

CONTRACTUELE PRIVACYBEPALINGEN

In bepaalde gevallen hoeft geen verwerkersovereenkomst afgesloten te worden, bijvoorbeeld omdat de leverancier zelf ook Verwerkingsverantwoordelijke is of omdat de persoonsgegevens noodzakelijk zijn om juist andere producten/diensten aan te bieden waarvoor de overeenkomst wordt afgesloten.

In die gevallen wil de gemeente of Samenwerkingsorganisatie De Wolden Hoogeveen (SWO) als Opdrachtgever echter toch enkele bepalingen ten aanzien van de borging van privacy opgenomen hebben in de (hoofd)overeenkomst die met de Leverancier wordt gesloten. Een fout van de ene partij kan immers de andere partij ook schaden, zeker omdat het voor betrokkenen niet altijd duidelijk is wie de fout maakt.

PRIVACYBEPALINGEN

1. *Leverancier handelt niet als Verwerker in de zin van de Algemene Verordening Gegevensbescherming. Mogelijk worden wel persoonsgegevens verwerkt in de betreffende ICT Prestatie/-omgeving, maar dat is niet het hoofddoel van de verwerking.*
2. *Leverancier is verantwoordelijk voor een veilige, zorgvuldige en correcte omgang met betreffende persoonsgegevens. Hieronder valt onder andere het ontvangen, versturen, raadplegen, opslaan en muteren van gegevens.*
3. *Leverancier voldoet hierbij aan het volgende normenstelsel:*
 - Algemene Verordening Gegevensbescherming (AVG en UAVG)
 - NEN/ISO 27001
 - PCI/DSS: *bij uitwisseling persoonsgegevens bij kaart- en transactiegegevens*
 - NTA7516: *bij uitwisseling persoonsgegevens binnen het zorgdomein**Leverancier stelt Opdrachtgever in staat te voldoen aan de normen, zoals gesteld in de Baseline Informatiebeveiliging Nederlandse Overheid (BIO).
De toereikendheid van de informatieveiligheid blijkt uit:*
 - Certificering *óf*
 - Periodieke externe controles zoals audits of TPM's *óf*
 - Een Assurance rapport van een gecertificeerd auditor *óf*
 - Eigen controles of eigen mededelingen
4. *Leverancier heeft een eigen protocol over hoe om te gaan met privacy.*
5. *De persoonsgegevens mogen door Leverancier uitsluitend gebruikt worden voor **het leveren van trapliften** bij betrokkene. Daarbij worden alleen de noodzakelijke persoonsgegevens gebruikt (proportionaliteit).*
6. *Direct na beëindiging van de hoofdovereenkomst/opdracht worden de betreffende persoonsgegevens bij Leverancier vernietigd, tenzij vanuit wettelijke bepalingen een langere bewaartermijn vereist is.*
7. *Waar mogelijk worden persoonsgegevens gepseudonimiseerd of geanonimiseerd.*
8. *Persoonsgegevens tussen Opdrachtgever en Leverancier worden alleen beveiligd verzonden.*
9. *Personen in dienst van, dan wel werkzaam ten behoeve van de Leverancier, evenals de Leverancier zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, ook na beëindiging van de hoofdovereenkomst, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht.*
10. *Leverancier informeert Opdrachtgever bij een datalek, als dat kan leiden tot schending van privacy van betrokkenen. Leverancier meldt een dergelijk datalek zelf bij de Autoriteit Persoonsgegevens. Indien zich bij Opdrachtgever een datalek voordoet dat gevolgen kan hebben voor Leverancier, dan wordt Leverancier hierover zo spoedig mogelijk geïnformeerd.*

11. *Leverancier dient mee te werken aan controles door Opdrachtgever op de informatieveiligheid en waarborging van de privacybescherming. De redelijke kosten van deze controle worden gedragen door Opdrachtgever, tenzij uit de controle blijkt dat Leverancier bovenstaande bepalingen niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de Leverancier. Opdrachtgever zal de controle slechts (laten) uitvoeren bij een ernstig vermoeden dat Leverancier bovenstaande bepaling niet of gebrekkig naleeft. De Opdrachtgever zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Leverancier.*
12. *Opdrachtgever erkent geen enkele aansprakelijkheid bij niet of niet volledig nakomen van bovenstaande verplichtingen door Leverancier, tenzij het niet (volledig) nakomen het gevolg is van een handelen of nalaten van Opdrachtgever.*

Voor toelichting of vragen, neem contact op:

Erik Poelman Privacy Officer
Jan Lemstra CISO