VERWERKERSOVEREENKOMST | WONINGCORPORATIE

Uitkomst van de toets

Uw organisatie | getoetst op 14-09-2026

CONCEPT De beoordeling loopt nog: 57 van 57 signaleringen staan open.

14 punten om te verbeteren.

0	14	0	15
Nu regelen	**Verbeteren**	**Goed om te weten**	**Niets gevonden**
Weegt zwaar, pak dit eerst op	Kan duidelijker of volledig	Kleiner punt, niet dringend	Bij deze vragen geen punt

Eerst doen

1. **Is precies opgesomd welke gegevens het zijn?**
   Laat de gegevens opsommen en gevoelige gegevens (zoals gezondheid of BSN) apart noemen of uitsluiten.
2. **Staat erin wat de organisatie zelf mag en moet?**
   Laat vastleggen wie namens de organisatie opdrachten geeft en via welk kanaal.
3. **Waarschuwt de leverancier als een opdracht in strijd is met de privacywet?**
   Laat vastleggen dat de leverancier dat meteen meldt en wat hij in de tussentijd doet.
4. **Houden medewerkers van de leverancier de gegevens geheim?**
   Laat een geheimhoudingsplicht voor alle medewerkers en ingehuurde mensen vastleggen.
5. **Beveiligt de leverancier de gegevens goed?**
   Laat de beveiligingsmaatregelen concreet opnemen in een bijlage.

CONCEPT

Per onderwerp

Waar de punten zitten. Groen betekent dat Datavoogd daar niets vond; dat is geen garantie dat alles klopt.

Waar gaat de samenwerking over	4 niets gevonden
Welke gegevens en van wie	1 verbeteren, 2 niets gevonden
Wie heeft de regie	2 verbeteren, 1 niets gevonden
Beveiliging en toegang	2 verbeteren, 2 niets gevonden
Als er iets misgaat	2 verbeteren, 2 niets gevonden
Andere bedrijven en buitenland	4 niets gevonden
Hulp bij vragen en onderzoeken	2 verbeteren
Bewaren en verwijderen	2 verbeteren
Up-to-date houden	3 verbeteren

Welke gegevens en van wie

Welke persoonsgegevens de leverancier gebruikt en over wie. Hoe preciezer, hoe beter u kunt zien of dat niet te veel is.

CONCEPT

VERBETEREN

Is precies opgesomd welke gegevens het zijn?

UITLEG

Datavoogd ziet dat Bijlage 1 de gegevens per veld opsomt (naam, adres, telefoonnummer, e-mailadres, omschrijving van het gebrek en door de bewoner zelf gemelde bijzonderheden) en dat BSN en bijzondere persoonsgegevens expliciet aan bod komen, met een toelichting op mogelijke gezondheidsinformatie.

OOK OPGEMERKT

- In Bijlage 2 is het hokje voor gewone persoonsgegevens (NAW, e-mail, telefoon) niet aangekruist, terwijl die gegevens volgens Bijlage 1 juist de kern van de verwerking vormen.
- De categorie 'door de bewoner zelf gemelde bijzonderheden' kan gezondheidsgegevens bevatten; Bijlage 1 duidt deze niet als art. 9-gegevens met bijbehorend regime.

→ **Laat de gegevens opsommen en gevoelige gegevens (zoals gezondheid of BSN) apart noemen of uitsluiten.**

AP2025-1.4 | AP aanbeveling 1 (maak afspraken zo concreet mogelijk), p. 6: soort persoonsgegevens

Wie heeft de regie

De organisatie bepaalt wat er met de gegevens gebeurt, niet de leverancier. Dat moet uit de afspraken blijken.

VERBETEREN

Staat erin wat de organisatie zelf mag en moet?

UITLEG

Datavoogd ziet dat de rechten en verplichtingen van de verantwoordelijke op hoofdlijnen zijn vastgelegd: instructierecht en zeggenschap (F033), auditrecht en keuze voor zelfevaluatie (F046, F049), bezwaar tegen subverwerkers (F037) en de eigen verantwoordelijkheid voor melden aan toezichthouder en betrokkenen (F062).

OOK OPGEMERKT

- Er is geen termijn of procedure afgesproken waarbinnen de verantwoordelijke de verwerker informeert over wijzigingen in de verwerking die gevolgen hebben voor Bijlage 1.

→ **Laat vastleggen wie namens de organisatie opdrachten geeft en via welk kanaal.**

ART28-03 | AVG art. 28 lid 3, aanhef: rechten en verplichtingen van de verwerkingsverantwoordelijke

VERBETEREN

Waarschuwt de leverancier als een opdracht in strijd is met de privacywet?

UITLEG

Datavoogd ziet dat artikel 4.6 een meldplicht bevat met de term "onmiddellijk", maar dat deze uitsluitend verwijst naar instructies "als bedoeld in artikel 4.4", het artikel over controle en audit.

OOK OPGEMERKT

- De verwijzing naar artikel 4.4 lijkt een verschrijving in het gebruikte sjabloon; verduidelijking dat de meldplicht op alle instructies ziet, ligt voor de hand.

→ **Laat vastleggen dat de leverancier dat meteen meldt en wat hij in de tussentijd doet.**

ART28-H2 | AVG art. 28 lid 3, slotzin: melden van een instructie die in strijd is met de AVG

Beveiliging en toegang

Hoe de gegevens beschermd zijn, wie erbij kan en hoe u dat kunt controleren.

VERBETEREN

Houden medewerkers van de leverancier de gegevens geheim?

UITLEG

Datavoogd ziet dat artikel 6 een geheimhoudingsbepaling bevat die zowel eigen personeel als ingeschakelde hulppersonen omvat en die is geborgd via een geheimhoudingsbeding in de (arbeids-)contracten. Artikel 2.4 regelt dat de geheimhoudingsplicht van Verwerker voortduurt na beëindiging van de Verwerkersovereenkomst.

OOK OPGEMERKT

- Bijlage 1 benoemt dat 6 planners en monteurs toegang hebben (F094); er is geen afspraak over een actueel overzicht of register van personen met toegang en hun geheimhoudingsverklaring.

→ **Laat een geheimhoudingsplicht voor alle medewerkers en ingehuurde mensen vastleggen.**

ART28-B | AVG art. 28 lid 3 onder b: vertrouwelijkheid van gemachtigde personen

VERBETEREN

Beveiligt de leverancier de gegevens goed?

UITLEG

Datavoogd ziet dat de overeenkomst een beveiligingsbepaling bevat (artikel 4.1-4.2) met een gevulde Bijlage 2 waarin concrete maatregelen staan: versleuteling, MFA, ISO 27001-certificering, gegevensscheiding en BIC 2.0 als kader.

OOK OPGEMERKT

- In Bijlage 2 zijn de aanvinkvakjes voor ISO 27001-certificering en MFA niet aangekruist, terwijl dezelfde maatregelen via 'Anders, namelijk' en de toelichting wél worden geclaimd.
- Bijlage 2 merkt de gegevens aan als categorie B met 'verhoogd risicoprofiel', wat zwaardere maatregelen veronderstelt dan de nu benoemde set.

→ **Laat de beveiligingsmaatregelen concreet opnemen in een bijlage.**

ART28-C | AVG art. 28 lid 3 onder c, in samenhang met art. 32: beveiliging van de verwerking

Als er iets misgaat

Bij een datalek moet de organisatie binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Dat lukt alleen als de leverancier snel en volledig meldt.

VERBETEREN

Is dat meldpunt ook 's avonds, in het weekend en in de vakantie bereikbaar?

UITLEG

Datavoogd ziet dat de overeenkomst wel contactpersonen en contactgegevens aan beide zijden vastlegt (F131, F141), maar nergens vastlegt wanneer die contactpunten bereikbaar zijn: er zijn geen bereikbaarheidstijden, geen 24/7-afspraak en geen piket- of escalatieregeling als het primaire contactpunt niet reageert.

OOK OPGEMERKT

- Artikel 7.1 verplicht de verwerker tot melden binnen 24 uur (F060); zonder vastgelegde bereikbaarheid buiten kantooruren is die termijn in de praktijk moeilijk te waarborgen.
- De AVG-mailbox avg@voorbeeldwonen.example fungeert feitelijk als tweede kanaal, maar er is geen reactie- of escalatietermijn aan verbonden.

→ **Laat bereikbaarheidstijden en een tweede contact voor noodgevallen vastleggen.**

AP2025-2.2 | AP aanbeveling 1, datalekafspraken, p. 6: bereikbaarheid van het contactpunt (gezamenlijke mailbox)

VERBETEREN

Staat erin welke informatie de leverancier bij een datalek geeft?

UITLEG

Datavoogd ziet dat Bijlage 3 een concrete lijst met te verstrekken informatie bevat (contactgegevens, datum/tijd, omschrijving van het incident, welke gegevens en van wie) en dat artikel 7.2 verplicht tot het overleggen van getroffen maatregelen en nieuwe ontwikkelingen.

OOK OPGEMERKT

- Bijlage 3 vraagt om bewijsmateriaal en aangiftegegevens, maar niet om een inschatting van de waarschijnlijke gevolgen; dat is juist wat de corporatie bij de AP-melding moet invullen.

→ **Laat de informatie opsommen die nodig is voor de melding, zoals aantal mensen en gevolgen.**

AP2025-2.4 | AP aanbeveling 1, datalekafspraken, p. 7: minimale inhoud van de dataleknotificatie

Hulp bij vragen en onderzoeken

Mensen mogen hun gegevens inzien of laten verwijderen. De leverancier moet daarbij helpen, en ook bij een DPIA.

VERBETEREN

Helpt de leverancier als iemand zijn gegevens wil inzien of laten verwijderen?

UITLEG

Datavoogd ziet dat de overeenkomst bijstand bij verzoeken van betrokkenen regelt met een termijn van 14 dagen (binnen de maand van art. 12 lid 3 AVG) en dat is vastgelegd hoe rechtstreekse verzoeken worden behandeld: onverwijld melden, niet zelf beantwoorden en doorverwijzen naar de verantwoordelijke.

→ **Laat een termijn vastleggen en beschrijven hoe de leverancier helpt, bijvoorbeeld met een export per persoon.**

ART28-E | AVG art. 28 lid 3 onder e: bijstand bij verzoeken van betrokkenen

VERBETEREN

Helpt de leverancier bij beveiliging, datalekken en een DPIA?

UITLEG

Datavoogd ziet dat de bijstand bij datalekken en bij beveiliging is uitgewerkt (meldtermijn van 24 uur, proces en informatielijst in Bijlage 3, jaarlijkse beveiligingsrapportage), maar dat een bepaling over bijstand bij een gegevensbeschermingseffectbeoordeling (DPIA) en bij voorafgaande raadpleging van de Autoriteit Persoonsgegevens in de hoofdtekst en de bijlagen ontbreekt.

OOK OPGEMERKT

- Bijlage 4 verplicht partijen tot actualisatie van de risicotoets binnen 12 maanden, maar legt geen medewerkingsplicht van de verwerker (aanleveren van informatie over systemen, dataflows en subverwerkers) vast.
- Artikel 7.3 legt de melding aan toezichthouder en betrokkenen volledig bij de verantwoordelijke, zonder afspraak over ondersteuning door de verwerker bij het informeren van betrokkenen (art. 34 AVG).

→ **Laat per onderwerp vastleggen wat de leverancier levert en binnen welke termijn.**

ART28-F | AVG art. 28 lid 3 onder f: bijstand bij art. 32 t/m 36 (beveiliging, datalekken, DPIA, voorafgaande raadpleging)

Bewaren en verwijderen

Hoe lang gegevens blijven staan en wat er gebeurt als de samenwerking stopt.

VERBETEREN

Worden de gegevens verwijderd of teruggegeven als de samenwerking stopt?

UITLEG

Datavoogd ziet dat artikel 9 een exit-bepaling bevat met keuze tussen teruggave en wissen, het wissen van bestaande kopieën, een schriftelijke bevestiging en doorwerking naar subverwerkers, inclusief uitzondering voor wettelijke bewaarplicht.

OOK OPGEMERKT

- Artikel 9.3 spreekt van vernietiging 'op verzoek van de Verwerker'; gelet op de context lijkt de verwerkingsverantwoordelijke bedoeld, wat een tekstuele onduidelijkheid oplevert over wie het verzoek doet.
- Bijlage 1 noemt back-up in Nederland (F102), maar nergens is geregeld hoe back-upkopieën na einde van de overeenkomst worden gewist of overschreven.

→ **Laat een termijn vastleggen, ook voor back-ups, en een schriftelijke bevestiging dat alles is verwijderd.**

ART28-G | AVG art. 28 lid 3 onder g: wissen of teruggeven na afloop

VERBETEREN

Staat erin hoe lang gegevens worden bewaard?

UITLEG

Datavoogd ziet dat Bijlage 1 per gegevenscategorie een in tijd uitgedrukte bewaartermijn bevat (2 jaar na afronding van de opdracht), die in artikel 9.1 bindend is verklaard, en dat Bijlage 2 dezelfde termijn herhaalt.

OOK OPGEMERKT

- Artikel 9.1 koppelt verwijdering aan een verzoek van de verantwoordelijke; wat er automatisch gebeurt zodra de termijn van 2 jaar verstrijkt, is niet vastgelegd.

→ **Laat bewaartermijnen in dagen, maanden of jaren vastleggen, ook voor back-ups en logbestanden.**

AP2025-1.2 | AP aanbeveling 1 (maak afspraken zo concreet mogelijk), p. 6: duur en bewaartermijnen, dataminimalisatie

Up-to-date houden

Afspraken verouderen. Een datum, een versie en een moment om te herzien houden ze bij de praktijk.

VERBETEREN

Hebben de overeenkomst en de bijlagen een datum en versie?

UITLEG

Datavoogd ziet dat de hoofdtekst wel een datum draagt (1 oktober 2026) maar geen eigen versienummer; het genoemde versienummer 1.3 van 12 september 2023 betreft het onderliggende Aedes-sjabloon, niet deze overeenkomst.

OOK OPGEMERKT

- De ondertekeningsdatum in het handtekeningenblok is nog een placeholder (F080), terwijl artikel 2.1 de inwerkingtreding juist aan de datum van ondertekening koppelt.
- Bijlage 4 spreekt af de risicotoets binnen 12 maanden te actualiseren; zonder versieaanduiding per bijlage is later niet na te gaan welke versie van de bijlage bij welke actualisatie hoort.

→ **Zet een datum en versienummer op de overeenkomst en op elke bijlage.**

AP2025-4.1 | AP aanbeveling 3 (geef meer prioriteit aan opstellen en bijhouden), p. 10-11: bijhouden en periodiek herzien

VERBETEREN

Is afgesproken wanneer de afspraken opnieuw worden bekeken?

UITLEG

Datavoogd ziet dat het document alleen een algemene wijzigingsbepaling kent (art. 10.3) en losse afspraken over actualisering van de risicotoets (Bijlage 4) en overleg bij wijziging van beveiligingsmaatregelen (art. 4.9).

OOK OPGEMERKT

- De jaarlijkse beveiligingsrapportage (art. 4.3) en de actualisering van de risicotoets (Bijlage 4) bieden een natuurlijk moment om ook de verwerkersovereenkomst en bijlagen te herzien; dat verband is nu niet gelegd.

→ **Spreek een vast moment af, bijvoorbeeld jaarlijks, en bij grote veranderingen.**

AP2025-4.2 | AP aanbeveling 3 (geef meer prioriteit aan opstellen en bijhouden), p. 11: periodiek herzien van afspraken

VERBETEREN

Kloppen de bijlagen met hoe het nu echt gaat?

UITLEG

Datavoogd ziet dat alle vijf bijlagen zijn ingevuld en op hoofdlijnen aansluiten op de hoofdtekst: de subverwerkerslijst (Nederland, EER) spreekt de doorgiftebepaling in artikel 5 niet tegen en bijlage 5 verklaart de SCC's om die reden niet van toepassing.

OOK OPGEMERKT

- In bijlage 2 zijn de vakjes 'Certificering ISO 27001' en 'Multi Factor Authenticatie' niet aangekruist, terwijl bij 'Anders' juist ISO 27001 en MFA worden genoemd; dezelfde dubbeling staat bij de dienstomschrijving in bijlage 1 (vakje reparatie-/onderhoudswerkzaamheden leeg, 'Anders' beschrijft hetzelfde).
- De risicotoets in bijlage 4 dateert van 15 februari 2026, ruim voor de documentdatum van 1 oktober 2026; partijen spreken af de toets binnen 12 maanden te actualiseren.

→ **Loop de bijlagen samen met de leverancier na, vul ze volledig in en haal tegenstrijdigheden weg.**

AP2025-4.3 | AP aanbeveling 3 (geef meer prioriteit aan opstellen en bijhouden), p. 10-11: afspraken sluiten aan op de praktijk; gebruik van bijlagen

Hier vond Datavoogd niets

Bij deze vragen is geen punt gevonden. Dat is geen oordeel dat de afspraak voldoet.

- Staat erin waar de samenwerking over gaat en hoe lang die duurt?
- Staat erin wat de leverancier met de gegevens doet en waarom?
- Is de overeenkomst echt op deze dienst gemaakt?
- Gebruikt de leverancier de gegevens alleen voor deze opdracht?
- Staat erin welke gegevens worden gebruikt en van wie?

- Is duidelijk over welke mensen het gaat?
- Doet de leverancier alleen wat de organisatie vraagt?
- Kan de organisatie controleren of de leverancier zich aan de afspraken houdt?
- Staat erin welke systemen worden gebruikt, waar de gegevens staan en wie erbij kan?
- Is er aan beide kanten een vast meldpunt voor datalekken?
- Meldt de leverancier een datalek snel genoeg?
- Mag de leverancier zomaar andere bedrijven inschakelen?
- Staat erin welke andere bedrijven meewerken en waar die zitten?
- Wat gebeurt er als de leverancier een ander bedrijf wil inschakelen?
- Kunnen gegevens buiten Europa terechtkomen?

Daarnaast noteerde Datavoogd 43 kleine opmerkingen. Die staan in het volledige rapport; na de beoordeling komen de bevestigde opmerkingen in dit overzicht.

Over dit overzicht

Datavoogd leest het document en signaleert. Het geeft geen juridisch oordeel: de beoordeling is aan de functionaris gegevensbescherming of de privacy officer van de organisatie.

Beoordeling: 0 signaleringen bevestigd, 0 afgewezen, 57 open.

Dit is een concept: ook punten die nog niet beoordeeld zijn staan erin.

Toetsregels: vwo_art28 v2026-09-13.1, vwo_ap_2025 v2026-09-14.1. Teksten in gewone taal: v2026-09-18.1.

CONCEPT