PROFLEXIS

Wat zit er in de gegevensbeschermingsbeoordeling?

Dit is wat in de wandelgangen de DPIA heet.

De beoordeling van het effect op de bescherming van persoonsgegevens.

Algemene verordening gegevensbescherming (AVG), artikel 35. De vier onderdelen in het midden zijn wat de wet woordelijk eist; de rest is wat eromheen hoort.

EERST VASTSTELLEN OF U HEM MOET MAKEN

0 — Moet u dit überhaupt doen? — artikel 35, lid 1, 3 en 4

Verplicht als uw verwerking waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van mensen. De wet noemt drie gevallen met name: een systematische en uitgebreide geautomatiseerde beoordeling van mensen waarop besluiten met rechtsgevolg worden gebaseerd (waaronder profilering); grootschalige verwerking van bijzondere of strafrechtelijke gegevens; en stelselmatige grootschalige monitoring van openbaar toegankelijke ruimten. Daarnaast heeft de Autoriteit Persoonsgegevens een eigen lijst met verplichte gevallen. Twijfelt u? Maak hem dan, en leg vast waarom.

DE VIER ONDERDELEN DIE DE WET VERPLICHT STELT

1 — Wat u gaat doen, en waarom — artikel 35, lid 7, onder a

Een systematische beschrijving van de verwerkingen en van het doel ervan. Welke gegevens, van wie, waar vandaan, hoe lang, wie erbij kan. Beroept u zich op een gerechtvaardigd belang, dan hoort dat belang hier ook benoemd te worden.

2 — Is het nodig, en staat het in verhouding — artikel 35, lid 7, onder b

Noodzaak en evenredigheid. Kan het doel ook worden bereikt met minder gegevens, of met gegevens die minder gevoelig liggen? Dit is het hoofdstuk dat het vaakst wordt overgeslagen en het vaakst het verschil maakt.

3 — Welk risico levert dit op voor de mensen om wie het gaat — artikel 35, lid 7, onder c

Niet het risico voor uw organisatie — het risico voor de betrokkenen. Wat merken zij ervan als de gegevens uitlekken, onjuist zijn, of voor iets anders worden gebruikt dan waarvoor ze zijn verzameld?

4 — Wat u eraan doet — artikel 35, lid 7, onder d

De maatregelen om die risico's aan te pakken: waarborgen, beveiliging, en mechanismen waarmee u kunt áántonen dat u aan de AVG voldoet. Dat laatste woord staat er met opzet: het is niet genoeg dat het goed is geregeld, u moet het ook kunnen laten zien.

WAT ER OM DIE VIER HEEN HOORT

5 — Advies van uw functionaris gegevensbescherming — artikel 35, lid 2

Hebt u een functionaris gegevensbescherming aangesteld, dan moet u zijn advies inwinnen. Hebt u er geen — en voor veel organisaties is dat niet verplicht — dan vervalt deze stap, maar schrijf dat dan wel op.

6 — De mening van de mensen om wie het gaat — artikel 35, lid 9

In voorkomend geval vraagt u betrokkenen of hun vertegenwoordigers naar hun mening over wat u van plan bent. Bij medewerkers is dat vaak de ondernemingsraad. Dit wordt bijna altijd vergeten en is bij een controle makkelijk te missen.

7 — Gedragscodes meewegen — artikel 35, lid 8

Bestaat er voor uw sector een goedgekeurde gedragscode, dan telt mee of u zich daaraan houdt. Dat kan uw beoordeling korter maken, want u kunt ernaar verwijzen in plaats van alles opnieuw uit te schrijven.

8 — Toetsen of het nog klopt — artikel 35, lid 11

Verandert het risico, dan gaat u na of de verwerking nog overeenkomt met wat u hebt opgeschreven. Geen vaste termijn, wel een verplichting zodra er iets wezenlijks wijzigt.

9 — Blijft er een hoog risico over? Dan eerst naar de toezichthouder — artikel 36

Kunt u een hoog risico niet wegnemen met maatregelen, dan raadpleegt u de Autoriteit Persoonsgegevens vóórdat u begint. Dit is de enige situatie waarin deze beoordeling de deur uit gaat — verder houdt u hem zelf.

Twee beoordelingen, één dossier

Gebruikt u een hoog-risico AI-systeem dat persoonsgegevens verwerkt, dan hebt u deze beoordeling én de grondrechtenbeoordeling nodig. Ze overlappen, maar ze zijn niet hetzelfde: deze gaat over gegevens, die andere over mensen. Sinds juli 2026 mag u in de grondrechtenbeoordeling kruisverwijzen naar de betreffende delen van deze beoordeling. Wie zijn AVG-huiswerk heeft gedaan, hoeft dat dus niet over te doen.