VOORBEELD-DPIA: gegevensbeschermingseffectbeoordeling

Werkdocument voor [naam organisatie]

> **Disclaimer.** Dit is een voorbeelddocument en werkinstrument, geen juridisch advies. Het invullen van dit model garandeert niet dat je aan de AVG voldoet. Elke verwerking is anders: pas het document aan op jouw situatie. Blijkt uit de beoordeling dat er een hoog restrisico is dat je niet met maatregelen kunt beperken, dan ben je verplicht de Autoriteit Persoonsgegevens (AP) vooraf te raadplegen (art. 36 AVG). Twijfel je over de uitkomst of de aanpak, schakel dan een privacyjurist of functionaris gegevensbescherming (FG) in.

Wanneer is een DPIA verplicht?

Een DPIA (Data Protection Impact Assessment, in het Nederlands: gegevensbeschermingseffectbeoordeling) is verplicht als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen (art. 35 AVG). Dat is in elk geval zo bij:

1. Verwerkingen die op de **AP-lijst van verwerkingen** staan waarvoor een DPIA verplicht is. Denk aan: heimelijk onderzoek, zwarte lijsten, fraudebestrijding, cameratoezicht, controle van medewerkers, grootschalige verwerking van gezondheidsgegevens, locatiegegevens, financiele situatie, en profilering. Raadpleeg de actuele lijst op autoriteitpersoonsgegevens.nl.

2. Verwerkingen die voldoen aan **twee of meer criteria uit de EDPB-richtsnoeren (WP248)**: evaluatie of scoring, geautomatiseerde besluitvorming met rechtsgevolg, stelselmatige monitoring, gevoelige gegevens, grootschalige verwerking, koppelen van datasets, kwetsbare betrokkenen (zoals kinderen, patienten, werknemers), innovatieve technologie, of het blokkeren van een recht, dienst of contract.

Twijfel je? Voer de DPIA dan toch uit. Het proces zelf helpt je risico's te zien en maatregelen te kiezen, en je toont aan dat je je verantwoordingsplicht serieus neemt.

0. Documentgegevens

Onderdeel	Invullen
Naam verwerking	[naam verwerking, bijv. "cameratoezicht bedrijfspand"]
Organisatie (verwerkingsverantwoordelijke)	[naam organisatie], KvK [nummer]
Opsteller	[naam, functie]
Betrokken afdelingen/personen	[bijv. directie, HR, ICT-leverancier]
Versie en datum	[versienummer], [datum]

Status	[concept / vastgesteld]

1. Systematische beschrijving van de verwerking

Beschrijf de verwerking zo concreet dat een buitenstaander begrijpt wat er gebeurt.

1.1 Aard van de verwerking

[Beschrijf wat je doet: welke gegevens verzamel je, hoe verzamel je ze, wat gebeurt ermee, waar worden ze opgeslagen en wanneer worden ze verwijderd.]

1.2 Categorieen betrokkenen

[Bijv. klanten, medewerkers, websitebezoekers, sollicitanten. Vermeld of er kwetsbare groepen bij zitten, zoals kinderen of patienten.]

1.3 Categorieen persoonsgegevens

[Bijv. NAW-gegevens, e-mailadres, camerabeelden, IP-adres, personeelsdossier. Benoem apart of je bijzondere persoonsgegevens (gezondheid, geloof, biometrie), strafrechtelijke gegevens of het BSN verwerkt.]

1.4 Verwerkingsprocessen en systemen

[Welke software, apparatuur en leveranciers gebruik je? Wie heeft toegang? Zijn er verwerkers (bijv. hostingpartij, salarisverwerker)? Is er een verwerkersovereenkomst?]

1.5 Bewaartermijnen

[Per gegevenscategorie: hoe lang bewaar je de gegevens en waarom die termijn?]

1.6 Doorgifte buiten de EER

[Worden gegevens buiten de Europese Economische Ruimte verwerkt, bijv. via een Amerikaanse clouddienst? Zo ja, op welke grondslag (adequaatheidsbesluit, standaardcontractbepalingen)?]

2. Doeleinden en belangen

2.1 Doeleinden van de verwerking

[Beschrijf per doel waarom je de gegevens verwerkt. Wees specifiek: "beveiliging van pand en personeel tegen diefstal" in plaats van "veiligheid".]

2.2 Rechtsgrondslag (art. 6 AVG)

[Kies per doel: toestemming, uitvoering overeenkomst, wettelijke plicht, vitaal belang, taak van algemeen belang, of gerechtvaardigd belang. Bij gerechtvaardigd belang: beschrijf de belangenafweging.]

2.3 Belangen van de organisatie en van derden

[Welk belang heeft [naam organisatie] bij deze verwerking? Zijn er belangen van derden, zoals klanten of de maatschappij?]

3. Noodzaak en evenredigheid

Beoordeel of de verwerking noodzakelijk is voor het doel en of het doel opweegt tegen de inbreuk op de privacy.

3.1 Noodzaak. [Kun je het doel bereiken zonder deze gegevens, met minder gegevens, of op een minder ingrijpende manier? Beschrijf welke alternatieven je hebt overwogen en waarom die afvallen.]

3.2 Proportionaliteit. [Staat de inbreuk op de privacy in verhouding tot het doel? Onderbouw dit.]

3.3 Subsidiariteit. [Is dit het minst ingrijpende middel dat het doel bereikt?]

3.4 Dataminimalisatie. [Welke gegevens verzamel je bewust niet? Welke velden, beelden of logbestanden heb je beperkt?]

4. Rechten van betrokkenen

Beschrijf hoe je de rechten van betrokkenen borgt en hoe je hen informeert.

Recht	Hoe geborgd bij [naam organisatie]
Informatie (privacyverklaring)	[bijv. privacyverklaring op website, bordjes bij camera's, personeelsreglement]
Inzage	[procedure en reactietermijn, max. 1 maand]
Rectificatie en verwijdering	[procedure]
Beperking en bezwaar	[procedure]
Dataportabiliteit	[indien van toepassing]
Klachtrecht bij de AP	[vermeld in privacyverklaring]

[Beschrijf ook: is er sprake van geautomatiseerde besluitvorming? Zo ja, hoe kan een betrokkene menselijke tussenkomst vragen?]

5. Risico-inschatting

Benoem per risico de kans en de impact voor de **betrokkene** (niet voor de organisatie). Gebruik een schaal van 1 (laag) tot 3 (hoog). Risicoscore = kans x impact. Score 1-2 is laag, 3-4 is middel, 6-9 is hoog.

Nr	Risico voor betrokkene	Kans (1-3)	Impact (1-3)	Score	Toelichting
1	[bijv. onbevoegde toegang tot gegevens door datalek]	[ ]	[ ]	[ ]	[waarom deze inschatting]
2	[bijv. gegevens langer bewaard dan nodig]	[ ]	[ ]	[ ]	[ ]

3	[bijv. functiecreep: beelden gebruikt voor ander doel, zoals prestatiecontrole]	[ ]	[ ]	[ ]	[ ]
4	[bijv. onjuiste gegevens leiden tot verkeerd besluit over betrokkene]	[ ]	[ ]	[ ]	[ ]
5	[bijv. doorgifte aan derde land zonder passende waarborgen]	[ ]	[ ]	[ ]	[ ]

Denk bij impact aan: identiteitsfraude, financiele schade, reputatieschade, discriminatie, stress of gevoel van voortdurende observatie, verlies van controle over eigen gegevens.

6. Voorgenomen maatregelen

Koppel elke maatregel aan een risico uit hoofdstuk 5 en geef het restrisico na de maatregel.

Nr risico	Maatregel	Type	Verantwoordelijke	Deadline	Restrisico
1	[bijv. versleuteling, tweefactorauthenticatie, toegangsbeperking op need-to-know basis]	technisch	[naam]	[datum]	[laag/middel/hoog]
2	[bijv. automatische verwijdering na X dagen]	technisch	[naam]	[datum]	[ ]
3	[bijv. schriftelijk vastgelegd doel, instructie medewerkers, periodieke controle]	organisatorisch	[naam]	[datum]	[ ]
4	[bijv. controleprocedure op juistheid, menselijke beoordeling van besluiten]	organisatorisch	[naam]	[datum]	[ ]
5	[bijv. EU-leverancier kiezen of standaardcontractbepalingen plus aanvullende maatregelen]	contractueel	[naam]	[datum]	[ ]

Conclusie restrisico: [Beschrijf of het totale restrisico aanvaardbaar is. Blijft er een hoog restrisico over dat je niet verder kunt beperken? Dan moet je de AP vooraf raadplegen voordat je met de verwerking start.]

7. Raadpleging FG en betrokkenen

7.1 Functionaris gegevensbescherming.

[Heeft [naam organisatie] een FG? Zo ja: vraag de FG om advies en neem het advies hier op. Wijk je af van het advies, motiveer dat. Geen FG? Vermeld dat en overweeg bij hoog-risicoverwerkingen extern advies.]

- Advies FG/adviseur: [samenvatting advies, datum]
- Reactie organisatie: [overgenomen / afgeweken, met motivering]

7.2 Betrokkenen of hun vertegenwoordigers.

De AVG vraagt om waar passend de mening van betrokkenen te vragen. [Beschrijf hoe je dat hebt gedaan: bijv. overleg met de personeelsvertegenwoordiging of OR, een klantenpanel, of een korte enquete. Heb je betrokkenen niet geraadpleegd, leg dan uit waarom niet.]

Let op: bij controle of monitoring van personeel heeft de ondernemingsraad vaak instemmingsrecht (art. 27 WOR).

8. Vaststelling en ondertekening

Met ondertekening stelt de verwerkingsverantwoordelijke deze DPIA vast en aanvaardt het beschreven restrisico.

Naam	**[naam tekenbevoegde]**
Functie	[bijv. directeur/eigenaar]
Datum	[datum]
Handtekening	.....

Herziening. Een DPIA is geen eenmalige exercitie. Herzie dit document in elk geval:

- op de vaste herzieningsdatum: **[datum, uiterlijk 3 jaar na vaststelling; bij hoog-risicoverwerkingen jaarlijks]**;
- bij wijziging van de verwerking (nieuw systeem, nieuwe leverancier, nieuw doel, nieuwe gegevenscategorieen);
- na een datalek of incident dat met deze verwerking samenhangt;
- bij relevante nieuwe wetgeving of richtsnoeren van de AP of EDPB.

Volgende geplande herziening: [datum]. Verantwoordelijk voor herziening: [naam, functie].

Bewaar deze DPIA samen met je verwerkingsregister (art. 30 AVG). Je hoeft de DPIA niet naar de AP te sturen, maar je moet haar wel kunnen tonen als de AP erom vraagt.
