VAN PAPIER NAAR BEWIJS

Wat Duitse privacy- en informatiebeveiligingsfunctionarissen MSP's in 2026 vertellen

Juli 2026

Circa 100 gesprekken met Duitse privacy- en informatiebeveiligingsfunctionarissen

Een kwalitatieve studie in aanloop naar de Nederlandse NIS2-implementatie (Cyberbeveiligingswet, 15 augustus 2026)

Opdrachtgever

GUARDIAN 360°

Kruisplein 484, 3012 CC Rotterdam – Nederland

Inleiding

Sinds 6 december 2025 is de Duitse NIS2-Umsetzungsgesetz zonder overgangstermijn van kracht. Voor MSP's betekent dat: klanten vragen tegenwoordig niet meer alleen „zijn we veilig?“, maar „kunnen we dat aantonen?“

Om te begrijpen hoe Duitse privacyfunctionarissen (DSB) en informatiebeveiligingsfunctionarissen (ISB) die vraag in de praktijk beantwoorden, heeft Guardian360 circa 100 open, kwalitatieve vakgesprekken gevoerd over een concrete aanpak: het koppelen van technische beveiligingsbevindingen aan AVG-, NIS2- en ISO 27001-verplichtingen.

Dit is uitdrukkelijk geen representatieve benchmarkstudie, maar een kwalitatieve verzameling van vakinhoudelijke meningen. De hier genoemde percentages hebben betrekking op de ontvangen reacties en moeten gelezen worden als tendens, niet als statistisch onderbouwd cijfer.

Dit rapport vat samen wat we hebben geleerd, en wat dat betekent voor uw klantgesprek.

Kernbevinding 1: het gat tussen documentatie en bewijs

Uit de gesprekken met DSB's en ISB's is duidelijk geworden: de grootste zwakke plek zit zelden in de techniek zelf, maar in het feit dat gedocumenteerde controles na invoering nauwelijks nog opnieuw worden getoetst. Ongeveer een op de twintig gesprekspartners (ca. 5%) beschreef onafhankelijk hetzelfde patroon: een maatregel wordt eenmalig ingevoerd, gedocumenteerd, en in het jaarlijkse auditritme niet meer bevraagd, tot verantwoordelijkheid „in het zand verloopt“.

> **Citaat uit een gesprek**
> *„Wetten zijn risicogebaseerd, scanners zijn binair.“ Aldus een IT-beveiligingsauditor.*

Deze observatie sluit aan bij extern onderzoek: een studie van Proliance onder 122 beslissers in het Duitse mkb laat zien dat bedrijven hun eigen veiligheidsvolwassenheid overwegend hoog inschatten, terwijl er tegelijk sprake is van een hoog aantal ernstige beveiligingsincidenten en aanzienlijke onzekerheid over NIS2 (bron: Proliance, „Lage der Informationssicherheit im deutschen Mittelstand 2025“).

> **Wat dit voor u als MSP betekent**
> *Uw klanten denken vaak goed voorbereid te zijn omdat een maatregel ooit is gedocumenteerd; het bewijs van de voortdurende werkzaamheid is een gesprek dat de minsten uit zichzelf voeren, maar de meesten nodig hebben.*

Kernbevinding 2: NIS2 laat zich technisch beter afbeelden dan de AVG

Een van de meest verhelderende inzichten betreft een verschil dat we in onze oorspronkelijke aanpak niet zo scherp hadden voorzien: circa 6% van de gesprekspartners, overwegend ervaren juristen en auditors, wees onafhankelijk van elkaar en ongevraagd erop dat technische bevindingen zich duidelijk directer laten koppelen aan NIS2-vereisten dan aan AVG-artikelen. Een gesprekspartner formuleerde het pointeert: „NIS2-mapping kan meerwaarde bieden, AVG-mapping naar mijn mening niet."

De reden: NIS2-vereisten zijn grotendeels technisch en organisatorisch van aard en laten zich daardoor relatief goed onderbouwen met technisch bewijs. De AVG daarentegen is bewust technologieneutraal en risicogebaseerd geformuleerd. Art. 32 AVG vereist een risicoafweging op basis van de verwerkingscontext, het soort persoonsgegevens en de risico's voor betrokkenen, iets wat een kwetsbaarheidsscanner principieel niet kan beoordelen. Een gesprekspartner wees bovendien op art. 6 AVG: of een verwerking überhaupt een rechtsgrondslag heeft, ziet een scanner helemaal niet, ongeacht de kwaliteit van de technische koppeling.

Nog breder gedragen, bij ongeveer een op de tien gesprekspartners (ca. 10%), kwam de algemenere waarschuwing naar voren: een technische koppeling moet altijd worden begrepen als indicator en prioriteringshulp, nooit als geautomatiseerd compliancebewijs. Een bevinding is geen overtreding.

Wat dit voor u als MSP betekent

Wanneer u klanten technisch bewijs van beveiliging aanbiedt, positioneer dit dan realistisch: als een sterke, directe bijdrage aan NIS2-verantwoording, en als een waardevolle, maar aanvullende bouwsteen voor de AVG, die de juridische beoordeling door een privacyfunctionaris niet vervangt. Dit onderscheid beschermt u en uw klanten tegen een vals gevoel van veiligheid en maakt uw aanbod geloofwaardiger.

Kernbevinding 3: eigen verantwoordelijkheid werkt beter dan dwang, maar alleen met naam en termijn

Circa 5% van de gesprekspartners bevestigde onafhankelijk van elkaar: maatregelen die aansluiten bij de bedrijfswerkelijkheid worden vrijwillig nageleefd. Maatregelen die naast de praktijk staan, verzanden vrijwel altijd.

Citaat uit een gesprek

„risicoadequaat", zo omschreef een gesprekspartner het: afgestemd op de concrete dagelijkse bedrijfsvoering en gestaffeld naar risico

Tegelijk is duidelijke verantwoordelijkheid onmisbaar. Een auditor met een privacyachtergrond legde uit waarom een pure afdelingstoewijzing („de IT is verantwoordelijk") in de praktijk niet volstaat: bij een vraag van de toezichthouder of in een geschil is „de IT" geen houdbaar antwoord. Nodig is een naam met tijdstempel, en een mechanisme dat bij het uitblijven van actie automatisch escaleert.

Een andere gesprekspartner voegde een vaak over het hoofd geziene kant toe: zelfs als het SOC of de IT-afdeling een bevinding correct oplost, blijft dit vaak „stil" binnen de IT en bereikt het de directie niet, terwijl die wel het uiteindelijke aansprakelijkheidsrisico draagt.

Interessant: niet elke organisatie worstelt met dit probleem. Eén gesprekspartner, wiens organisatie wijzigingen consequent via een change- en ticketsysteem afhandelt, gaf aan dat bij elke wijziging automatisch de hele daaropvolgende procesketen wordt meegetoetst. Het jaarlijkse auditprobleem ontstaat bij hem structureel helemaal niet, een helder individueel bewijs dat het probleem oplosbaar is wanneer verantwoordelijkheid en trigger goed op elkaar zijn afgestemd.

Wat dit voor u als MSP betekent

Wanneer u beveiligingsoplossingen bij klanten invoert, let dan op twee dingen: dat maatregelen aansluiten bij de werkelijke bedrijfsvoering (anders worden ze genegeerd); en dat elke controle een benoemde, in tijd navolgbare verantwoordelijke heeft, geen afdeling, en met een zichtbaar pad naar de directie.

Waarom dit voor MSP's bijzonder relevant is

In de gesprekken kwam herhaaldelijk een patroon naar voren dat direct de rol van MSP's raakt: bij kleinere organisaties draagt vaak één persoon tegelijk de verantwoordelijkheid voor privacy, informatiebeveiliging en NIS2. Deze persoon heeft zelden de tijd of specialisatie om alle drie de terreinen even diep te doorgronden.

Dat verklaart waarom externe ondersteuning juist in het mkb zo gewild is. Als belangrijkste redenen voor achterstand bij de NIS2-implementatie noemen bedrijven volgens marktonderzoek de behoefte aan gespecialiseerde kennis (62 procent) en een gebrek aan interne capaciteit (39 procent) (bron: Proliance-studie 2025). Precies dat gat kunnen MSP's dichten, mits zij niet alleen kunnen beweren, maar ook kunnen aantonen dat controles werken.

Een blik op Nederland: wat valt er te leren?

Terwijl Duitsland sinds december 2025 onder de NIS2-Umsetzungsgesetz valt, wordt de NIS2-richtlijn in Nederland pas op 15 augustus 2026 in nationale wetgeving omgezet (Cyberbeveiligingswet). Nederlandse organisaties en MSP's staan daarmee voor dezelfde uitdaging, maar met een tijdsvoorsprong om te leren van de Duitse ervaring.

De centrale les uit de Duitse gesprekken: de overgang verloopt daar het best waar verantwoordelijkheid vroegtijdig en op naam is vastgelegd, in plaats van pas vlak voor de deadline pauschal afdelingen toe te wijzen. Ook blijkt dat organisaties die beveiligingsmaatregelen al vóór de wettelijke verplichting „risicoadequaat“ in plaats van puur formeel hadden ingericht, de overgang merkbaar soepeler ervaren. Nederlandse MSP's hebben tot augustus 2026 de gelegenheid om precies deze twee punten, benoemde verantwoordelijkheid en risicoadequate in plaats van generieke maatregelen, nu al met hun klanten te bespreken, in plaats van onder tijdsdruk te reageren.

Praktische aanknopingspunten voor het klantgesprek

Op basis van de reacties van de bevraagde DSB's en ISB's raden wij MSP's de volgende gespreksbenaderingen aan:

1. Vraag naar het laatste bewijs, niet alleen naar de laatste documentatie. „Wanneer is voor het laatst getoetst of deze maatregel nog werkt?“ is vaak een vraag die veel klanten niet kunnen beantwoorden, en die laat zien waar de werkelijke behoefte ligt.
2. Scheid NIS2- en AVG-communicatie bewust. Bied technisch bewijs zelfverzekerd aan voor NIS2, maar communiceer bij de AVG uitdrukkelijk dat de juridische eindbeoordeling bij de privacyfunctionaris blijft. Dat schept vertrouwen in plaats van scepsis.
3. Benoem altijd een persoon, nooit een afdeling. Wanneer u actieplannen met klanten afspreekt, zorg er dan voor dat elk punt een benoemde verantwoordelijke met termijn heeft, en dat compliance-relevante bevindingen ook de directie bereiken, niet alleen het SOC of de IT.
4. Laat zien wat er tussen de audits gebeurt. Klanten met een jaarlijks auditritme zijn kwetsbaar voor precies het gat dat in onze gesprekken het vaakst werd genoemd. Een aanbod voor doorlopende in plaats van alleen jaarlijkse toetsing is een duidelijk onderscheidend kenmerk.

Hoe Guardian360 Lighthouse hierbij ondersteunt

Guardian360 Lighthouse voert technische scans dagelijks uit in plaats van eenmalig per jaar, en koppelt elke bevinding direct aan een duidelijk benoemde, in tijd navolgbare aanbeveling. Dat adresseert rechtstreeks de in dit rapport beschreven gaten: het maakt het bewijs van werkzaamheid doorlopend in plaats van momentopname beschikbaar, ondersteunt een eerlijke scheiding tussen technische indicator en juridische beoordeling, en legt de basis zodat compliance-relevante bevindingen navolgbaar bij de juiste verantwoordelijken terechtkomen. Bevindingen zijn gekoppeld aan ISO 27001, de AVG, NIS2/de Cyberbeveiligingswet, NEN 7510 en de BIO, naast diverse andere normen, waardoor de technische werking van getroffen maatregelen aantoonbaar wordt in plaats van slechts afgevinkt. Guardian360 Lighthouse is opgezet als technische aanvulling op het managementsysteem van een klant, niet als vervanging daarvan.

Over deze studie

De in dit rapport samengevatte inzichten komen uit een kwalitatieve gespreksreeks die Guardian360 heeft gevoerd met Duitse privacyfunctionarissen, informatiebeveiligingsfunctionarissen en auditors, in het kader van de validatie van een aanpak die technische beveiligingsbevindingen koppelt aan AVG-, NIS2- en ISO 27001-verplichtingen. De genoemde percentages hebben betrekking op de ontvangen reacties en moeten worden gelezen als kwalitatieve tendens, niet als representatieve statistiek. Externe bronvermeldingen zijn als zodanig aangeduid.

Guardian360 is een Nederlandse onderneming met ISO 27001-certificering. Via het platform Guardian360 Lighthouse ondersteunen wij MSP's en IT-dienstverleners in heel Europa bij het aanbieden van continue beveiligingsmonitoring aan hun klanten.

Kengetal	Waarde
Ontvangen inhoudelijke vakgesprekken	ca. 100
Periode	Juni tot en met juli 2026
Doelgroep	Privacy- en informatiebeveiligingsfunctionarissen in Duitsland
Methode	Open, kwalitatieve vakgesprekken (geen representatieve steekproef)