GIDS

De complete gids voor Data Encryptie & Key Management

Versleuteling, sleutelbeheer, AVG, NIS2, post-quantum en kosten. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Data-encryptie is een van de krachtigste beveiligingsmaatregelen, maar wordt nog te weinig ingezet. Deze cijfers onderbouwen waarom.

33%
van Nederlandse micro-ondernemingen (2--10 pers.) gebruikt data-encryptie
CBS Cybersecuritymonitor 2024 [1]

90%
van grote bedrijven (250+ pers.) gebruikt data-encryptie
CBS Cybersecuritymonitor 2024 [1]

8%
van organisaties versleutelt het merendeel van hun sensitieve cloud-data
Thales Data Threat Report 2025 [2]

USD 4,44M
gemiddelde kosten van een datalek wereldwijd (2025)
IBM Cost of Data Breach 2025 [3]

60%
van organisaties evalueert post-quantum cryptografie (PQC) oplossingen
Thales Data Threat Report 2025 [2]

57%
van organisaties gebruikt 5+ verschillende key managers -- te complex
Thales Data Threat Report 2025 [2]

USD 3,37B
verwachte marktomvang key management software (2026)
Business Research Company [4]

Art. 34
AVG: bij versleutelde data geen meldplicht aan betrokkenen bij datalek
AVG/GDPR [5]

1. Wat is data encryptie & key management?

Data-encryptie is het omzetten van leesbare data naar onleesbare code met behulp van een cryptografische sleutel. Key management is het beheren van die sleutels.

Encryptie beschermt data op twee manieren: at rest (opgeslagen data: databases, bestanden, backups) en in transit (data tijdens transport: netwerk, API's, e-mail). Zonder de juiste sleutel is versleutelde data onleesbaar, zelfs als een aanvaller fysieke toegang krijgt tot je systemen.

Key management is minstens zo belangrijk als de encryptie zelf. Het omvat de volledige levenscyclus van cryptografische sleutels: generatie, distributie, opslag, gebruik, rotatie, archivering en vernietiging. NIST SP 800-57 is de standaard die deze lifecycle definieert [6].

TYPEN ENCRYPTIE

TYPE	BESCHERMT	STANDAARD
At rest	Opgeslagen data: databases, disk, backup	AES-256
In transit	Data tijdens transport: netwerk, API	TLS 1.2/1.3
End-to-end	Volledig pad: verzender tot ontvanger	S/MIME, PGP
Tokenisatie	Gevoelige velden (creditcard, BSN)	PCI DSS

2. Waarom is het belangrijk?

Encryptie is de meest effectieve maatregel om de impact van een datalek te beperken, en het is steeds vaker verplicht.

Slechts 33% van Nederlandse micro-ondernemingen gebruikt data-encryptie [1]. Dat betekent dat twee derde van de kleinste bedrijven hun gevoelige data onversleuteld opslaat. Bij een datalek is de impact dan maximaal: volledige blootstelling van persoonsgegevens, financiele data en bedrijfsgeheimen.

Encryptie biedt een krachtige bescherming in de AVG: bij datalekken met correct versleutelde data vervalt de meldplicht aan betrokkenen (Art. 34) [5]. Dit beperkt niet alleen de schade, maar ook de reputatie-impact en potentiele boetes.

> **Business case:** Gemiddelde kosten datalek: USD 4,44 miljoen. Een encryptie-implementatie voor MKB: EUR 3.000--40.000. Encryptie als verzachtende factor bij AVG-boetes kan miljoenen schelen.

3. Hoe werkt het? Het implementatieproces

1 Data-inventarisatie en classificatie

WEEK 1--2

Breng alle data in kaart: wat heb je, waar staat het, hoe gevoelig is het? Classificeer op basis van regelgeving (AVG, NIS2, PCI DSS) en bedrijfsimpact.

2 Key management-architectuur kiezen

WEEK 2--3

Kies tussen cloud KMS (AWS, Azure, Google), on-premise HSM of hybrid. De keuze hangt af van budget, compliance-eisen en data-soevereiniteitsbehoeften.

3 Encryptie implementeren

WEEK 3--6

Versleutel data at rest (databases, endpoints, backups) en in transit (TLS, VPN). Begin met de gevoeligste data en werk uit naar de rest.

4 Key rotation en beleid

WEEK 5--7

Configureer automatische key rotation. Stel beleid op: wie mag sleutels aanmaken, gebruiken en vernietigen? Documenteer procedures.

5 Testen en monitoring

WEEK 7--8

Test recovery-procedures: kun je data herstellen na sleutelverlies? Monitor sleutelgebruik, detecteer afwijkingen, evalueer periodiek.

4. Wat kost het?

TIER	OMSCHRIJVING	PRIJSINDICATIE	EENHEID
Basis	Data-inventarisatie, endpoint en e-mail encryptie, basis key management, beleid opstellen	EUR 3.000 -- 10.000	per project
Standaard	Volledige implementatie: at rest en in transit, centraal key management, cloud KMS, compliance rapportage	EUR 10.000 -- 40.000	per project
Premium	Enterprise key management: HSM-integratie, multi-cloud, automated rotation, PQC-readiness, managed service	EUR 3.000 -- 15.000	per maand

MKB-TIP

Begin met wat je al hebt: veel cloud-providers bieden standaard encryptie at rest. Focus je investering op key management (wie beheert de sleutels?) en encryptie van de gevoeligste data die nog niet versleuteld is.

5. Waar moet je op letten bij een aanbieder?

- **Key management-expertise** -- Encryptie zonder goed sleutelbeheer is zinloos
- **Cloud-ervaring** -- Ervaring met jouw cloud-provider (AWS, Azure, Google)
- **NIST SP 800-57 kennis** -- De standaard voor key management lifecycle
- **Compliance-ervaring** -- AVG, NIS2, PCI DSS, NEN 7510 waar relevant
- **Post-quantum readiness** -- Kan de aanbieder adviseren over toekomstige migratie?

> **RED FLAGS**
>
> Wees alert als een aanbieder: encryptie als "plug-and-play" presenteert zonder key management, geen recovery-procedures bespreekt, sleutels en data op dezelfde locatie opslaat, of post-quantum cryptografie niet op de radar heeft.

6. Veelgemaakte fouten

1. Encryptie zonder key management

Versleuteling is zo sterk als je sleutelbeheer. Als sleutels onveilig zijn opgeslagen of nooit geroteerd worden, is encryptie schijnveiligheid.

2. Alles tegelijk versleutelen

Begin met de gevoeligste data (persoonsgegevens, financieel) en werk gefaseerd uit. Alles tegelijk implementeren leidt tot fouten en performance-problemen.

3. Performance-impact onderschatten

Encryptie kost rekenkracht. Test de impact op je systemen voordat je live gaat, vooral bij databases met hoge transactievolumes.

4. Recovery niet testen

Als je een sleutel kwijtraakt en geen recovery-procedure hebt getest, is je data permanent verloren. Test recovery voordat je afhankelijk bent van encryptie.

5. Cloud-encryptie als voldoende beschouwen

Standaard cloud-encryptie (server-side encryption) beschermt tegen fysieke diefstal, maar niet tegen een gecompromitteerd admin-account. Overweeg BYOK of client-side encryption voor gevoelige data.

7. Compliance: AVG, NIS2 en regelgeving

AVG / GDPR

Encryptie wordt in Art. 32 AVG expliciet genoemd als "passende technische maatregel" [5]. Bij datalekken met correct versleutelde data vervalt de meldplicht aan betrokkenen (Art. 34). Boetes: tot EUR 20 miljoen of 4% van jaaromzet.

NIS2 / CYBERBEVEILIGINGSWET

Encryptie is expliciet benoemd in de Cyberbeveiligingswet als onderdeel van de verplichte "passende maatregelen" [7]. Boetes: tot EUR 10 miljoen of 2% van jaaromzet.

PCI DSS

Verplichte encryptie voor creditcardgegevens met specifieke key management-vereisten.

NEN 7510

Encryptie vereist voor medische en gezondheidsdata in de zorgsector.

8. Verschil: HSM vs Cloud KMS vs BYOK

OPTIE	WAT IS HET?	KOSTEN	GESCHIKT VOOR
Cloud KMS	Beheerde cloudservice (AWS, Azure, Google)	EUR 50--500/maand	Cloud-native MKB, lage complexiteit
Dedicated Cloud HSM	Hardware security module als cloudservice	Vanaf EUR 3.000/ maand	Hoge compliance-eisen, financieel
On-premise HSM	Fysiek HSM-apparaat in eigen datacenter	EUR 10.000--50.000 aanschaf	Overheid, defensie, maximale controle
BYOK	Eigen sleutels in cloud-omgeving	Afhankelijk van KMS + tooling	Data-soevereiniteit, compliance

9. Trends 2025--2026

Post-Quantum Cryptografie (PQC)

60% van organisaties evalueert PQC-oplossingen [2]. NIST publiceerde in 2024 de eerste post-quantum standaarden (FIPS 203, 204, 205). De "harvest now, decrypt later"-dreiging maakt vroege migratie belangrijk: 58% van organisaties noemt dit als zorg [2].

Encryption as a Service

Cloud-based encryptie en key management maakt enterprise-grade beveiliging toegankelijk voor MKB. Pay-per-use modellen verlagen de instapdrempel.

Data Soevereiniteit

Europese regelgeving drijft vraag naar lokale key management en BYOK. Organisaties willen zekerheid dat sleutels binnen de EU worden opgeslagen en beheerd.

10. Aan de slag

DRIE DIRECTE ACTIES

1. Inventariseer welke gevoelige data nog niet versleuteld is
2. Controleer je huidige key management: wie heeft toegang tot sleutels? Worden ze geroteerd?
3. Plan een encryptie-assessment om je specifieke risico's en prioriteiten te identificeren

Hulp nodig? Op ibgids.nl/word-gematcht word je vrijblijvend gematcht met encryptie en key management specialisten die passen bij jouw situatie.

Bronnenlijst

[1] **CBS Cybersecuritymonitor 2024** -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[2] **Thales Data Threat Report 2025** -- thalesgroup.com/en/press_release/2025-thales-data-threat-report-reveals-nearly-70-organizations-identify-ais-fast

[3] **IBM Cost of Data Breach Report 2025** -- ibm.com/reports/data-breach

[4] **Business Research Company Key Management Market** -- thebusinessresearchcompany.com/report/key-management-as-a-service-global-market-report

[5] **AVG/GDPR Netherlands** -- gdprregulation.eu/gdpr-in-netherlands/

[6] **NIST SP 800-57 Key Management** -- csrc.nist.gov/projects/key-management/key-management-guidelines

[7] **NCSC Cyberbeveiligingswet (NIS2)** -- ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[8] **Digital Trust Center - Encryptie** -- digitaltrustcenter.nl/informatie-advies/wat-is-encryptie

[9] **Fortanix HSM vs KMS** -- fortanix.com/blog/cloud-hsm-vs-kms-which-is-right-for-your-enterprise-data-security-strategy

[10] **Google Cloud KMS Pricing** -- cloud.google.com/kms/pricing

[11] **Kiteworks Key Rotation Best Practices** -- kiteworks.com/regulatory-compliance/encryption-key-rotation-strategies/

[12] **MKB Eindhoven Data Encryptie** -- mkbgroeit.nl/belang-data-encryptie-gegevens-versleuteling/

[13] **CBS Cybersecuritymaatregelen** -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024/2-cybersecuritymaatregelen-door-bedrijven

[14] **NTNT Cybersecurity Kosten MKB** -- ntnt.nl/wat-kost-goede-cybersecurity-voor-een-mkb/

[15] **Thales 2025 Cloud Security Study** -- cpl.thalesgroup.com/about-us/newsroom/thales-2025-cloud-security-study-reveals-ai-tool-sprawl-security-gap