FAB CAMPAIGNS ONE-PAGER · DATA RISK · VERSION 1.0

10 Questions Every Board Should Ask About Data Risk

Qualifying the data governance maturity of the board you sit on, or advise.

PREPARED BY	Fabrizio De Liberali, Fab Campaigns Ltd	**DATE**	May 2026
DOCUMENT REF.	FC-2026-DAT-01	**VERSION**	1.0 — Live
CLASSIFICATION	C1 · Public	**PAIRS WITH**	Cyber + AI Governance

Most boards are being asked: *"Are we GDPR compliant?"* The more urgent question is the one underneath it: **what data are we actually holding, who has access to it, and what happens when it leaks, not if?** These ten questions cut through compliance documentation to the accountability you cannot afford to lose.

01 • INVENTORY & OWNERSHIP

1 What is our complete inventory of personal and sensitive data, including data held by third-party processors, and who is accountable for keeping it current?

WHY IT MATTERS *You cannot protect data you cannot see. Most data breaches originate in systems or processors management had forgotten they owned.*

2 For each data category we hold, can we name the lawful basis under which we collected it, and is that basis still valid for the way we use it today?

WHY IT MATTERS *Lawful basis is not a one-time decision. Business model changes, new use cases, and acquired datasets all create silent compliance failures.*

02 • ACCESS & EXPOSURE

3 Who has access to our most sensitive data, internally and externally, and when did we last audit whether that access is still appropriate?

WHY IT MATTERS *Insider risk and stale permissions are the two most common causes of preventable data exposure. Access should follow need, not history.*

4 Which third-party suppliers and cloud services hold or process our data, and what contractual and technical controls do we have over what they do with it?

WHY IT MATTERS *Data risk does not stop at your boundary. Your processor's breach is your regulatory liability. Supply chain due diligence is a board responsibility.*

03 • BREACH READINESS

5 **Have we tested our data breach response, including the 72-hour GDPR notification clock, under realistic conditions, or do we only have a procedure document?**

WHY IT MATTERS *A procedure that has never been run is a false assurance. The 72-hour window starts from awareness, and regulators have little patience for boards that were surprised.*

6 **When a breach occurs, are we clear on what we are required to report, to whom, by when, and who in the boardroom owns that notification decision?**

WHY IT MATTERS *Regulatory exposure multiplies when notification is late, incomplete, or inconsistent. Clarity of ownership before the incident is the only kind that works.*

04 • RETENTION & DELETION

7 **Do we have a tested data deletion and retention process, including backups and archived systems, or are we retaining data indefinitely by default?**

WHY IT MATTERS *Retention is a liability that compounds. Data you no longer need is data you still have to protect, disclose in litigation, and account for to regulators.*

8 **When an individual exercises their right to erasure, portability, or access, can we fulfil that request completely, accurately, and within the statutory timescale?**

WHY IT MATTERS *Rights that exist in policy but not in practice are the definition of regulatory and reputational exposure. The test is operational, not documentary.*

05 • GOVERNANCE & ASSURANCE

9 **What independent assurance do we have on our data protection posture, and is management being tested on the questions we would want them to ask?**

WHY IT MATTERS *Self-assessed compliance is where governance theatre lives. The board that relies only on management reporting has no visibility of what management does not want to see.*

10 **Is our investment in data governance proportionate to the value and sensitivity of the data we hold, and can we defend that proportionality to a regulator or in court?**

WHY IT MATTERS *Data is now a material asset and a material liability. Boards that treat data governance as an IT overhead rather than a fiduciary responsibility will be judged accordingly.*

> **THE DATA STEWARDSHIP PRINCIPLE**
>
> *Data you hold is a trust relationship, not an asset class. The board that treats personal data as something to extract value from, rather than something held on behalf of people, has already failed its governance test. Stewardship starts before the regulator arrives.*

A LIVE DOCUMENT

This is Version 1. I am testing and refining these questions with boards across the UK and Italy through 2026. If you use them, or disagree with any of them, I want to hear from you. **Reputations are built by being cited, not by being followed.**

Fabrizio De Liberali

Partnership Architect, Fab Campaigns Ltd

Pairs with: 10 Questions on Cyber Governance + AI Governance