Verwerkersovereenkomst

Als je gebruikmaakt van AO-online, leg je diverse gegevens van je medewerkers, leveranciers en/of anderen daarin vast. Daarbij zitten ook persoonsgegevens, zoals namen, (e-mail)adressen, telefoonnummers en geboortedata.

Juridisch gezien word jij aangemerkt als verantwoordelijke voor de verwerking van deze persoonsgegevens. Wijzelf worden aangemerkt als de verwerker, omdat wij het met ons systeem voor je mogelijk maken om deze gegevens op te slaan en te gebruiken.

Volgens de Algemene Verordening Gegevensverwerking (AVG) moet je afspraken met ons maken over de verwerking van de persoonsgegevens waarvoor jij de verantwoordelijke bent. Zo moet je ons expliciet de opdracht geven om die gegevens via ons systeem te verwerken. Ook moet je aangeven wat wij wel en niet met die gegevens mogen doen en hoe wij de gegevens moeten beveiligen. In deze verwerkersovereenkomst leggen we deze afspraken met je vast.

1. Wat betekenen alle juridische termen? Zoals verwerker, betrokkene en verantwoordelijke?

Omdat er in de AVG veel juridische termen gebruikt worden, leggen we deze graag eerst uit. Dit helpt je bij het lezen van de rest van dit document.

Persoonsgegeven: elk gegeven dat informatie geeft over een natuurlijk persoon en waarmee je direct of indirect de identiteit van deze persoon kunt vaststellen. Bijvoorbeeld een naam, (e-mail)adres of telefoonnummer.

Betrokkene: de persoon op wie een persoonsgegeven betrekking heeft, of zijn vertegenwoordiger. Dit is bijvoorbeeld de medewerker of leverancier van wie jij het adres en telefoonnummer hebt opgeslagen.

Verwerken van persoonsgegevens: alles wat je met persoonsgegevens kunt doen, zoals:

- het verzamelen, vastleggen en ordenen van gegevens;
- het opvragen, wijzigen en raadplegen van gegevens;
- het verstrekken van gegevens aan anderen;
- het afschermen of vernietigen van gegevens.

Verantwoordelijke: de persoon of organisatie die bepaalt:

- of er persoonsgegevens mogen worden verwerkt en zo ja, welke;
- met welk doel deze persoonsgegevens mogen worden verwerkt;
- wat die verwerking precies inhoudt; en
- welke middelen daarbij gebruikt mogen worden.

In deze verwerkersovereenkomst ben jij de verantwoordelijke.

Verwerker: de persoon of de organisatie die voor de verantwoordelijke persoonsgegevens verwerkt, bijvoorbeeld via een webapplicatie. In deze verwerkersovereenkomst zijn wij, AO-online, de verwerker.

Verwerkersovereenkomst: een overeenkomst waarin de verantwoordelijke (jij) en de verwerker (wij) afspraken maken over de verwerking van persoonsgegevens. Dit is de overeenkomst die je nu voor je hebt.

2. Wie is wie?

Als je in deze verwerkersovereenkomst ‘jij’, ‘je’ of ‘jou(w)’ leest, bedoelen we jou als klant van de online procesmanagement applicatie en/of de apps van AO-online en die met ons een overeenkomst tot gebruik van AO-online heeft gesloten.

Lees je ‘wij’, ‘we’, ‘ons’, of ‘onze’, dan bedoelen we AO-online V.O.F., gevestigd aan de Sparrendaal 6, 3452 LJ, in VLeuten. AO-online is ingeschreven bij de Kamer van Koophandel onder nummer 30205780.

3. Wanneer geldt deze verwerkersovereenkomst? Kan je deze tussentijds opzeggen?

Deze verwerkersovereenkomst geldt vanaf de datum waarop deze wordt afgesloten. Door online akkoord te geven, komt de verwerkersovereenkomst tot stand. Deze verwerkersovereenkomst is onderdeel van de overeenkomst die we met je hebben gesloten voor het gebruik van AO-online. Als jij of wij die overeenkomst beëindigen, eindigt deze verwerkersovereenkomst automatisch ook.

Je kunt deze verwerkersovereenkomst niet apart opzeggen. Je kunt hem alleen opzeggen als je ook de overeenkomst voor het gebruik van AO-online opzegt. In dat geval wordt deze verwerkersovereenkomst per direct beëindigd.

4. Welke persoonsgegevens verwerken we voor jou? En met welke doelen doen we dat?

Jij bent verantwoordelijk voor de persoonsgegevens die je via AO-online aan ons beschikbaar stelt. Wij verwerken deze persoonsgegevens alleen in opdracht van jou. Met deze verwerkersovereenkomst geef je ons de opdracht om de volgende gegevens te verwerken:

- Bedrijfsnaam
- Voornaam + achternaam
- T.a.v. gegevens
- Adres
- Postcode
- Plaats
- Land
- E-mailadres facturen
- KvK-nummer
- Btw-nummer
- Telefoonnummer
- Rekeningnummer

Voor het doel: het vastleggen, publiceren en beheren van processen en de functionaliteiten die hierbij horen.

Het kan zijn dat we op een later moment extra functionaliteiten aanbieden die horen bij het vastleggen, publiceren en beheren van processen. Als dit het geval is, dan hoort dat binnen de opdracht die je ons hebt gegeven en hoeven we niet apart toestemming te vragen voor het gebruik.

5. Aan welke regels houden wij ons?

Bij het verwerken van persoonsgegevens houden wij ons aan de wet. We verwerken deze gegevens op een behoorlijke, zorgvuldige en transparante manier, zoals de wet dat voorschrijft. De persoonsgegevens zijn van jou en we gebruiken deze alleen voor de doelen die we hierboven in artikel 4 hebben genoemd. Als we de gegevens ruimer willen gebruiken, vragen we hiervoor toestemming van jou of soms ook van jouw klanten en/of zorgen voor een wettelijke grondslag hiervoor.

De persoonsgegevens die je invoert blijven van jou. Dat betekent dat als je de overeenkomst opzegt, je de persoonsgegevens terugkrijgt. Dit kan je doen door deze te exporteren. Let op: doe dit wel voor de beëindiging van de overeenkomst. We verwijderen de persoonsgegevens namelijk na de beëindiging.

6. Wie krijgen er nog meer toegang tot de persoonsgegevens?

We maken zonder jouw toestemming geen gebruik van de diensten van andere organisaties, als deze daarbij toegang krijgen tot de persoonsgegevens waarvoor jij verantwoordelijk bent.

Als we eventueel toch een subverwerker gaan gebruiken, informeren we je altijd vooraf. Blijf je na de aankondiging gebruik maken van AO-online, dan heb je hierbij het akkoord gegeven voor die subverwerkers.

7. Waar worden de persoonsgegevens opgeslagen?

We hosten en verwerken de persoonsgegevens binnen de Europese Economische Ruimte (EER). We maken gebruik van Europese servers bij Trans-IP in Amsterdam.

8. Hoe beveiligen we de persoonsgegevens?

Om de persoonsgegevens te beveiligen hebben we passende technische en organisatorische maatregelen genomen. De keuze van deze maatregelen hebben we gebaseerd op de beschikbare technologie, de uitvoeringskosten, het type persoonsgegevens dat wij voor jou verwerken (zie artikel 4) en de risico's die daaraan verbonden zijn. We streven er naar dat deze maatregelen voldoen aan de eisen in artikel 32 van de AVG. Onze website heeft bijvoorbeeld een SSL certificaat en we maken gebruik van een firewall om misbruik te voorkomen.

Daarnaast hebben we een responsible disclosure beleid. Dat betekent dat we – naast het zelf actief zoeken naar kwetsbaarheden in ons systeem — ook open staan voor meldingen van kwetsbaarheden ontdekt door derden. We lossen deze gemelde kwetsbaarheden zo spoedig mogelijk op.

We beseffen dat de beveiligingseisen en de technologie voortdurend veranderen. Daarom spannen we ons in om de maatregelen die we op basis van dit artikel hebben genomen, voortdurend te evalueren en waar nodig te verscherpen, aan te vullen of te verbeteren.

9. Wat kan jij doen om de uitvoering van onze afspraken te controleren?

Als opdrachtgever heb jij het recht om periodiek audits uit te (laten) voeren om te controleren of wij voldoen aan de afspraken die in deze verwerkersovereenkomst staan. Hierover spreken we het volgende af:

1. We spannen ons altijd in om aan de afspraken uit deze verwerkersovereenkomst te voldoen. Ook kan het zijn dat we ons door een onafhankelijke en externe auditor laten controleren en dus een audit laten uitvoeren. Als dit het geval is, dan kan je altijd een afspraak maken om de rapportage van de externe en onafhankelijke auditor in te zien.
2. Als we een dergelijk auditrapport ter inzage hebben liggen, dan is dit de manier waarop je kan controleren of we ons aan de afspraken houden uit deze overeenkomst. Alleen als je met goede argumenten kunt aantonen dat we ons niet aan de afspraken uit deze overeenkomst hebben gehouden, dan heb je het recht om zelf een audit uit te laten voeren door een externe auditor op jouw eigen kosten. Dit recht heb je ook als we nog geen auditrapport ter inzage hebben liggen.
3. Als jij een audit wilt (laten) uitvoeren, kondig je dit minimaal 14 dagen van tevoren schriftelijk aan ons aan. Komt de datum en/of het tijdstip van de audit ons niet uit, dan laten we dit aan je weten en doen we een voorstel voor een vervangende datum en/of tijdstip.

4. Je maakt gebruik van een externe auditor die lid is van de Norea, of een auditor die voldoet aan dezelfde kwaliteitsstandaarden die de Norea stelt aan haar leden, zoals bijvoorbeeld de eis van geheimhouding en onafhankelijkheid. Voldoet de externe auditor niet aan deze kwaliteitseisen, dan behouden we het recht voor om deze te weigeren.
5. De personen die de audits uitvoeren, houden zich aan de beveiligingsprocedures die bij ons van kracht zijn. Dat betekent bijvoorbeeld dat ze geheimhouding afspreken. Ook jij houdt de uitslag van de audit geheim. Het is niet toegestaan hierover met derden te communiceren. Dit mag wel als we hiervoor toestemming hebben gegeven. We overleggen dan hier graag met je over.
6. Wij werken aan de audits mee en leveren zo tijdig mogelijk alle informatie aan die hiervoor redelijkerwijs relevant is. De kosten van de audits zijn voor jouw rekening.

10. Wat moeten jij en wij doen als er een datalek is?

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of waarbij er mogelijk onrechtmatig verwerking van persoonsgegevens niet kan worden uitgesloten. Hierover maken we de volgende afspraken:

1. Ontdekken wij dat er een datalek is of is geweest? En is er een aanzienlijke kans dat dit datalek nadelige gevolgen heeft voor de bescherming van de persoonsgegevens die wij voor jou verwerken? Dan laten we dit onmiddellijk aan je weten. Dit doen we uiterlijk binnen 48 uur nadat we het datalek hebben ontdekt.
2. Vervolgens overleggen we met jou over:
    - de aard van het datalek;
    - het risico dat jij en wij hiermee lopen, hebben gelopen of hadden kunnen lopen;
    - de maatregelen die we treffen of al getroffen hebben om het datalek op te lossen of om de gevolgen of schade zo veel mogelijk te beperken.
3. Na onze melding beoordeel jij of je het datalek moet melden aan de Autoriteit Persoonsgegevens en aan de mensen op wie de persoonsgegevens betrekking hebben (bijvoorbeeld jouw klanten en leveranciers). Wij doen dit zelf niet, omdat jij verantwoordelijk bent voor de wettelijke verplichtingen in dit kader.
4. Als de Autoriteit Persoonsgegevens een onderzoek naar het datalek start, dan laten wij dit meteen aan jou weten en werken we mee aan een onderzoek van de Autoriteit Persoonsgegevens.

11. Wat doen wij om de persoonsgegevens geheim te houden?

Wij zijn verplicht om alle persoonsgegevens die we voor jou verwerken, geheim te houden voor anderen. Daarbij gaat het om de gegevens die we van jou ontvangen en/of die we zelf verzamelen om ze te verwerken zoals we in onze overeenkomst hebben afgesproken. Hierover spreken we het volgende af:

1. Wij staan ervoor in dat al onze medewerkers zich houden aan deze geheimhoudingsplicht. Daarbij gaat het om medewerkers in de ruimste zin van het woord, dus ook stagiair(e)s en freelancers.
2. Deze geheimhoudingsplicht is niet van toepassing:
    - als jij uitdrukkelijk toestemming hebt gegeven om bepaalde persoonsgegevens met anderen te delen; of
    - als de persoon op wie de persoonsgegevens betrekking hebben (bijvoorbeeld een klant) uitdrukkelijk toestemming heeft gegeven om deze gegevens met anderen te delen; of
    - als er een wettelijke verplichting is om bepaalde persoonsgegevens aan een andere instantie of persoon, bijvoorbeeld aan het Openbaar Ministerie te verstrekken.
3. Als wij gebruikmaken van de diensten van een andere partij, zorgen wij er onvoorwaardelijk voor dat deze partij schriftelijk akkoord gaat met dezelfde geheimhoudingsplicht als die we met jou hebben afgesproken.

12. Hoe gaan wij om met de rechten van de betrokkenen?

De personen op wie de persoonsgegevens betrekking hebben, bijvoorbeeld jouw klanten en leveranciers, noemen we de betrokkenen. Deze betrokkenen hebben op basis van de AVG een aantal rechten. Jij bent verplicht om aan die rechten tegemoet te komen. Waar mogelijk helpen we jou daarbij. Daarbij gaat het onder meer om de volgende rechten:

1. De betrokkenen mogen vragen welke persoonsgegevens jij van hen verwerkt en opslaat. Dit staat in artikel 15 van de AVG. Als wij een dergelijk verzoek ontvangen, sturen we dat aan jou door. Jij bent dan verplicht om deze informatie te verstrekken, binnen het kader van de wet.
2. De betrokkenen mogen vragen om de persoonsgegevens die jij van hen hebt opgeslagen, te corrigeren of aan te vullen. Dit staat in artikel 16 van de AVG. Als wij een dergelijk verzoek ontvangen, sturen we het aan jou door. Je bent dan mogelijk verplicht om deze gegevens te corrigeren of aan te vullen. Dit kan je bijvoorbeeld doen door in je contactenlijst de gegevens te verwijderen en/of te corrigeren.

13. Wat zijn jouw verantwoordelijkheden en wie is er aansprakelijk bij schade?

Als verantwoordelijke voor de verwerking van persoonsgegevens, moet je aan een aantal eisen voldoen:

1. Je moet voldoen aan de wettelijke eisen die voor de verwerking van persoonsgegevens gelden. Dat betekent dat je moet nagaan of je volgens de wet het recht hebt om bepaalde persoonsgegevens vast te leggen. Dit is niet voor alle persoonsgegevens toegestaan. Zo mag je bijvoorbeeld niet zomaar een kopie van iemands paspoort of andere gevoelige (persoons)gegevens opslaan.
2. Je moet nagaan of de persoonsgegevens die je wilt vastleggen, voldoende beschermd worden door de beveiligingsmaatregelen. Wij hebben ons beveiligingsbeleid afgestemd op het soort gegevens dat we omschreven hebben – en met jou zijn overeengekomen – in artikel 4 van deze overeenkomst. Wil je een ander soort gegevens vastleggen, dan kunnen wij niet garanderen dat onze veiligheidsmaatregelen daarvoor voldoende zijn.
3. Je moet je account zo goed mogelijk beveiligen. Daarvoor bieden we je een aantal extra beveiligingsmaatregelen aan, die je zelf moet instellen. Zo kan je inloggen via tweestapsverificatie. Ook kan je aparte toegangsrechten aanmaken voor jouw administratiekantoor of voor iemand anders die je toegang tot AO-online wilt geven.

Voldoe je niet aan deze eisen en worden wij door anderen aansprakelijk gesteld voor schade die hierdoor ontstaan is? Dan stel je ons schadeloos en vrijwaar je ons voor die aansprakelijkheid.

Wij zijn alleen aansprakelijk voor schade die aan ons toegerekend kan worden. Gaat het om schade die verband houdt met de beveiliging van persoonsgegevens? Dan zijn we hier niet aansprakelijk voor als we kunnen bewijzen dat we voldoende technische en organisatorische beveiligingsmaatregelen hebben genomen, zoals omschreven in artikel 8 van deze overeenkomst. In dat geval kan deze schade ons niet toegerekend worden. Deze schade kan ons ook niet toegerekend worden als je geen extra beveiligingsmaatregelen hebt ingesteld, die we je aangeboden hebben.

Zijn we wel aansprakelijk, dan is deze aansprakelijkheid beperkt. Daarvoor gelden de afspraken die staan in onze overeenkomst voor het gebruik van AO-online.

14. Hoe gaan we om met geschillen?

Als we een geschil hebben, doen we ons best om samen met jou tot een oplossing te komen. Lukt dat niet, dan leggen we het geschil voor aan de bevoegde rechter te Utrecht of – als op basis van de wet een andere rechter bevoegd is – aan deze bevoegde rechter. Voor deze verwerkersovereenkomst geldt het Nederlandse recht. Dit geldt ook voor alle overeenkomsten en andere rechtshandelingen die uit deze overeenkomst voortvloeien of hiermee samenhangen.

15. Wat doen we als onze overeenkomsten elkaar tegenspreken?

Zit er een tegenstrijdigheid tussen deze verwerkersovereenkomst en de overeenkomst die we met je hebben gesloten voor het gebruik van AO-online? Dan gaat deze verwerkersovereenkomst voor en geldt wat hierin staat.