

Toelichting Verwerkingsovereenkomst AVG

Door de KNB is een [voorbeeld \(docx\)](#) ter beschikking gesteld van een verwerkingsovereenkomst die notariskantoren kunnen afsluiten met leveranciers. Deze overeenkomst kan ook worden gebruikt om overeenkomsten die door andere partijen zijn opgesteld mee te toetsen.

Wat is een verwerkingsovereenkomst?

Een verwerkingsovereenkomst is een overeenkomst waarin met een derde, de verwerker, afspraken worden gemaakt over de verwerking van persoonsgegevens.

Op een notariskantoor worden verschillende persoonsgegevens verwerkt, met name gegevens van cliënten en van het personeel. Voor deze gegevens is de notaris meestal de *verwerkingsverantwoordelijke*. Dat betekent dat de notaris de verantwoordelijkheid heeft ervoor te zorgen dat de regels voor correcte verwerking van persoonsgegevens worden nageleefd.

De notaris verwerkt niet alle gegevens zelf: meestal wordt gebruik gemaakt van andere dienstverleners, zogenaamde *verwerkers*. Ook als de notaris anderen inschakelt bij de verwerking van persoonsgegevens blijft hij verantwoordelijk. De notaris is onder de Algemene Verordening Gegevensbescherming (AVG) verplicht schriftelijk afspraken met zijn verwerkers te maken. Dat gebeurt in een zogenaamde *verwerkingsovereenkomst*. Deze afspraken moeten er onder andere voor zorgen dat de gegevens goed beveiligd zijn en dat de notaris zijn wettelijke verplichtingen kan nakomen.

Waar moet een verwerkingsovereenkomst aan voldoen?

De belangrijkste eisen aan de verwerkingsovereenkomst staan opgesomd in artikel 28 AVG. Deze zijn verwerkt in de voorbeeldovereenkomst.

Met wie moet een verwerkingsovereenkomst worden afgesloten?

Een verwerkingsovereenkomst moet worden afgesloten met alle dienstverleners die voor de notaris persoonsgegevens verwerken en die niet onder direct gezag van de notaris staan. Met personeelsleden hoeft dus geen verwerkingsovereenkomst te worden afgesloten.

Voorbeelden van verwerkers

- Leveranciers van softwarepakketten die de bedrijfsvoering ondersteunen, tenzij zij geen toegang hebben tot persoonsgegevens, deze niet ontvangen/opslaan en ook niet op een andere manier verwerken.
- Aanbieders van cliënten- of werknemers portalen waarin gegevens worden verwerkt / uitgewisseld / opgeslagen.
- Externe salarisadministrateurs.
- Verhuurders van multifunctionals (printer/scanner) waarin op de harde schijf van het apparaat gegevens worden opgeslagen.
- Externe systeembeheerders.
- Aanbieders van opslagdiensten (clouddiensten, servers) die buiten het notariskantoor persoonsgegevens opslaan.

Tips voor een aanpak:

1. Inventariseer binnen uw organisatie welke externe verwerkers betrokken zijn bij de verwerking van persoonsgegevens. De belangrijkste staan waarschijnlijk al in uw verwerkingsregister
2. Breng in kaart wat deze verwerkers met de gegevens doen, waar de gegevens staan en wie toegang heeft tot de gegevens. Controleer of dat overeenstemt met de opdracht aan de verwerker.
3. Informeer bij de verwerkers of zij anderen inschakelen bij de verwerking van persoonsgegevens (zogenaamde subverwerkers), wie dit zijn en wat zij doen. De verwerker moet met de subverwerkers dezelfde afspraken maken om de verwerkingsovereenkomst met u na te kunnen komen.
4. Sluit met de verwerkers een verwerkingsovereenkomst af, die voldoet aan de AVG. Leg (in de overeenkomst zelf of in een bijlage) vast op welke verwerking de overeenkomst ziet:
 - het onderwerp en de duur van de verwerking;
 - aard en doel van de verwerking;
 - het soort persoonsgegevens dat wordt verwerkt;
 - de categorieën van personen van wie de gegevens zijn (bijvoorbeeld: cliënten, personeel).

Gebruik hiervoor het verwerkingsregister.

Maak praktische afspraken over wat er moet gebeuren bij een beveiligingsincident / datalek.