

Wet Bescherming Persoonsgegevens belangrijke fragmenten

Onderstaand vind je enkele belangrijke fragmenten uit de WBP; merk dus op dat het om fragmenten gaat en dat dus niet alle genoemde artikelen volledig zijn afgedrukt.

Art. 1

a.persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

b.verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

d.verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

e.bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

f.betrokkene: degene op wie een persoonsgegeven betrekking heeft;

Art. 8

Persoonsgegevens mogen slechts worden verwerkt indien:

a.de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

b.de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;

c.de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;

d.de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;

e.de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of

f.de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Art. 9

1. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

2. Bij de beoordeling of een verwerking onverenigbaar is als bedoeld in het eerste lid, houdt de verantwoordelijke in elk geval rekening met:

a.de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;

b.de aard van de betreffende gegevens;

c.de gevolgen van de beoogde verwerking voor de betrokkene;

d.de wijze waarop de gegevens zijn verkregen en

e.de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Artikel 10

1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

Artikel 13

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich

meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 16

De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Artikel 24

1. Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

Artikel 27

1. Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt alvorens met de verwerking wordt aangevangen gemeld bij het College of de functionaris.

Memorie van toelichting –belangrijke fragmenten

Ad WBP Art. 1 onderdeel d

“Het begrip «verantwoordelijke» knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. De richtlijn gaat ervan uit dat deze bevoegdheden in de regel in dezelfde hand liggen. Is dit niet het geval, dan is er sprake van gezamenlijke verantwoordelijkheid.”

...

“Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds –in aanvulling daarop – van een functionele inhoud van het begrip. Het laatste criterium speelt met name een rol als er verschillende actoren bij de gegevensverwerking betrokken zijn en de juridische bevoegdheid onvoldoende helder is geregeld om te kunnen bepalen wie van de betrokken actoren als verantwoordelijke in de zin van de wet moet worden aangemerkt.”

Ad WBP Art. 8 onderdeel f

“De vraag rijst op welke wijze van de daarin gegeven interpretatieruimte gebruik moet worden gemaakt. In de eerste plaats vereist onderdeel f dat er sprake is van een gerechtvaardigd belang van de verantwoordelijke of van een derde. Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking voor laatstgenoemde noodzakelijk is om zijn reguliere bedrijfsactiviteiten te kunnen verrichten. De verantwoordelijke kan zijn beroep of bedrijf niet goed uitoefenen indien hem de mogelijkheid zou worden ontzegd de met het oog daarop noodzakelijke gegevens te verwerken.”

Vrijstellingsbesluit WBP –belangrijke fragmenten

Art. 33

1. Artikel 27 van de wet is niet van toepassing op verwerkingen die uitsluitend zijn gericht op het onderhoud, het beheer, de beveiliging, het gebruik en de goede werking van computersystemen of computerprogramma's binnen de organisatie van de verantwoordelijke, voor zover deze verwerkingen voldoen aan de in dit artikel vermelde eisen.

2. De verwerking geschiedt slechts voor:

- a. de controle op en de beveiliging van de computersystemen of computerprogramma's;
- b. de ondersteuning van de goede werking van de computersystemen of computerprogramma's;
- c. het sorteren en herstellen van (tussen)bestanden;
- d. het aanmaken van reservekopieën van (tussen)bestanden;
- e. het beheer van de systemen of programma's.

3. Geen andere persoonsgegevens worden verwerkt dan:

- a. gegevens met betrekking tot het gebruik van de programmatuur;

- b. technische en besturingsgegevens;
- c. gegevens ter bevordering van een goede werking;
- d. historische gegevens;
- e. gebruikersgegevens.

Achtergrondstudies & Verkenningen nr. 23 –belangrijke fragmenten

“De verantwoordelijke komt tot een afweging in welke risicoklasse de gegevens vallen. In alle gevallen moet de verantwoordelijke op grond van een grondige analyse kiezen voor een bepaalde risicoklasse en het daarbij behorende beveiligingsniveau. Deze analyse moet toetsbaar zijn en hierover moet verantwoording kunnen worden afgelegd. “

3.3 Risicoklassen (blz. 26 e.v.)

*Risicoklasse 0 publiek niveau;

“Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene.”

*Risicoklasse I basis niveau;

“De risico’s voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.”

*Risicoklasse II verhoogd risico;

“De uitkomst van de analyse toont aan dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens.” ...

“ In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkene);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.”

*Risicoklasse III hoog risico.

“Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren dat het gerechtvaardigd is deze verwerking van persoonsgegevens in risicoklasse III te plaatsen.” ... “De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt.” ... “Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse.”

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	Aard van de verwerking		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Veel persoonsgegevens	Hoge complexiteit van verwerking	Risicoklasse I	Risicoklasse III	

4.6 Beheer en classificatie van de ICT infrastructuur (blz. 42)

Risicoklasse II

“Voor het testen van informatiesystemen met persoonsgegevens mogen uitsluitend gegevens van fictieve personen gebruikt worden.”

4.14 Uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens (blz. 52)

“In een aantal gevallen zal een organisatie niet alle verwerkingen van persoonsgegevens zelf uitvoeren maar geheel of gedeeltelijk uitbesteden aan een bewerker (artikel 14 WBP). Voor de beveiliging van persoonsgegevens geldt dat de bewerker hetzelfde niveau van beveiliging moet garanderen als de verantwoordelijke organisatie. In de contracten met bewerkers moet de beveiliging van de persoonsgegevens opgenomen worden. Ook is het wenselijk dat de bewerker een geheimhoudingsverklaring tekent. Wanneer de bewerker persoonsgegevens uit de hoogste risicoklasse verwerkt, zal er toezicht moeten worden gehouden op de beveiligingsmaatregelen die deze neemt, bijvoorbeeld in de vorm van periodieke controles.

Risicoklasse I

In het kader van de controle van de verantwoordelijke op de bewerker kan deze gebruikmaken van een Third Party Mededeling. Dit is een onafhankelijk oordeel over de kwaliteit van de door de bewerker getroffen maatregelen van de beveiliging van persoonsgegevens.

In een contract tussen de verantwoordelijke en de bewerker wordt vastgelegd dat beide zich aan de, op de risicoklasse betrekking hebbende, eisen zullen houden. Hierbij wordt onder meer het volgende vastgelegd:

- procedures rond autorisaties;
- het bijhouden van logbestanden;
- de opslag van gegevensdragers met persoonsgegevens;
- het verstrekken van persoonsgegevens aan derden.

Het fysieke en logische beveiligingsniveau bij de bewerker moet toereikend zijn voor de risicoklasse van de te verwerken persoonsgegevens.

De verantwoordelijke dient zich op de hoogte te stellen van het beveiligingsniveau voor de persoonsgegevens bij de bewerker. De verantwoordelijke moet een geheimhoudingsartikel in het contract opnemen.

Risicoklasse II

De verantwoordelijke moet het niveau van het beleid voor de beveiliging van persoonsgegevens bij de bewerker (laten) controleren. De controle en rapportage geschieden jaarlijks. De verantwoordelijke voert hierop steekproefsgewijs een controle bij de bewerker uit.

Risicoklasse III

Persoonsgegevens worden alleen opgeslagen of bewerkt door een bewerker indien de verantwoordelijke zich er, middels een overeenkomst en afspraken over controle, van heeft verzekerd dat vereiste beveiligingsmaatregelen zijn getroffen.”