NIS 2 ART. 21(2)(D)

Questionario per i fornitori NIS 2

Un questionario aperto e ancorato al diritto dell'UE per la valutazione dei fornitori ai sensi di NIS 2

Profilo del fornitore	18 campi
Pratiche di sicurezza	26 campi
Specifico per SaaS	5 campi
Specifico per On-Premise	4 campi
Professional Services	3 campi
Managed Services	3 campi

Ogni campo è ancorato a una fonte primaria a livello UE: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28 o il Cyber Resilience Act. Le integrazioni settoriali (TISAX, VDA ISA, BSI C5, KRITIS) si aggiungono a questa base.

Fonte: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

Licenza: MIT (schema) + CC BY 4.0 (contenuto). Libero di usare, forkare e adattare.

1. Profilo del fornitore

18 campi

Denominazione legale

STRING · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2

Il nome registrato della vostra azienda, così come appare nel registro delle imprese. Esempio: Müller GmbH o Acme Software Ltd.

Indirizzo della sede legale

STRING · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2

L'indirizzo commerciale registrato della vostra azienda. È sufficiente un solo indirizzo, anche se avete più sedi.

Paese

COUNTRY · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2

Il paese in cui la vostra azienda è legalmente stabilita. Due lettere, ad esempio DE per la Germania.

Dominio principale

URL · FACOLTATIVO · BASE GIURIDICA: ENISA TIG §5.2(B)

Il vostro dominio principale, di solito l'URL del vostro sito web. Esempio: acmesoftware.com.

Slogan (una riga, visibile ai clienti)

STRING · FACOLTATIVO · BASE GIURIDICA: ENISA TIG §5.2(B)

Una riga che riassume ciò che offrite. I clienti la vedono nel vostro profilo fornitore. Esempio: ERP per la produzione delle PMI.

Descrizione pubblica (più estesa)

TEXT · FACOLTATIVO · BASE GIURIDICA: ENISA TIG §5.2(B)

Due o tre frasi sulla vostra azienda e su ciò che fate. Questo testo appare nel vostro profilo fornitore. Argomentazione commerciale, posizionamento di sicurezza o entrambi.

Descrizione dei servizi forniti

TEXT · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2(B) + §5.1.4 TIPS

Un paragrafo su ciò che la vostra azienda fornisce tecnicamente ai clienti. Prodotti, moduli o servizi concreti. Evitate il linguaggio puramente di marketing.

Paesi / regioni in cui vengono trattati i dati dei clienti

STRING · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Tutti i paesi in cui i dati dei vostri clienti vengono archiviati o trattati. Separati da virgole, codici paese ISO. Esempio: DE, NL, US. Se trattate interamente all'interno dell'UE, è sufficiente elencare i paesi dell'UE.

Nome del referente per la sicurezza

STRING · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(D)

La persona che i clienti contattano in caso di incidente di sicurezza. Nelle aziende più piccole spesso l'amministratore delegato o il responsabile IT. È sufficiente una sola persona.

E-mail di contatto per gli incidenti

EMAIL · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(D)

Indirizzo e-mail che i clienti utilizzano per segnalare un incidente di sicurezza. Idealmente una lista di distribuzione come security@example.com che raggiunge più persone.

Telefono di contatto per gli incidenti (24/7)

PHONE · FACOLTATIVO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(D)

Numero di telefono per le segnalazioni urgenti di incidenti. Se non disponete di reperibilità 24/7, indicate il vostro orario lavorativo tra parentesi.

SLA di notifica degli incidenti (ore)

INTEGER · FACOLTATIVO · BASE GIURIDICA: NIS2 ART. 23

Ore tra il rilevamento di un incidente e la notifica al cliente, al più tardi. Autovalutazione realistica, non un valore ideale. Valori comuni: 24, 48 o 72 ore.

ID di registrazione BSI (solo se la vostra azienda è essa stessa regolamentata da NIS2)

STRING · FACOLTATIVO · BASE GIURIDICA: ENISA TIG §5.1.2

Se la vostra azienda è essa stessa soggetta a NIS 2 e registrata presso il BSI, inserite qui l'ID di registrazione. Facoltativo. Consente ai clienti di vedere a colpo d'occhio che soddisfate lo stesso obbligo di un'entità regolamentata.

Forniamo servizi SaaS / in hosting

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2(B)

Eseguite software per i clienti sulla vostra infrastruttura e lo erogate tramite internet. Selezionate più caselle se offrite più modelli.

Forniamo software on-premise

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2(B)

Fornite software che i clienti installano ed eseguono sulla propria infrastruttura.

Forniamo servizi professionali / consulenza

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2(B)

La vostra prestazione principale è il lavoro umano: consulenza, implementazione, formazione, audit o personalizzazione.

Forniamo servizi gestiti / MSP

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.2(B)

Gestite per il cliente parti della sua infrastruttura IT, con personale proprio. Tipico dei modelli MSP e MSSP.

Utilizziamo, integriamo o forniamo sistemi di IA

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(D)

I vostri prodotti o servizi trattano i dati dei clienti tramite un modello di IA o ML? Sono inclusi i modelli esterni richiamati tramite API, ad esempio OpenAI o Anthropic.

2. Pratiche di sicurezza

26 campi

Sistema di gestione della sicurezza delle informazioni documentato (ISMS)

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.2(A)

Selezionare sì se si dispone di una politica scritta di sicurezza delle informazioni con ruoli assegnati, revisioni periodiche e gestione documentata degli incidenti. Una certificazione ISO 27001 o BSI Grundschutz implica sì.

Possesso di una certificazione ISO 27001, BSI Grundschutz o equivalente

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.2(B)

Selezionare sì se la vostra azienda possiede attualmente una certificazione ISO 27001, BSI Grundschutz, SOC 2 Type II o equivalente. Caricate il certificato nella scheda Certificazioni.

Formazione annuale di sensibilizzazione alla sicurezza per tutto il personale

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(B)

Selezionare sì se ogni dipendente riceve almeno una formazione annuale di sensibilizzazione alla sicurezza delle informazioni. L'e-learning è valido; le simulazioni di phishing si aggiungono.

Verifiche dei precedenti per il personale con accesso ai dati dei clienti

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(C)

Selezionare sì se si effettua una verifica dei precedenti per il personale con accesso ai dati dei clienti. Livello comune: estratto del casellario giudiziale o documento equivalente al momento dell'assunzione.

Processo documentato di gestione delle vulnerabilità e di patching

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(F)

Selezionare sì se si dispone di un processo scritto per la gestione delle vulnerabilità di sicurezza: rilevare, valutare, dare priorità, applicare patch o mitigare. Il monitoraggio delle CVE e il patching guidato da SLA sono lo standard.

Accettare il diritto di audit del cliente (o fornire relazioni di audit)

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(E)

Selezionare sì se si concede ai clienti un diritto di audit in loco oppure si forniscono relazioni di audit sostitutive (ad esempio SOC 2, ISAE 3402).

Ricorso a subincaricati / subfornitori

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(G)

Selezionare sì se per erogare il servizio si ricorre ad altre aziende che hanno accesso ai dati o all'infrastruttura dei clienti. Esempi tipici: AWS, Azure, Cloudflare, Stripe.

Elenco dei subincaricati

TEXT · CONDIZIONALE · BASE GIURIDICA: CIR 2024/2690 §5.1.4(G)

Elencare ogni subincaricato con nome, luogo di trattamento e attività svolta per voi. È sufficiente una tabella o un elenco puntato. Aggiornatela ogni volta che ne aggiungete o rimuovete uno.

Impegno a restituire / distruggere i dati dei clienti alla cessazione

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: CIR 2024/2690 §5.1.4(H)

Selezionare sì se ci si impegna contrattualmente a restituire o distruggere i dati dei clienti al termine del contratto. Prassi comune: export e restituzione, quindi cancellazione entro 30 giorni.

Accordo standard sul trattamento dei dati (DPA) disponibile

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: GDPR ART. 28

Selezionare sì se si dispone di un accordo standard sul trattamento dei dati ai sensi dell'articolo 28 del GDPR che i clienti possono firmare. Richiesto non appena si trattano dati personali.

Politiche di sicurezza riviste almeno annualmente

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(A) / ENISA TIG §1.1

Selezionare sì se le vostre politiche di sicurezza vengono riviste almeno una volta all'anno e aggiornate secondo necessità. Una nota scritta nel documento è una prova sufficiente.

Piano di risposta agli incidenti documentato

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Selezionare sì se si dispone di un piano scritto per la gestione degli incidenti di sicurezza: chi decide, chi comunica, chi documenta. Almeno un'esercitazione tabletop all'anno è una buona prassi.

Piano di continuità operativa / ripristino di emergenza documentato

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Selezionare sì se si dispone di un piano che spiega come mantenere l'operatività o ripristinare rapidamente durante un'interruzione: sistemi critici, soluzioni di ripiego, obiettivi RTO e RPO.

Politica di crittografia documentata

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Selezionare sì se avete messo per iscritto quale crittografia utilizzate e dove: dati in transito (TLS 1.2+), dati a riposo (AES-256), gestione delle chiavi, algoritmi di hashing.

Gestione degli accessi privilegiati (PAM) per il personale interno

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Selezionare sì se gli amministratori e gli account privilegiati dispongono di controlli aggiuntivi: accesso separato, MFA, registrazione delle sessioni o accesso just-in-time.

MFA imposto per tutti gli account amministrativi / privilegiati interni

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(J)

Selezionare sì se ogni account amministrativo o privilegiato interno deve utilizzare l'MFA. I token hardware o le app di autenticazione sono validi; gli SMS no.

Mantenere un inventario degli asset informativi

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(I) / ENISA TIG §12.4

Selezionare sì se si mantiene un elenco aggiornato di ogni sistema informativo utilizzato per erogare il servizio: server, database, strumenti SaaS, endpoint. È sufficiente un foglio di calcolo.

Programma di penetration test annuale o biennale

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Selezionare sì se si commissiona un penetration test esterno almeno ogni uno o due anni. Per le aziende più piccole, una scansione esterna delle vulnerabilità come passo minimo è accettabile.

Divulghiamo gli eventi di cibersicurezza notificabili passati su richiesta dei clienti

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.2

Selezionare sì se, su richiesta del cliente, divulgate apertamente se e quali incidenti di sicurezza notificabili la vostra azienda ha avuto in passato. Finestra comune: gli ultimi tre-cinque anni.

Fornire assistenza ai clienti in caso di incidente senza costi / a costo predefinito

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Selezionare sì se ci si impegna ad assistere i clienti senza costi aggiuntivi quando un incidente è causato dal proprio prodotto o servizio. Se invece si concorda in anticipo una tariffa giornaliera predefinita, selezionare comunque sì.

Cooperare pienamente con le autorità competenti (BSI, ENISA, CSIRT nazionali)

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Selezionare sì se ci si impegna a cooperare pienamente con le autorità competenti come BSI, ENISA o i CSIRT nazionali durante le ispezioni, gli audit e la gestione degli incidenti. Standard per i fornitori seri.

Notificare ai clienti qualsiasi modifica sostanziale che incida sull'erogazione del servizio

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Selezionare sì se ci si impegna a notificare ai clienti qualsiasi modifica sostanziale che incida sulla capacità di erogare il servizio: acquisizioni, cambi di subincaricato, importanti cambiamenti tecnici.

Notificare ai clienti in anticipo in caso di cambiamento dei luoghi di trattamento dei dati

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Selezionare sì se si informano i clienti in anticipo prima che cambi il luogo di trattamento dei loro dati. Importante per la protezione dei dati e per una supervisione della catena di approvvigionamento conforme al GDPR.

Strategia di uscita documentata con periodo di transizione obbligatorio

BOOLEAN · OBBLIGATORIO · BASE GIURIDICA: ENISA TIG §5.1.4 TIPS

Selezionare sì se si dispone di una strategia di uscita scritta: quanto dura un passaggio di consegne ordinato, quali dati e conoscenze vengono trasferiti, a cosa ci si impegna durante la transizione.

Fornire un SBOM-for-AI secondo gli elementi minimi del G7

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

Facoltativo. Selezionare sì se è possibile fornire un SBOM-for-AI secondo gli elementi minimi del G7 (maggio 2026). Documenta metadati, modelli, dati di addestramento, infrastruttura, proprietà di sicurezza, KPI e comportamento del sistema. Standard volontario.

URL del documento SBOM-for-AI

URL · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

URL pubblico o condiviso del vostro documento SBOM-for-AI. Può essere un PDF, un file JSON o una pagina di progetto.

3. Specifico per SaaS

5 campi

Regione di hosting

STRING · CONDIZIONALE · BASE GIURIDICA: ENISA TIG §5.2

La regione cloud in cui sono ospitati i dati dei clienti. Esempio: AWS eu-central-1, Azure West Europe. Indicare la regione principale; le regioni secondarie o di backup possono essere aggiunte separate da virgole.

Cifratura dei dati a riposo

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Selezionare sì se i dati dei clienti su disco sono cifrati a riposo con AES-256 o equivalente. È valida la cifratura del disco gestita dal cloud (AWS EBS, Azure Disk Encryption).

Cifratura in transito (TLS ≥ 1.2)

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Selezionare sì se tutti gli endpoint rivolti ai clienti impongono TLS 1.2 o superiore. TLS 1.3 è da preferire. Il semplice HTTP deve reindirizzare a HTTPS.

MFA imposto per tutti gli account amministrativi

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(J) / ENISA TIG §11.3

Selezionare sì se ogni account amministrativo interno sulla piattaforma SaaS deve utilizzare l'MFA. Stesso standard della vostra policy amministrativa interna.

Obiettivo del tempo di ripristino (RTO) in ore

INTEGER · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Numero massimo di ore in cui il servizio può essere non disponibile prima del ripristino. Valore SLA realistico, non un valore ideale. Valori SaaS comuni: 4, 8 o 24 ore.

4. Specifico per On-Premise

4 campi

Fornire una distinta base del software (SBOM)

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: CRA / NIS2 ART. 21(2)(D)

Selezionare sì se si fornisce una distinta base del software (SBOM) con ogni release. CycloneDX o SPDX sono i formati standard. Obbligatorio ai sensi del Cyber Resilience Act per i prodotti immessi sul mercato dell'UE a partire da dicembre 2027.

Le release sono firmate crittograficamente

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Selezionare sì se ogni artefatto di release reca una firma crittografica verificabile dai clienti. Le chiavi di firma sono documentate e soggette a rotazione. Sono valide sia le firme Sigstore sia quelle PGP.

Politica di divulgazione delle vulnerabilità pubblicata

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(E) / ENISA TIG §3

Selezionare sì se si dispone di una modalità documentata pubblicamente per segnalare le vulnerabilità di sicurezza. È sufficiente un file security.txt sul proprio dominio (secondo RFC 9116) o un indirizzo e-mail dedicato come security@example.com.

SLA delle patch per CVE critiche (ore)

INTEGER · CONDIZIONALE · BASE GIURIDICA: CIR 2024/2690 §5.1.4(F)

Ore tra la divulgazione pubblica di una CVE e una release con patch per le vulnerabilità critiche (CVSS 9.0+). Impegno realistico, non un valore ideale. Valori comuni: 24, 48 o 72 ore.

5. Professional Services

3 campi

Ambito delle verifiche dei precedenti

STRING · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(I) / CIR 2024/2690 §5.1.4(C)

Descrivere come vengono valutati i consulenti per i ruoli sensibili. Esempio: estratto del casellario giudiziale per tutti i consulenti, oltre a verifiche delle referenze per gli incarichi che coinvolgono dati classificati.

NDA stipulato con tutti i consulenti

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.4

Selezionare sì se ogni consulente firma un accordo di riservatezza prima di essere assegnato al lavoro presso il cliente. Come parte del contratto di lavoro oppure come NDA separato.

Politica di comportamento documentata presso la sede del cliente

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Selezionare sì se si dispone di un codice di condotta scritto per i consulenti che operano presso la sede del cliente: gestione dei badge, obbligo di blocco dello schermo, comportamento da tenere se i dati lasciano la sede.

6. Managed Services

3 campi

Gestione degli accessi privilegiati (PAM) attiva

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Selezionare sì se si utilizza uno strumento di gestione degli accessi privilegiati per le sessioni remote amministrative sui sistemi dei clienti. Esempi: CyberArk, BeyondTrust, Teleport. Una configurazione jump-host con registrazione dei log è valida.

Le sessioni amministrative vengono registrate

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(F) / ENISA TIG §10

Selezionare sì se le sessioni amministrative sui sistemi dei clienti vengono registrate e conservate per la verifica. Conservazione comune: da 90 giorni a 1 anno. Necessaria per la ricostruzione forense dopo gli incidenti.

Reperibilità 24/7

BOOLEAN · CONDIZIONALE · BASE GIURIDICA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Selezionare sì se si gestisce una reperibilità 24/7 che risponde agli incidenti di sicurezza sui sistemi dei clienti. Il supporto limitato all'orario lavorativo non è sufficiente.