From incident to insight: proving accountability under UK GDPR

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Why the organisations facing the greatest GDPR exposure are not the ones who get it wrong, but the ones who cannot explain their decisions.

GDPR enforcement has matured

Regulators, courts, and complainants are no longer focused primarily on whether an organisation made a mistake. Instead, scrutiny increasingly falls on a more difficult question:

'Can the organisation demonstrate that its decisions were reasonable, proportionate and well-governed at the time they were made?'

This shift is visible across breaches, subject access requests, and now, the UK's evolving complaints regime. In each area, accountability is no longer theoretical. It must be **demonstrated**.

When things go wrong: breaches and the burden of judgement

Data breaches are, by their nature, unpredictable. Even well-resourced organisations with strong controls experience incidents. Regulatory scrutiny is rarely triggered by the incident itself, but by how cleanly an organisation recovers. It is how risk was **assessed, explained and recorded** in the hours and days that followed.

Risk assessments under Articles 33 and 34 are not compliance tick boxes. They are the organisation's clear record of why a particular course of action was taken at the time, whether that is notifying the ICO, communicating with individuals, or deciding that neither step is required.

Enforcement activity consistently shows that problems arise when:

- Decisions are taken informally and not documented
- Assumptions about low risk are asserted rather than assessed
- The rationale only emerges retrospectively, once scrutiny begins

The legal test is not whether hindsight proves the decision wrong, but whether a reasonable organisation could have reached that decision on the information available at the time. Without evidence, judgement becomes indefensible.

When people push back: subject access requests and the need to explain restraint

The same theme runs through subject access requests. Courts have made clear that controllers are not required to perform limitless searches or provide every document in which a name appears. But they are required to conduct reasonable and proportionate searches and to be able to justify where lines were drawn.

Recent case law reinforces that failures rarely arise because organisations searched too little data. They arise because organisations cannot show:

- How search scope was defined
- Why certain systems were included or excluded
- What effort was involved
- Why further steps would have been disproportionate

An SAR response is not just a delivery of data, it is a narrative of judgement – an explanation of how access rights were

balanced against practicality, third-party rights and organisational reality. Without that narrative, even well-intentioned responses become vulnerable to challenge.

When trust erodes: complaints as the new accountability frontier

The Data (Use and Access) Act 2025 formalises a trend that has been building for several years: organisations are expected to resolve GDPR concerns internally before they reach the regulator.

The new complaints framework elevates everyday governance failures into regulatory risk. Poor explanations, delayed responses, or inconsistent handling across teams are no longer merely operational issues. They are signals of weak accountability.

Many data protection complaints originate downstream of earlier decisions:

- Breach communications that fail to explain risk clearly
- SAR responses that feel obstructive or opaque
- Inconsistent application of stated policies

In this context, complaints handling becomes the final proof point of whether an organisation truly understands (and can defend) how it uses personal data.

The common thread: accountability as evidence, not intention

Across breaches, SARs and complaints, a single theme emerges: GDPR accountability is no longer about having the right answers, it is about being able to evidence how those answers were reached.

Policies, training, and legal awareness matter, but they only protect an organisation if they are translated into decisions that are:

- Structured
- Recorded
- Consistent
- Capable of explanation under scrutiny

This is where many organisations struggle, not because they lack commitment to compliance, but because decision-making is left to individuals operating without sufficient support, structure, or documentation.

Where this leaves organisations now

The next phase of GDPR maturity is not about more regulation. It is about operationalising judgement.

That means embedding decision-making frameworks that help teams:

- Assess risk coherently during incidents
- Articulate proportionality during SARs
- Resolve complaints transparently and consistently

Organisations that succeed will not be those that avoid every mistake, but those that can demonstrate that their governance works even under pressure. This is where informed legal interpretation meets operational reality, and where specialist support can make a material difference.

At Net-Defence, we see this every day: organisations that understand the law but need help translating it into defensible action when it matters most.

Accountability is no longer something organisations assert. It is something they must prove.

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com