GIDS

De complete gids voor privacy & data protection (DPIA/ PbD)

DPIA, Privacy by Design, verwerkingsregister, DPO en AVG-compliance.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Privacy is geen formaliteit maar een bedrijfsrisico.

EUR 1,2 mld
AVG-boetes in Europa in 2024
DLA Piper [1]

33.471
dataleknotificaties in Nederland -- top 3 Europa
DLA Piper [1]

EUR 290M
AP-boete voor Uber (doorgifte data naar VS)
AP [2]

EUR 20M
maximale AVG-boete of 4% mondiale jaaromzet
AVG [3]

82%
van consumenten wil meer controle over persoonsgegevens
Diverse [4]

2.245
AVG-boetes in Europa sinds GDPR, totaal EUR 5,65 mld
CMS [5]

34,2%
CAGR groei MKB Privacy as a Service tot 2030
Fortune BI [6]

9 criteria
van EU om DPIA-verplichting te beoordelen
AP [7]

1. Wat is privacy & data protection?

Privacy & data protection omvat de bescherming van persoonsgegevens en het voldoen aan privacywetgeving -- van DPIA tot verwerkingsregister en DPO.

Drie pijlers: juridische compliance (AVG, AI Act), technische implementatie (encryptie, pseudonimisering) en organisatorische maatregelen (beleid, training, governance). Een DPIA beoordeelt privacy-risico's voordat je een nieuwe verwerking start [7].

2. Waarom is het belangrijk?

EUR 1,2 miljard aan boetes in 2024. Nederland top 3 dataleknotificaties. Privacy-compliance is geen optie.

De AP legde boetes op van EUR 290M (Uber) en EUR 3,7M (Belastingdienst) [2]. MKB vergeet vaak verwerkingsregister, DPIA en datalekprocedure [8]. Handhaving breidt uit naar finance en energie [1].

3. Het compliance-proces

1 Privacy scan en gap analyse

WEEK 1--2

Beoordeel AVG-compliance: verwerkingsregister, beleid, verwerkersovereenkomsten, datalekprocedure.

2 Verwerkingsregister

WEEK 2--4

Documenteer alle verwerkingen: welke data, doel, grondslag, bewaartermijn, delen met wie.

3 DPIA's uitvoeren

WEEK 3--6

DPIA's voor hoog-risico verwerkingen. AP heeft verplichte lijst gepubliceerd [7].

4 Beleid implementeren

WEEK 4--8

Privacybeleid, datalekprocedure, verwerkersovereenkomsten, rechten betrokkenen.

5 DPO en doorlopend beheer

DOORLOPEND

Stel (externe) DPO aan indien verplicht. Review register bij wijzigingen. DPIA bij nieuwe verwerkingen.

4. Wat kost het?

TIER	WAT JE KRIJGT	PRIJSINDICATIE
Basis	Privacy scan + verwerkingsregister + datalekprocedure	EUR 2.500--7.500 eenmalig
Standaard	Basis + DPIA's + externe DPO + jaarlijkse review	EUR 8.000--20.000/jaar
Premium	Volledig managed: DPO-as-a-Service, training, audits	EUR 20.000--50.000/jaar

> **DPO kosten:** Intern EUR 4.000-7.000/maand [9]. Extern (DPO-as-a-Service): EUR 500-2.500/maand -- vaak kosteneffectiever voor MKB.

5. Selectiecriteria

- **Nederlandse AVG-kennis** -- AP-richtlijnen, DPIA-verplichtingenlijst
- **DPIA-ervaring in jouw sector** -- Zorg, HR, finance, marketing
- **Juridisch en technisch** -- Privacy is beide
- **DPO-onafhankelijkheid** -- Geen belangenconflicten
- **EU AI Act kennis** -- Nieuwe DPIA-verplichtingen

6. Veelgemaakte fouten

1. Register niet bijhouden

Eenmalig document dat veroudert is nutteloos. Update bij elke wijziging.

2. DPIA alleen als het moet

Privacy by Design vereist vroege beoordeling, niet achteraf.

3. Datalekprocedure niet oefenen

72-uur AP-melding vereist voorbereiding.

4. Privacy als juridisch probleem

Het is ook technisch en organisatorisch.

7. AVG, NIS2 en AI Act

AVG: Register, DPIA, datalekprocedure, verwerkersovereenkomsten. Boetes tot EUR 20M of 4% [3].

NIS2: Privacy als onderdeel van cybersecurity. Meldplicht bij incidenten met persoonsgegevens.

AI Act: DPIA verplicht voor high-risk AI. Privacy impact vooraf beoordelen.

8. Verschil met verwante oplossingen

KENMERK	PRIVACY & DP	INFOSEC	DPO/FG
Focus	Persoonsgegevens	Alle data	Toezichtsrol
Scope	AVG, AI Act	ISO 27001, NIS2	Advies en toezicht
Relatie	Specifiek	Breder	Onderdeel governance

9. Trends 2025--2026

1. EU AI Act en privacy

DPIA's voor high-risk AI-systemen.

2. Privacy engineering

PETs: differential privacy, federated learning.

3. Geautomatiseerde DPIA tools

AI-ondersteunde privacy impact assessments.

10. Aan de slag

Heb je een verwerkingsregister, en is het actueel? Begin daar. Het register is de basis voor alle andere privacy-maatregelen.

Bronnenlijst

[1] **DLA Piper** -- GDPR Fines 2025. dlapiper.com/en/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025

[2] **AP** -- Boetes. autoriteitpersoonsgegevens.nl/boetes-en-andere-sancties

[3] **Privacy Zeker** -- AVG boetes. privacyzeker.nl/avg-privacy-kennisbank/wat-zijn-de-boetes-bij-een-overtreding-van-de-avg/

[4] **Diverse** -- Consumer preferences

[5] **CMS** -- Enforcement Tracker. cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures

[6] **Fortune BI** -- Data Privacy Software. fortunebusinessinsights.com/data-privacy-software-market-105420

[7] **AP** -- DPIA. autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia

[8] **Law & More** -- AVG MKB. lawandmore.nl/nieuws/verwerkingsregister-dpia-en-datalek-welke-avg-verplichtingen-vergeten-mkb-bedrijven-vaak/

[9] **Nationale Beroepengids** -- DPO. nationaleberoepengids.nl/data-protection-officer

[10] **ICTrecht** -- DPIA verplichting. ictrecht.nl/blog/wanneer-is-een-dpia-verplicht-volgens-de-autoriteit-persoonsgegevens

[11] **AP** -- Lijst verplichte DPIA. autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia

[12] **Business Research Insights** -- Privacy as a Service. businessresearchinsights.com/market-reports/privacy-as-a-service-market-117339

[13] **Statista** -- GDPR fines. statista.com/statistics/1172494/gdpr-fines-by-type-violation/

[14] **Digitale Overheid** -- Cbw. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[15] **Alation** -- DPIA Guide. alation.com/blog/data-protection-impact-assessment-dpia-2025-guide/