure compliance.

Do you have these DPAs in place with all your cloud providers, and are your client contracts clear on data processing roles and responsibilities?



Client determines retention period - only keep what's needed for legitimate business purposes.

HOW LONG CAN WE KEEP CLIENT DATA?

Data retention should be determined by your client (the data controller), aligned with their legal obligations and business needs.

Your contracts should specify the retention period and the process for data deletion or return after project completion.

You should only retain data for legitimate business purposes, such as providing ongoing support, which must be clearly defined in your contract.

Any data not required for these purposes should be securely deleted.

Do you have a documented data retention policy and clear contractual clauses addressing this?

This can prevent future legal issues.



Notify client immediately - they handle ICO reporting while you focus on containment and recovery.

RANSOMWARE ATTACK: OUR LEGAL OBLIGATIONS

If your client suffers a ransomware attack, you must notify them *immediately* upon discovery.

As the data processor, you don't report directly to the ICO.

However, you must provide all necessary information to your client (the data controller) so they can determine if the incident meets the reporting threshold for the ICO.

Your client is responsible for notifying the ICO and potentially affected individuals.

Your focus should be on containment, recovery, and providing all necessary support to your client within the legal framework of your contract and the GDPR.

Do your client contracts outline the responsibilities and communication protocols in such scenarios?

This is essential for a coordinated response.



READY FOR INSTANT GDPR GUIDANCE?

These 5 questions are just the beginning.

AXIS AI can answer virtually any UK data protection question your business faces - instantly and accurately.

What AXIS AI Can Do for Your IT Business:

- Instant answers to complex GDPR questions
- Client-ready compliance explanations
- Contract guidance and templates
- Breach response procedures
- Industry-specific advice

Transform from IT support to trusted advisor with AXIS AI at your fingertips.

**Request
Your Free
Tailored
AXIS AI
Demo**