FROM PAPER TO PROOF

What German data protection and information security officers are telling MSPs in 2026

July 2026

Around 100 conversations with German data protection and information security officers

A qualitative study ahead of the Dutch NIS2 transposition (Cyberbeveiligingswet, 15 August 2026)

Commissioned by

GUARDIAN 360°

Kruisplein 484, 3012 CC Rotterdam, The Netherlands

Introduction

Since 6 December 2025, Germany's NIS2 transposition act has been in force without a transition period. For MSPs, this means clients no longer ask only “are we secure?”, but “can we prove it?”

To understand how German data protection officers (DPOs) and information security officers (ISOs) answer that question in practice, Guardian360 conducted around 100 open, qualitative professional conversations about a specific approach: linking technical security findings to GDPR, NIS2 and ISO 27001 obligations.

This is explicitly not a representative benchmark study, but a qualitative collection of professional opinions. The percentages mentioned here relate to the responses received and should be read as a tendency, not as a statistically robust figure.

This report summarises what we learned, and what that means for your client conversations.

Key finding 1: the gap between documentation and proof

Conversations with DPOs and ISOs made one thing clear: the biggest weakness rarely lies in the technology itself, but in the fact that documented controls are barely re-tested once they are in place. Roughly one in twenty conversation partners (around 5%) independently described the same pattern: a measure is implemented once, documented, and never questioned again within the annual audit cycle, until accountability “disappears into the sand”.

Quote from a conversation

“Laws are risk based, scanners are binary.” As one IT security auditor put it.

This observation aligns with external data: a Proliance study among 122 decision makers in the German Mittelstand shows that companies tend to rate their own security maturity as high, while at the same time facing a high number of serious security incidents and considerable uncertainty about NIS2 (source: Proliance, “Lage der Informationssicherheit im deutschen Mittelstand 2025”).

What this means for you as an MSP

Your clients often believe they are well prepared because a measure was documented once; proof of ongoing effectiveness is a conversation that few clients initiate themselves, but most of them need.

Key finding 2: NIS2 maps more readily to technical evidence than the GDPR

One of the most revealing insights concerns a distinction our original approach had not anticipated so clearly: around 6% of conversation partners, mostly experienced lawyers and auditors, pointed out independently and unprompted that technical findings map far more directly onto NIS2 requirements than onto GDPR articles. One conversation partner put it pointedly: “NIS2 mapping can add value; GDPR mapping, in my view, cannot.”

The reason: NIS2 requirements are largely technical and organisational in nature, and therefore relatively straightforward to support with technical evidence. The GDPR, by contrast, is deliberately technology neutral and risk based. Article 32 GDPR requires a risk assessment based on the processing context, the category of personal data, and the risks to data subjects, something a vulnerability scanner cannot judge in principle. One conversation partner also pointed to Article 6 GDPR: whether a processing activity has a lawful basis at all is something a scanner never sees, regardless of how good the technical mapping is.

An even broader concern, raised by roughly one in ten conversation partners (around 10%), was the general warning that a technical mapping should always be understood as an indicator and prioritisation aid, never as an automated compliance proof. A finding is not a violation.

What this means for you as an MSP

When offering clients technical security evidence, position it realistically: as a strong, direct contribution to NIS2 accountability, and as a valuable but complementary building block for the GDPR, one that does not replace legal assessment by a DPO. This distinction protects you and your clients from a false sense of security and makes your offering more credible.

Key finding 3: ownership beats enforcement, but only with a name and a deadline

Around 5% of conversation partners independently confirmed: measures that fit an organisation's actual reality are adopted voluntarily. Measures that ignore that reality almost always fall by the wayside.

Quote from a conversation

"risk-appropriate", as one conversation partner described it: aligned with the concrete day-to-day business and staged according to risk

At the same time, clear accountability is essential. An auditor with a data protection background explained why assigning a finding to a department alone ("IT is responsible") does not hold up in practice: when a regulator asks, or in a dispute, "IT" is not a defensible answer. What is needed is a named individual with a timestamp, and a mechanism that automatically escalates if the issue is not resolved.

Another conversation partner added an often overlooked angle: even when the SOC or IT correctly resolves a finding, this frequently stays "quiet" within IT and never reaches senior management, even though management carries the ultimate liability.

Interestingly, not every organisation struggles with this. One conversation partner, whose organisation handles changes consistently through a change and ticketing system, reported that every change automatically triggers a review of the entire downstream process chain. The annual audit problem simply never arises for them structurally, a clear individual example that the problem is solvable when ownership and triggers are properly linked.

What this means for you as an MSP

When implementing security solutions at clients, pay attention to two things: that measures fit the actual reality of the business (otherwise they are ignored); and that every control has a named, time-stamped owner, not a department, with a visible path to senior management.

Why this matters particularly for MSPs

Conversations repeatedly surfaced a pattern that directly affects the role of MSPs: at smaller organisations, a single person often carries responsibility for data protection, information security and NIS2 simultaneously. This person rarely has the time or specialisation to master all three areas in equal depth.

That explains why external support is in such demand, particularly among SMEs. According to market research, companies cite the need for specialised expertise (62 percent) and lack of internal capacity (39 percent) as the main reasons for falling behind on NIS2 implementation (source: Proliance study 2025). That is precisely the gap MSPs can close, provided they can not only claim, but actually show, that controls work.

A look at the Netherlands: what can be learned?

While Germany has been subject to its NIS2 transposition act since December 2025, the Netherlands will only transpose the NIS2 directive into national law on 15 August 2026 (the Cyberbeveiligingswet). Dutch organisations and MSPs face the same challenge, but with a time advantage to learn from the German experience.

The central lesson from the German conversations: the transition works best where accountability is established early and by name, rather than assigning departments wholesale just before the deadline. It also shows that organisations that had already set up security measures in a “risk-appropriate” rather than purely formal way before the legal obligation kicked in experienced a noticeably smoother transition. Dutch MSPs have until August 2026 to address exactly these two points, named accountability and risk-appropriate rather than generic measures, with their clients now, rather than reacting under time pressure.

Practical talking points for the client conversation

Based on the responses from the DPOs and ISOs we spoke with, we recommend MSPs use the following conversation approaches:

1. Ask about the last proof, not just the last piece of documentation. “When was it last checked whether this measure still works?” is often a question many clients cannot answer, and it shows exactly where the real need lies.
2. Deliberately separate NIS2 and GDPR communication. Offer technical evidence confidently for NIS2, but make clear for the GDPR that the final legal assessment remains with the DPO. This builds trust rather than scepticism.
3. Always name a person, never a department. When agreeing action plans with clients, make sure every item has a named owner with a deadline, and that compliance-relevant findings also reach senior management, not just the SOC or IT.
4. Show what happens between audits. Clients on an annual audit cycle are vulnerable to exactly the gap most frequently mentioned in our conversations. Offering continuous rather than only annual review is a clear point of differentiation.

How Guardian360 Lighthouse supports this

Guardian360 Lighthouse runs technical scans daily rather than once a year, and links every finding directly to a clearly named, time-stamped recommendation. This directly addresses the gaps described in this report: it makes proof of effectiveness continuously available rather than a one-off snapshot, supports an honest separation between technical indicator and legal assessment, and creates the basis for compliance-relevant findings to reach the right people in a traceable way. Findings are mapped to ISO 27001, GDPR, NIS2, DORA and OWASP, among other standards, making the technical effectiveness of implemented measures demonstrable rather than merely ticked off. Guardian360 Lighthouse is designed as a technical complement to a client's management system, not a replacement for it.

About this study

The insights summarised in this report come from a qualitative series of conversations that Guardian360 held with German data protection officers, information security officers and auditors, as part of validating an approach that links technical security findings to GDPR, NIS2 and ISO 27001 obligations. The percentages mentioned relate to the responses received and should be read as a qualitative tendency, not as representative statistics. External sources are marked accordingly.

Guardian360 is a Dutch company with ISO 27001 certification. Through the Guardian360 Lighthouse platform, we support MSPs and IT service providers across Europe in offering their clients continuous security monitoring.

Metric	Value
Substantive professional conversations received	approx. 100
Period	June to July 2026
Target group	Data protection and information security officers in Germany
Method	Open, qualitative professional conversations (not a representative sample)