SMEDR

Verwerkersovereenkomst

Versie 1.2 · laatst bijgewerkt 27 augustus 2026 · www.smedr.nl

Deze verwerkersovereenkomst hoort bij de overeenkomst waarmee je smedr gebruikt. Hij regelt hoe wij omgaan met de persoonsgegevens die jij in smedr zet, en is voor al onze klanten gelijk — zodat je hem kunt lezen en accepteren zonder onderhandeling. Voor de gegevens die wij van jóu als klant verwerken geldt de privacyverklaring (www.smedr.nl/privacy.html).

1. Partijen en toepasselijkheid

Deze overeenkomst geldt tussen Elfrink Consulting (KvK 17254008, Berkstraat 24, 5492 EB Sint-Oedenrode), hierna de verwerker, en de organisatie die smedr gebruikt, hierna de verantwoordelijke.

De overeenkomst gaat in op het moment dat de verantwoordelijke smedr in gebruik neemt en loopt zolang dat gebruik duurt. Bij tegenstrijdigheid tussen deze overeenkomst en de algemene voorwaarden gaat deze overeenkomst voor, waar het de verwerking van persoonsgegevens betreft.

Deze overeenkomst is een concept dat nog juridisch wordt nagekeken. Heeft de verantwoordelijke een ondertekend exemplaar nodig, dan is dat op te vragen via info@smedr.nl.

2. Onderwerp: wat wij met de gegevens doen

De verwerker verwerkt persoonsgegevens uitsluitend om de dienst te leveren: het opslaan en bewerken van relaties, contactpersonen, offertes, facturen, abonnementen en de bijbehorende documenten, het versturen daarvan per e-mail namens de verantwoordelijke, en het beschikbaar en veilig houden van de omgeving.

De verwerker gebruikt de gegevens niet voor eigen doeleinden. Ze worden niet verkocht, niet gebruikt voor reclame, en niet gebruikt om modellen te trainen. De verwerker kijkt niet in de gegevens van een verantwoordelijke, behalve wanneer dat nodig is om een storing op te lossen of een verzoek om ondersteuning uit te voeren, en dan zo beperkt mogelijk.

De verwerker handelt uitsluitend op instructie van de verantwoordelijke. Die instructie is: de dienst leveren zoals hij is ingericht en zoals de verantwoordelijke hem gebruikt. Meent de verwerker dat een instructie in strijd is met de wet, dan meldt hij dat.

3. Om welke gegevens en personen het gaat

Wat er in smedr staat, bepaalt de verantwoordelijke zelf. In de praktijk gaat het om:

Categorie betrokkenen	Soorten persoonsgegevens
Contactpersonen bij klanten en prospects van de verantwoordelijke	Naam, aanhef, functie of afdeling, zakelijk e-mailadres, telefoonnummer, bezoek- en factuuradres
Medewerkers van de verantwoordelijke die met smedr werken	Naam, e-mailadres, rol en rechten, inloggegevens, persoonlijke ondertekening en afsluiting
Ondertekenaars van een offerte	Naam, handtekeningafbeelding, IP-adres en tijdstip van het akkoord, en een eventuele opmerking
Contactpersonen bij leveranciers van de verantwoordelijke	Naam en zakelijke contactgegevens

> *smedr is niet bedoeld voor bijzondere persoonsgegevens (zoals gezondheid, ras of politieke voorkeur) en niet voor burgerservicenummers. Die horen er dus niet in te staan.*

4. Vertrouwelijkheid

De verwerker houdt de gegevens vertrouwelijk. Iedereen die er namens de verwerker bij kan, is tot geheimhouding verplicht en krijgt alleen toegang voor zover het werk dat vereist.

5. Beveiliging

De verwerker neemt passende technische en organisatorische maatregelen. Op hoofdlijnen:

- Alle verbindingen lopen over HTTPS, met HSTS en een strikte Content Security Policy.
- Gegevens van verschillende organisaties zijn in de database van elkaar gescheiden met row-level security: de scheiding wordt op één plek in de database afgedwongen, niet per zoekopdracht opnieuw.
- Wachtwoorden worden gehasht opgeslagen, nooit leesbaar. Tweefactor-authenticatie (authenticator-app) is beschikbaar en per organisatie verplicht te maken.
- Na te veel mislukte inlogpogingen wordt een account tijdelijk vergrendeld. Sessies zijn centraal te beëindigen.
- Wachtwoorden, sleutels en verbindingsgegevens staan buiten de programmacode, in de beveiligde instellingen van het platform.
- Gegevens staan versleuteld op de opslag van de hostingpartij (encryptie at rest) en back-ups worden door die partij gemaakt en bewaard.
- Toegang tot de productieomgeving is beperkt tot de personen die deze toegang nodig hebben, met meervoudige verificatie.
- Toegang via de programmeerkoppeling (API) loopt over een sleutel die per organisatie geldt, alleen de rechten heeft die eraan zijn gegeven, in te trekken is en kan verlopen. Het verkeer is per sleutel begrensd, en van elke sleutel wordt bijgehouden wanneer hij voor het laatst is gebruikt.

De maatregelen kunnen veranderen als de techniek verandert; het beschermingsniveau wordt daarbij niet verlaagd. De verwerker heeft geen ISO 27001- of SOC 2-certificering.

6. Subverwerkers

De verantwoordelijke geeft de verwerker toestemming om de partijen hieronder in te schakelen. Zij mogen de gegevens alleen gebruiken voor de taak die erbij staat, en zijn daaraan contractueel gebonden, met verplichtingen die niet lichter zijn dan die uit deze overeenkomst.

Partij	Waarvoor	Waar	Status
Microsoft Azure	Hosting, database en bestandsopslag	EU — West Europe	In gebruik
Microsoft Graph	Verzenden van e-mail (offertes, facturen, herinneringen)	EU	In gebruik
Microsoft Entra ID	Inloggen met een werkaccount (SSO), bij organisaties die dat gebruiken	EU	In gebruik
Icecat	Productcontent opzoeken, alleen bij organisaties met die module aan	EU	In gebruik
Mollie	Betaallinks op facturen (iDEAL), via het eigen Mollie-account van de organisatie	EU — Nederland	In gebruik, alleen bij organisaties met de betaalmodule aan

Twee partijen in deze lijst zijn alleen aan de orde bij een verantwoordelijke die de bijbehorende module gebruikt: Icecat wordt pas aangeroepen als iemand productcontent opzoekt, en Mollie alleen als de verantwoordelijke betaallinks op zijn facturen aanzet.

Bij Mollie hoort een aantekening. Betalen loopt via het eigen Mollie-account van de verantwoordelijke: hij sluit die overeenkomst zelf, het geld gaat rechtstreeks naar zijn eigen rekening en komt nooit bij de verwerker. De verwerker zet de betaling voor hem klaar en stuurt daarbij het bedrag, een omschrijving (standaard het factuurnummer) en de webadressen voor terugkeer en terugmelding — geen naam, adres of e-mailadres van de betaler. Wat de betaler bij Mollie invult om te betalen, gaat rechtstreeks naar Mollie en loopt niet langs smedr.

Wil de verwerker een subverwerker toevoegen of vervangen, dan meldt hij dat minstens 30 dagen vooraf. De verantwoordelijke kan daar binnen die termijn met redenen bezwaar tegen maken; komen partijen er niet uit, dan mag de verantwoordelijke de overeenkomst opzeggen voor het deel dat de wijziging raakt, zonder kosten.

Deze lijst wijzigt vaker dan de rest van deze overeenkomst. De datum bovenaan geldt daarom ook voor de lijst: die zegt wanneer hij voor het laatst is bijgewerkt.

7. Koppelingen die de verantwoordelijke zelf maakt

De verantwoordelijke kan smedr met andere systemen laten praten via een API-sleutel die hij zelf aanmaakt. Wat hij daarmee aansluit, bepaalt hij zelf: een eigen script, een ERP, een koppelplatform, een rapportagetool, een dienst die vandaag nog niet bestaat. Voor die bestemming is de verantwoordelijke de verwerkingsverantwoordelijke. De verwerker is er geen verwerker van, en de partij erachter is geen subverwerker in de zin van deze overeenkomst — de verwerker heeft hem niet gekozen en heeft er geen zicht op.

Dat geldt ook wanneer de verwerker de koppeling zelf levert. Biedt hij een kant-en-klare verbinding naar een andere dienst aan, dan levert hij de koppeling, niet de bestemming: hij beoordeelt niet wat de partij aan de andere kant met de gegevens doet.

Een API-sleutel geeft toegang tot alle gegevens in de omgeving van de verantwoordelijke waarvoor de sleutel rechten heeft. De verantwoordelijke gaat er daarom mee om als met een wachtwoord: hij geeft hem niet door, bewaart hem niet in gedeelde bestanden, en geeft hem niet meer rechten dan de koppeling nodig heeft. Vermoedt hij dat een sleutel is uitgelekt, dan trekt hij hem in en meldt hij dat. De verwerker zorgt dat sleutels in te trekken zijn, kunnen vervallen, te vervangen zijn zonder onderbreking, en dat zichtbaar is wanneer een sleutel voor het laatst is gebruikt. Een incident dat ontstaat doordat een sleutel aan de kant van de verantwoordelijke is uitgelekt, is geen datalek bij de verwerker.

Laat de verantwoordelijke gebeurtenissen doorgeven aan een webadres dat hij zelf opgeeft (een webhook), dan stuurt de verwerker daar berichten naartoe. De verantwoordelijke kiest dat adres en bepaalt waar het staat, ook als dat buiten de Europese Unie is. De verwerker controleert de bestemming niet en beoordeelt niet wat daar met de gegevens gebeurt. Die berichten bevatten uitsluitend welke gebeurtenis heeft plaatsgevonden en om welk record het gaat, niet de inhoud daarvan.

> *Deze afspraken veranderen de subverwerkerslijst niet. Partijen die de verantwoordelijke zelf aansluit staan daar niet in, en horen daar ook niet in: het zijn geen partijen die de verwerker namens hem inschakelt.*

8. Doorgifte buiten de EU

De gegevens die de verantwoordelijke in smedr zet, blijven in de Europese Unie: hosting, database, bestandsopslag en e-mailverzending vinden plaats in de EU-regio van de hostingpartij. Er is voor deze gegevens geen doorgifte naar een land buiten de EU.

Verandert daarin iets — bijvoorbeeld door een nieuwe subverwerker — dan meldt de verwerker dat volgens de procedure in het artikel over subverwerkers, en gebeurt de doorgifte op basis van de standaardcontractbepalingen van de Europese Commissie.

Het bovenstaande gaat over doorgifte die de verwerker veroorzaakt. Geeft de verantwoordelijke een webadres op om gebeurtenissen naartoe te sturen, of sluit hij zelf een systeem aan met een API-sleutel, dan bepaalt hij waar die gegevens terechtkomen. Staat die bestemming buiten de Europese Unie, dan is het aan de verantwoordelijke om daarvoor een geldige grondslag te hebben.

9. Rechten van betrokkenen

Een betrokkene die zijn of haar rechten wil uitoefenen, wendt zich tot de verantwoordelijke: dat is de partij die bepaalt wat er in smedr staat. De verwerker verwijst zo iemand daarom door en voert zelf geen wijzigingen of verwijderingen uit op eigen initiatief.

De verwerker helpt de verantwoordelijke wel om zulke verzoeken uit te voeren. In de praktijk kan de verantwoordelijke inzage, correctie, export en verwijdering grotendeels zelf uitvoeren in de software; waar dat niet lukt, helpt de verwerker binnen een redelijke termijn.

10. Datalekken

Ontdekt de verwerker een inbreuk op de beveiliging die persoonsgegevens van de verantwoordelijke raakt, dan meldt hij dat zonder onnodige vertraging en in ieder geval binnen 48 uur na constatering aan het bij de verwerker bekende contactadres van de verantwoordelijke.

De melding bevat wat er bekend is over de aard van de inbreuk, welke categorieën gegevens en betrokkenen het raakt, de vermoedelijke gevolgen en de maatregelen die zijn of worden genomen. Ontbreekt er nog informatie, dan volgt die zodra de verwerker erover beschikt. De melding aan de Autoriteit Persoonsgegevens en aan betrokkenen doet de verantwoordelijke; de verwerker levert daarvoor de informatie die hij heeft.

11. Verantwoording en controle

De verwerker geeft op verzoek de informatie die de verantwoordelijke nodig heeft om te beoordelen of deze overeenkomst wordt nagekomen: een beschrijving van de maatregelen, de actuele subverwerkerslijst en de locaties van verwerking.

Wil de verantwoordelijke een audit door een onafhankelijke deskundige laten uitvoeren, dan is dat mogelijk: maximaal één keer per jaar, met een aankondiging van minstens 30 dagen, tijdens kantooruren, en zonder dat de vertrouwelijkheid tegenover andere klanten wordt geraakt. De redelijke kosten daarvan draagt de verantwoordelijke, behalve wanneer uit de audit een wezenlijke tekortkoming van de verwerker blijkt.

> *De verwerker belooft geen jaarlijkse externe audit en geen certificering. Wat hierboven staat, is wat een organisatie van deze omvang waar kan maken.*

12. Bewaren, teruggeven en verwijderen

Zolang de overeenkomst loopt, kan de verantwoordelijke zijn gegevens zelf exporteren: offertes en facturen als pdf, en facturen, factuurregels, betalingen, abonnementen en de btw-opstelling als CSV-bestand.

Na het einde van de overeenkomst blijven de gegevens 90 dagen beschikbaar voor export. Daarna verwijdert de verwerker ze uit de productieomgeving; back-ups verdwijnen daarna volgens het normale back-upschema van de hostingpartij. Op verzoek verwijdert de verwerker eerder.

Eén ding kan de verantwoordelijke niet zelf weggooien: een verstuurde factuur. Op verkoopfacturen rust een fiscale bewaarplicht van zeven jaar, en de software handhaaft die — een relatie met verstuurde facturen is niet te verwijderen, alleen te deactiveren. Die plicht is die van de verantwoordelijke; de verwerker maakt alleen dat naleven ervan mogelijk.

Naast de exportfunctie in de software kan de verantwoordelijke zijn gegevens ook via de programmeerkoppeling ophalen. Bij het einde van de overeenkomst vervallen alle API-sleutels van de organisatie en stoppen de koppelingen die daarvan gebruikmaakten.

Rust op de verwerker zelf een wettelijke bewaarplicht — bijvoorbeeld voor de facturen die de verwerker aan de verantwoordelijke stuurde — dan bewaart hij uitsluitend die gegevens, uitsluitend zolang dat moet.

13. Aansprakelijkheid en toepasselijk recht

Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde Nederlandse rechter. De aansprakelijkheidsregeling uit de algemene voorwaarden van de overeenkomst geldt ook hier, voor zover de wet dat toestaat.

Vragen over dit document? Mail info@smedr.nl.