# DU PAPIER A LA PREUVE

Ce que les délégués à la protection des données et responsables de la sécurité de l'information allemands disent aux MSP en 2026

Juillet 2026

**Une centaine d'entretiens avec des délégués à la protection des données et responsables de la sécurité de l'information allemands**

Une étude qualitative en amont de la transposition néerlandaise de NIS2 (Cyberbeveiligingswet, 15 août 2026)

Commandité par

GUARDIAN 360°

Kruisplein 484, 3012 CC Rotterdam, Pays-Bas

# Introduction

Depuis le 6 décembre 2025, la loi allemande de transposition de NIS2 est en vigueur sans période transitoire. Pour les MSP, cela signifie que leurs clients ne demandent plus seulement «sommes-nous en sécurité ?», mais «pouvons-nous le prouver ?»

Pour comprendre comment les délégués à la protection des données (DPO) et les responsables de la sécurité de l'information allemands répondent à cette question dans la pratique, Guardian360 a mené une centaine d'entretiens professionnels ouverts et qualitatifs sur une démarche concrète : relier les constats techniques de sécurité aux obligations du RGPD, de NIS2 et d'ISO 27001.

Il ne s'agit délibérément pas d'une étude de référence représentative, mais d'un recueil qualitatif d'avis professionnels. Les pourcentages mentionnés ici concernent les réponses reçues et doivent être lus comme une tendance, non comme un chiffre statistiquement établi.

Ce rapport résume ce que nous avons appris, et ce que cela signifie pour vos échanges avec vos clients.

# Constat clé 1 : l'écart entre documentation et preuve

Les entretiens avec les DPO et responsables de la sécurité de l'information ont clairement montré que la principale faiblesse se situe rarement dans la technique elle-même, mais dans le fait que les contrôles documentés sont rarement retestés une fois mis en place. Environ un interlocuteur sur vingt (environ 5 %) a décrit indépendamment le même schéma : une mesure est mise en œuvre une fois, documentée, puis plus jamais remise en question dans le cycle d'audit annuel, jusqu'à ce que la responsabilité «se dilue dans le sable».

> **Citation extraite d'un entretien**
>
> *«Les lois sont fondées sur le risque, les scanners sont binaires.» Selon un auditeur en sécurité informatique.*

Cette observation rejoint des données externes : une étude de Proliance menée auprès de 122 décideurs du Mittelstand allemand montre que les entreprises ont tendance à surestimer leur propre maturité en matière de sécurité, alors même qu'elles font face à un nombre élevé d'incidents de sécurité graves et à une incertitude considérable concernant NIS2 (source : Proliance, «Lage der Informationssicherheit im deutschen Mittelstand 2025»).

> **Ce que cela signifie pour vous en tant que MSP**
>
> *Vos clients pensent souvent être bien préparés parce qu'une mesure a été documentée un jour ; la preuve de son efficacité continue est une conversation que peu de clients engagent d'eux-mêmes, mais dont la plupart ont besoin.*

# Constat clé 2 : NIS2 se prête mieux à une cartographie technique que le RGPD

L'un des enseignements les plus révélateurs concerne une distinction que notre démarche initiale n'avait pas anticipée avec autant de clarté : environ 6 % des interlocuteurs, principalement des juristes et auditeurs expérimentés, ont souligné indépendamment et sans qu'on le leur demande que les constats techniques se rattachent bien plus directement aux exigences de NIS2 qu'aux articles du RGPD. L'un d'eux l'a formulé de façon incisive : «La cartographie NIS2 peut apporter de la valeur ; la cartographie RGPD, à mon avis, non.»

La raison : les exigences de NIS2 sont largement techniques et organisationnelles par nature, et se prêtent donc relativement bien à une preuve technique. Le RGPD, en revanche, est délibérément neutre sur le plan technologique et fondé sur le risque. L'article 32 du RGPD exige une évaluation du risque tenant compte du contexte du traitement, de la catégorie de données personnelles et des risques pour les personnes concernées, ce qu'un scanner de vulnérabilités ne peut par principe pas évaluer. Un interlocuteur a également souligné l'article 6 du RGPD : un scanner ne voit absolument pas si un traitement dispose seulement d'une base légale, quelle que soit la qualité de la cartographie technique.

Plus largement partagée, chez environ un interlocuteur sur dix (environ 10 %), figurait la mise en garde plus générale selon laquelle une cartographie technique doit toujours être comprise comme un indicateur et une aide à la priorisation, jamais comme une preuve de conformité automatisée. Un constat n'est pas une violation.

**Ce que cela signifie pour vous en tant que MSP**

*Lorsque vous proposez à vos clients des preuves techniques de sécurité, positionnez-les de façon réaliste : comme une contribution forte et directe à la démonstration de conformité NIS2, et comme un complément précieux, mais non substitutif, pour le RGPD, qui ne remplace pas l'évaluation juridique d'un DPO. Cette distinction vous protège, vous et vos clients, d'un faux sentiment de sécurité et rend votre offre plus crédible.*

# Constat clé 3 : la responsabilisation l'emporte sur la contrainte, mais seulement avec un nom et un délai

Environ 5 % des interlocuteurs ont confirmé, indépendamment les uns des autres : les mesures adaptées à la réalité de l'entreprise sont suivies volontairement. Les mesures déconnectées de la pratique finissent presque toujours par s'enliser.

**Citation extraite d'un entretien**

*«proportionnée au risque», comme l'a décrit un interlocuteur : adaptée au quotidien concret de l'entreprise et graduée selon le risque*

Dans le même temps, une responsabilité claire reste indispensable. Un auditeur ayant une formation en protection des données a expliqué pourquoi une simple attribution à un service («c'est l'informatique qui est responsable») ne suffit pas dans la pratique : face à une question de l'autorité de contrôle, ou en cas de litige, «l'informatique» n'est pas une réponse défendable. Ce qu'il faut, c'est un nom associé à un horodatage, et un mécanisme d'escalade automatique en cas de non-résolution.

Un autre interlocuteur a ajouté un aspect souvent négligé : même lorsque le SOC ou l'informatique résout correctement un constat, cela reste fréquemment «silencieux» au sein de l'informatique et n'atteint jamais la direction, alors que celle-ci porte pourtant le risque de responsabilité final.

Fait intéressant, toutes les organisations ne sont pas confrontées à ce problème. Un interlocuteur, dont l'organisation traite les changements de façon systématique via un système de gestion des changements et de tickets, a indiqué que chaque changement déclenche automatiquement le contrôle de l'ensemble de la chaîne de processus en aval. Le problème de l'audit annuel ne se pose structurellement jamais chez lui, preuve individuelle claire que le problème est résoluble lorsque responsabilité et déclencheur sont correctement articulés.

**Ce que cela signifie pour vous en tant que MSP**

*Lorsque vous mettez en place des solutions de sécurité chez vos clients, veillez à deux choses : que les mesures correspondent à la réalité effective de l'entreprise (sinon elles seront ignorées) ; et que chaque contrôle ait un responsable nommé et horodaté, jamais un simple service, avec une voie visible vers la direction.*

## Pourquoi cela concerne particulièrement les MSP

Les entretiens ont fait ressortir de façon répétée un schéma qui touche directement le rôle des MSP : dans les organisations plus petites, une seule personne porte souvent la responsabilité de la protection des données, de la sécurité de l'information et de NIS2 à la fois. Cette personne a rarement le temps ou la spécialisation nécessaires pour maîtriser ces trois domaines avec la même profondeur.

Cela explique pourquoi le soutien externe est si recherché, en particulier au sein des PME. Selon des études de marché, les entreprises citent le besoin d'expertise spécialisée (62 %) et le manque de capacités internes (39 %) comme principales raisons de leur retard dans la mise en œuvre de NIS2 (source : étude Proliance 2025). C'est précisément l'écart que les MSP peuvent combler, à condition de pouvoir non seulement l'affirmer, mais aussi démontrer que les contrôles fonctionnent réellement.

# Un regard sur les Pays-Bas : quels enseignements en tirer ?

Alors que l'Allemagne est soumise à sa loi de transposition de NIS2 depuis décembre 2025, les Pays-Bas ne transposeront la directive NIS2 en droit national que le 15 août 2026 (la Cyberbeveiligingswet). Les organisations et MSP néerlandais font donc face au même défi, mais avec une avance dans le temps leur permettant de tirer les leçons de l'expérience allemande.

La leçon centrale des entretiens allemands : la transition se passe le mieux là où la responsabilité est établie tôt et nommément, plutôt que d'attribuer des services entiers juste avant l'échéance. Il apparaît également que les organisations ayant déjà mis en place des mesures de sécurité «proportionnées au risque» plutôt que purement formelles avant l'entrée en vigueur de l'obligation légale vivent une transition sensiblement plus fluide. Les MSP néerlandais ont jusqu'en août 2026 pour aborder dès maintenant ces deux points, responsabilité nommée et mesures proportionnées au risque plutôt que génériques, avec leurs clients, plutôt que de réagir sous la pression du temps.

# Pistes concrètes pour l'échange avec vos clients

Sur la base des réponses des DPO et responsables de la sécurité de l'information interrogés, nous recommandons aux MSP les approches suivantes :

1. Demandez la dernière preuve, pas seulement la dernière documentation. «Quand a-t-on vérifié pour la dernière fois que cette mesure fonctionne encore ?» est souvent une question à laquelle de nombreux clients ne peuvent pas répondre, et qui révèle précisément où se situe le véritable besoin.
2. Séparez délibérément la communication NIS2 et RGPD. Proposez des preuves techniques avec assurance pour NIS2, mais indiquez clairement, pour le RGPD, que l'évaluation juridique finale reste du ressort du DPO. Cela instaure la confiance plutôt que le scepticisme.
3. Nommez toujours une personne, jamais un service. Lorsque vous convenez de plans d'action avec vos clients, assurez-vous que chaque point ait un responsable nommé avec un délai, et que les constats pertinents pour la conformité parviennent aussi à la direction, pas seulement au SOC ou à l'informatique.
4. Montrez ce qui se passe entre les audits. Les clients soumis à un cycle d'audit annuel sont vulnérables précisément à l'écart le plus souvent mentionné dans nos entretiens. Proposer un contrôle continu plutôt qu'uniquement annuel constitue un facteur de différenciation clair.

## Comment Guardian360 Lighthouse y contribue

Guardian360 Lighthouse effectue des analyses techniques quotidiennes plutôt qu'une seule fois par an, et relie chaque constat directement à une recommandation clairement nommée et horodatée. Cela répond directement aux écarts décrits dans ce rapport : la preuve d'efficacité devient disponible en continu plutôt que sous forme d'instantané ponctuel, une séparation honnête est maintenue entre indicateur technique et évaluation juridique, et les bases sont posées pour que les constats pertinents pour la conformité parviennent, de façon traçable, aux bonnes personnes responsables. Les constats sont rattachés à ISO 27001, au RGPD, à NIS2, à DORA et à l'OWASP, parmi d'autres référentiels, ce qui rend l'efficacité technique des mesures mises en œuvre démontrable plutôt que simplement cochée. Guardian360 Lighthouse est conçu comme un complément technique au système de management d'un client, non comme un substitut.

## À propos de cette étude

Les enseignements résumés dans ce rapport proviennent d'une série d'entretiens qualitatifs menés par Guardian360 avec des délégués à la protection des données, des responsables de la sécurité de l'information et des auditeurs allemands, dans le cadre de la validation d'une démarche reliant les constats techniques de sécurité aux obligations du RGPD, de NIS2 et d'ISO 27001. Les pourcentages mentionnés concernent les réponses reçues et doivent être lus comme une tendance qualitative, non comme une statistique représentative. Les sources externes sont indiquées comme telles.

*Guardian360 est une entreprise néerlandaise certifiée ISO 27001. Via la plateforme Guardian360 Lighthouse, nous accompagnons les MSP et prestataires informatiques dans toute l'Europe afin qu'ils proposent à leurs clients une surveillance continue de la sécurité.*

| Indicateur | Valeur |
|---|---|
| Entretiens professionnels substantiels reçus | environ 100 |
| Période | Juin à juillet 2026 |
| Public cible | Délégués à la protection des données et responsables de la sécurité de l'information en Allemagne |
| Méthode | Entretiens professionnels ouverts et qualitatifs (échantillon non représentatif) |