

PUBLIEKE DOCUMENTATIE · VERSIE 1.0 · 13 OKTOBER 2026

Jouw data. Jouw regie. Onze verantwoordelijkheid.

Eigendom, privacy en beveiliging bij SocialNow en SocialNow OS.

Een uitgebreid handboek voor ondernemers, teamleden, ICT-beheerders en inkopers. Lees hoe gegevens worden gebruikt, hoe toegang en koppelingen zijn ingericht, wat je zelf beheert en welke afspraken gelden als je wilt stoppen.

100% jouw data.

Jouw bedrijfsgegevens blijven van jou. De rechten op software en ontwerpen staan afzonderlijk in de overeenkomst.

Veiligheid, zwart op wit.

Concrete maatregelen, heldere grenzen en afspraken voor het geval er iets misgaat.

Dit handboek verduidelijkt het gepubliceerde beleid. Het is geen certificaat, auditrapport, verwerkersovereenkomst of nieuwe garantie. De overeenkomst en de actuele juridische documenten blijven leidend. Een beveiligingsmaatregel verkleint risico's; absolute veiligheid bestaat niet.

00 · VEILIGHEID & DATA

Inhoud en leesroute

- 01 Leeswijzer en kernbeloften · pagina 3
- 02 Wat "jouw eigendom" betekent · pagina 4
- 03 Toegang en de grens van je werkruimte · pagina 5
- 04 Versleuteling en API-sleutels · pagina 6
- 05 Goedkeuring, koppelingen en AI · pagina 7
- 06 Leveranciers, locaties en gegevensstromen · pagina 8
- 07 Logging, ontwikkeling en continuïteit · pagina 9
- 08 Incidenten en kwetsbaarheden · pagina 10
- 09 Privacyrechten en veilig afscheid nemen · pagina 11
- 10 Jouw checklist voor veilig gebruik · pagina 12
- 11 Vragen voor ICT en inkoop · pagina 13
- 12 Veelgestelde vragen en contact · pagina 14

Bijlagen

A: gepubliceerde beveiligingsmaatregelen. B: relevante bepalingen over eigendom en gebruik. C: verwerking, beveiliging, incidenten en beëindiging. D: bronnen, versies en onderhoud.

Ondernemer: begin bij hoofdstukken 1, 2, 9 en 10. ICT-beheerder: lees vooral 3 tot en met 8 en 11.

Inkoper of privacyverantwoordelijke: combineer dit handboek met de verwerkersovereenkomst en de leverancierslijst. De bijlagen zijn gedateerde uittreksels; controleer de actuele online versie voordat je contractuele afspraken beoordeelt.

01 · VEILIGHEID & DATA

Leeswijzer en kernbeloften

Jij bepaalt het doel

Voor gegevens van jouw klanten, leads en medewerkers bepaal jij als organisatie het doel van de verwerking. SocialNow verwerkt die gegevens voor de afgesproken dienstverlening. Accountbeheer, facturering en eigen bedrijfsadministratie hebben een andere rolverdeling; die staat in het privacybeleid. Het gaat om de feitelijke verwerking, niet alleen om een etiket in een overeenkomst.

Jouw data blijft van jou

De eigendomsbelofte gaat over jouw bedrijfsgegevens en aangeleverde inhoud. Wij verkopen die gegevens niet, delen ze niet met andere klanten en gebruiken ze niet voor advertenties van derden. Je kunt gegevens laten teruggeven of wissen binnen de afspraken uit de verwerkersovereenkomst. Rechten van personen die in de gegevens voorkomen blijven daarnaast bestaan.

Beveiliging met concrete afspraken

Onze gepubliceerde maatregelen beschrijven versleuteling, controle op werkruimte en rol, beperkte beheerderstoegang en het veilig gebruiken van koppelsleutels. De sleutelbelofte beschrijft ook jouw goedkeuring voor wijzigingen en het uitsluiten van sleutels uit logs en AI-verzoeken. Deze maatregelen zijn bedoeld om ongewenste toegang en ongewenste acties te voorkomen.

Duidelijke grenzen

Dit document beweert niet dat elke gebruikte leverancier Europees is, dat iedere login tweestapsverificatie afdwingt of dat SocialNow ISO 27001- of SOC 2-gecertificeerd is. Het zegt ook niet dat een kopie van een gegeven direct uit iedere back-up verdwijnt. De hoofdstukken hieronder maken die verschillen expliciet, zodat je een zakelijke afweging kunt maken.

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

02 · VEILIGHEID & DATA

Wat “jouw eigendom” betekent

Data, accounts en materiaal

Jouw klantgegevens, bedrijfsinformatie en bestanden worden niet het eigendom van SocialNow doordat je ze in het OS zet. Je moet wel zelf het recht hebben om materiaal aan te leveren en gegevens te laten verwerken. Denk aan toestemming of een andere geldige grondslag voor persoonsgegevens, en aan gebruiksrechten voor foto's, muziek en teksten.

Software en ontwerpen zijn een ander onderwerp

De algemene voorwaarden behouden intellectuele eigendomsrechten van SocialNow en beschrijven hoe je geleverde ontwerpen, software en resultaten mag gebruiken. “100% jouw data” betekent daarom niet dat je automatisch de broncode van het SocialNow-platform, alle auteursrechten op een ontwerp of het intellectuele eigendom van een leverancier krijgt. Een afwijkende overdracht moet afzonderlijk en schriftelijk worden afgesproken.

Jouw regie over koppelingen

Gebruik accounts en sleutels die bij jouw organisatie horen. Een API-sleutel geeft toestemming voor bepaalde handelingen; hij draagt geen eigendom over. Bij het intrekken van de sleutel bij de bron stopt de betreffende koppeling. De bronleverancier bepaalt mede welke exportmogelijkheden, gebruiksrechten en bewaartermijnen gelden in zijn eigen dienst.

Teruggeven en wissen

Als je stopt, kun je kiezen voor teruggeven in een gangbaar formaat of wissen. Dat recht is iets anders dan een automatische volledige migratie naar een willekeurige andere applicatie. Spreek het gewenste exportformaat, de onderdelen, de verantwoordelijke persoon en eventuele migratiewerkzaamheden af voordat het account sluit.

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

03 · VEILIGHEID & DATA

Toegang en de grens van je werkruimte

Werkruimte en rol

Een werkruimte is de grens voor klantgegevens. Het gepubliceerde beveiligingsbeleid beschrijft controle per verzoek op werkruimte en rol. Rechten horen bij de taken van een persoon. Geef een medewerker alleen toegang tot de onderdelen die nodig zijn, en controleer na een functiewijziging of die rechten nog passend zijn.

Inloggen

Accountlogin gebruikt Google Firebase. Of een tweede factor wordt afgedwongen hangt af van de inlogroute en het accountbeleid. Het centrale beheerportaal ondersteunt passkeys en een tijdcode; daarmee is niet aangetoond dat iedere rechtstreekse app-login een tweede factor vraagt. Maak voor jouw organisatie expliciet welke routes worden gebruikt en welke extra beveiliging beschikbaar is.

Beheerderstoegang

Volgens het beleid werkt beheerderstoegang met een kortlevend, systeemgebonden toegangsbewijs. Het beschreven bewijs is twee minuten geldig en wordt door het klantsysteem beoordeeld. De uitgifte laat een auditspoor achter met wie, welk systeem en wanneer. Het toegangsbewijs zelf hoort niet in logs. Noodzakelijke ondersteuning en beveiliging geven bevoegde medewerkers beperkte, gelogde toegang.

- Gebruik persoonlijke accounts in plaats van een gedeeld teamwachtwoord.
- Trek toegang van vertrokken medewerkers tijdig in.
- Controleer rollen en actieve koppelingen bij het toevoegen van een nieuwe partner.
- Vraag bij twijfel welke toegang SocialNow voor een supportvraag nodig heeft.

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

04 · VEILIGHEID & DATA

Versleuteling en API-sleutels

Onderweg en in opslag

Het beveiligingsbeleid beschrijft TLS voor netwerkverkeer en versleuteling op de opslag van leveranciers. De sleutelbelofte noemt AES-256-GCM en een eigen sleutel per werkruimte voor koppelsleutels. Dit zijn verschillende lagen: versleuteling van verkeer beschermt de verbinding; versleuteling in opslag beschermt opgeslagen gegevens; controle op identiteit en rechten bepaalt wie een functie mag uitvoeren.

Een sleutel is een bevoegdheid

Gebruik een aparte API-gebruiker of sleutel voor het OS, met alleen de noodzakelijke rechten. Gebruik geen persoonlijk hoofdaccount als dat niet nodig is. Een gekoppelde bron kan eigen grenzen en abonnementseisen hebben. Controleer de rechten aan de kant van Odoo, Meta, Google, LinkedIn of de betreffende leverancier voordat je de sleutel invoert.

Geen sleutels in de browser, logs of AI

De sleutelbelofte zegt dat de sleutel niet terug naar de browser gaat, niet zichtbaar is in app of beheerscherm, uit logbestanden wordt gefilterd en niet in een vraag aan een AI-model wordt meegestuurd. Een gemaskeerde sleutel of een statusmelding is geen reden om een geheime waarde in een chat of screenshot te delen.

Intrekken en vervangen

Trek een sleutel in bij de bron als een gebruiker vertrekt, een bevoegdheid niet meer nodig is of je vermoedt dat een sleutel is uitgelekt. Alleen de socials-sleutel heeft volgens de sleutelbelofte een verwijdermogelijkheid in het OS; andere sleutels trek je bij de bron in of je vraagt ondersteuning. Test daarna of de bedoelde toegang werkelijk is gestopt.

Bron: [Veiligheid en sleutelbelofte](#)

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

05 · VEILIGHEID & DATA

Goedkeuring, koppelingen en AI

Van voorstel naar actie

De sleutelbelofte beschrijft dat het OS pas schrijft in gekoppelde systemen na een voorstel dat jij goedkeurt, en dat de actie in een logboek komt. Het privacybeleid beschrijft menselijke tussenkomst bij publiceren, versturen en betalen. Controleer bij een voorstel de ontvanger, inhoud, bron, timing en gevolgen voordat je akkoord geeft. Eerder geconfigureerde opdrachten en instellingen kunnen eveneens instructies zijn.

AI verwerkt wat nodig is

Voor teksten, beelden en analyses kunnen relevante gegevens naar een modelleverancier gaan. Het privacybeleid noemt onder meer je verhaal, branding en relevante cijfers. De verwerkersovereenkomst noemt Google, OpenAI, Anthropic en Higgsfield bij de modeldiensten. Welke dienst een taak uitvoert hangt af van de gekozen functie. Je gegevens blijven dus niet per definitie uitsluitend in één lokale omgeving.

Training en toestemming

De leverancierslijst in de verwerkersovereenkomst beschrijft dat contractueel is uitgesloten dat de invoer wordt gebruikt voor modeltraining. Dat is een beleids- en contractafpraak voor de genoemde dienstconfiguraties, geen algemene uitspraak over ieder consumentenaccount van dezelfde leverancier. Vraag bij een nieuwe functie of afwijkende configuratie om de geldende afspraken.

Noodzakelijk gebruik en optionele meting

De actuele algemene voorwaarden maken onderscheid tussen beperkte toegang voor ondersteuning en beveiliging, en optionele gebruiksmeting en afzonderlijke gemaskeerde sessieopnamen waarvoor toestemming nodig is. Een account aanmaken geeft geen algemene toestemming om bedrijfsinhoud voor eigen productontwikkeling te gebruiken. Je beheert de optionele keuzes onder Account.

Bron: [Privacybeleid](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

06 · VEILIGHEID & DATA

Leveranciers, locaties en gegevensstromen

De gegevensstroom in vijf stappen

1. Jij of je team voert gegevens in of koppelt een bron. 2. Het OS controleert de identiteit, werkruimte en bevoegdheden. 3. De gekozen functie gebruikt de relevante opslag, communicatie- of modeldienst. 4. Een voorstel wordt aan je getoond wanneer goedkeuring nodig is. 5. Een goedgekeurde actie gaat naar de aangesloten bron. Het precieze pad verschilt per functie en leverancier.

De rol van leveranciers

De gepubliceerde verwerkersovereenkomst noemt leveranciers voor hosting, opslag, inloggen, mail, meting, AI en socialkanalen. Die leveranciers zijn subverwerkers als zij persoonsgegevens namens SocialNow verwerken. Een merk in het partnerblok is niet automatisch een subverwerker voor jouw gegevens. Een mogelijke koppeling of een verkennend gesprek betekent ook niet dat die partij al toegang tot jouw werkruimte heeft.

Locatie en internationale doorgifte

De dienstverlening is niet uitsluitend Europees. De verwerkersovereenkomst vermeldt een EU-regio voor PostHog en Amerikaanse regio's voor de beschreven Vercel-appfuncties. Leveranciers, locaties en doorgiftemechanismen kunnen per dienst verschillen. Het beleid beschrijft passende doorgiftemechanismen, zoals standaardcontractbepalingen of waar toepasselijk het EU-VS Data Privacy Framework. Controleer voor gevoelige toepassingen de concrete dienst en regio.

Controle bij verandering

De leverancierslijst is een gedateerde momentopname. De overeenkomst beschrijft aankondiging van wijzigingen en de mogelijkheden om bezwaar te maken. Vraag voor een inkoopbesluit om de actuele lijst, de gebruikte configuratie en de gegevenscategorieën. Een logo of dit handboek vervangt die controle niet.

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

Bron: [Privacybeleid](#) · Laatst bijgewerkt: 20 september 2026

07 · VEILIGHEID & DATA

Logging, ontwikkeling en continuïteit

Auditsporen en foutmeldingen

Het beveiligingsbeleid beschrijft registratie van handelingen met gevolgen, zoals toegang verlenen, een systeem openen en een sleutel wijzigen. De sleutelbelofte beschrijft een logboek van acties. Sleutels horen niet in dat logboek. Deel bij een supportvraag bij voorkeur een tijdstip, werkruimte, foutmelding en een gemaskeerd voorbeeld; stuur geen complete klantendatabase als een klein voorbeeld voldoende is.

Ontwikkeling en wijzigingen

Het beleid beschrijft versiebeheer, herleidbare publicaties, automatische controles, een Content Security Policy en controles op kwetsbaarheden in afhankelijkheden. Dit handboek is geen onafhankelijke verificatie van iedere controle op iedere toepassing. Vraag bij een audit om bewijs dat past bij het systeem en de release die jouw organisatie gebruikt. De publieke website en de klantapp zijn verschillende toepassingen.

Back-ups zijn geen migratieplan

De verwerkersovereenkomst beschrijft het verlopen van back-ups na beëindiging. Daarmee is geen algemene dagelijkse back-upfrequentie, hersteltijd, maximaal gegevensverlies of beschikbaarheidspercentage afgesproken. Als jouw bedrijfsproces een specifieke RTO, RPO of SLA nodig heeft, laat die waarden voor jouw systeem expliciet vastleggen. Houd waar nodig ook eigen exports van bedrijfskritische gegevens bij.

Wat versleuteling niet oplost

Versleuteling voorkomt niet dat een bevoegd account een verkeerd bestand publiceert, een gebruiker een phishingverzoek volgt of een externe leverancier onbereikbaar raakt. Identiteitscontrole, beperkte rechten, menselijke controle en afspraken over herstel horen daarom bij dezelfde beveiligingsaanpak.

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

08 · VEILIGHEID & DATA

Incidenten en kwetsbaarheden

Melden bij SocialNow

Een vermoeden van ongewenste toegang, een uitgelekte sleutel of een kwetsbaarheid meld je aan security@socialnow.nl. Vermeld het tijdstip, het getroffen systeem, het gedrag dat je zag en hoe wij het kunnen reproduceren. Gebruik een gemaskeerde screenshot of een minimaal voorbeeld. Deel geen gegevens van andere klanten en publiceer het probleem niet voordat het verantwoord is afgehandeld.

De 24-uursafpraak

SocialNow meldt volgens de verwerkersovereenkomst een ontdekte inbreuk in verband met persoonsgegevens zonder onredelijke vertraging en uiterlijk binnen 24 uur bij de betrokken klant. De eerste melding bevat de feiten voor zover bekend; aanvullende informatie volgt zodra die beschikbaar is. Dit is een melding aan de klant. De klant beoordeelt zelf of een melding bij de toezichthouder of betrokkenen nodig is, tenzij SocialNow schriftelijk wordt gevraagd namens de klant te handelen.

De wettelijke termijn is een andere termijn

De Autoriteit Persoonsgegevens legt uit dat een meldplichtig datalek binnen 72 uur na kennisname moet worden gemeld. Niet elk beveiligingsincident is automatisch zo'n meldplichtig datalek. De feitelijke aantasting van persoonsgegevens en de risico's zijn bepalend. Houd het onderzoek, de afweging en de maatregelen bij in een incidentregister.

Verantwoord kwetsbaarheden melden

Het beveiligingsbeleid beschrijft een menselijke reactie binnen drie werkdagen en een inschatting van de ernst binnen tien werkdagen. Stop als je onbedoeld toegang krijgt tot andermans gegevens. Belast het systeem niet met zware scans, verwijder niets en gebruik geen phishing of social engineering. SocialNow heeft geen beloningsprogramma volgens het gepubliceerde beleid.

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

Externe uitleg: [AP · Zo meldt u een datalek](#)

09 · VEILIGHEID & DATA

Privacyrechten en veilig afscheid nemen

Rechten en verzoeken

Het privacybeleid beschrijft inzage, correctie, verwijdering, beperking, overdracht, bezwaar en het intrekken van toestemming, voor zover die rechten in de concrete situatie van toepassing zijn. Voor gegevens van jouw eigen klanten of medewerkers ben jij hun aanspreekpunt als verwerkingsverantwoordelijke. SocialNow ondersteunt je als verwerker bij de uitvoering van die verzoeken.

Identiteit en omvang

Beschrijf bij een verzoek welke persoon, werkruimte en gegevens bedoeld worden. Identiteitscontrole voorkomt dat een export bij de verkeerde persoon terecht komt. Vraag geen gegevens op via een openbaar gedeelde link of een onbeveiligd groepsgesprek. Leg voor een grote export het formaat, de bestemming en de bevoegde ontvanger vast. Bij twijfel over de juiste route kun je privacy@socialnow.nl gebruiken.

Als je stopt

Volgens de verwerkersovereenkomst kies je voor teruggeven in een gangbaar bestandsformaat of wissen. Zonder keuze binnen dertig dagen na het einde worden gegevens gewist. De afspraak beschrijft verwijdering uit actieve systemen binnen dertig dagen en uit back-ups uiterlijk na negentig dagen. Een kopie in een aflopende back-up wordt niet meer gebruikt of getoond.

Uitzonderingen en controle

Een wettelijke bewaarplicht kan verwijdering voor bepaalde gegevens uitstellen, bijvoorbeeld voor factuuradministratie. Dat verandert het doel van de bewaring niet: die gegevens worden dan voor de wettelijke verplichting bewaard. Vraag desgewenst schriftelijke bevestiging van het wissen. Trek ook sleutels bij bronleveranciers in en controleer afzonderlijk de accounts, abonnementen en gegevens die daar blijven staan.

Bron: [Privacybeleid](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

10 · VEILIGHEID & DATA

Jouw checklist voor veilig gebruik

Bij de start

Kies één verantwoordelijke voor de werkruimte en één vervanger. Breng in kaart welke bronnen je gaat koppelen, welke gegevens erin staan en wie toegang nodig heeft. Controleer dat je gegevens mag laten verwerken en dat de gekozen dienst past bij eventuele sector- of klantvereisten. Lees de verwerkersovereenkomst voordat je persoonsgegevens van derden gebruikt.

- Persoonlijke accounts en passende rollen ingericht.
- Beschikbare passkeys of tweestapsverificatie geactiveerd.
- Aparte API-gebruiker met beperkte rechten aangemaakt.
- Geen geheimen in gedeelde documenten of prompts opgeslagen.
- Optionele meting en sessieopnamen bewust gekozen.
- Contactpersoon voor privacy en incidenten bekend.

Bij dagelijkse werkzaamheden

Controleer voorgestelde acties voordat je goedkeurt. Neem geen complete databases op in een AI-verzoek als een beperkt deel voldoende is. Masker persoonsgegevens en sleutels bij support. Controleer toegang bij personeelwisselingen en na het inschakelen van een partner. Houd eigen procesafspraken bij; een veiligheidsfunctie kan een ontbrekende werkafpraak niet herstellen.

Bij wijziging of vertrek

Beoordeel rechten opnieuw als een functie of koppeling verandert. Controleer de actuele leverancierslijst bij een nieuwe dienst. Plan de export voordat een account sluit, trek bronrechten in en vraag om bevestiging van verwijdering waar dat nodig is. Spreek extra continuïteitseisen schriftelijk af in plaats van ze af te leiden uit een algemene marketingtekst.

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

Meer uitleg: [Veilig koppelen](#)

11 · VEILIGHEID & DATA

Vragen voor ICT en inkoop

Een zakelijke beoordeling gaat verder dan "is het veilig?". Gebruik onderstaande onderwerpen om vast te stellen of de dienstverlening past bij jouw organisatie. Dit is een vragenlijst voor controle, geen verklaring dat elke hieronder genoemde extra maatregel standaard aanwezig is.

Rol en doel

Welke gegevens verwerken jullie voor ons, voor welk doel en op welke instructie?

Toegang

Welke inlogroutes gebruiken wij, welke tweede factor is beschikbaar en welke beheerderstoegang is mogelijk?

Sleutels

Hoe worden onze koppelsleutels opgeslagen, uitgesloten van logs en AI, en ingetrokken?

Leveranciers

Welke subverwerkers en regio's gebruikt onze configuratie daadwerkelijk?

AI

Welke modeldienst verwerkt welke invoer, met welke afspraken over training en bewaring?

Continuïteit

Welke back-ups, hersteltests, hersteltijden en beschikbaarheidsafspraken gelden specifiek voor ons?

Incident

Wie is onze contactpersoon, hoe verloopt de melding en welke gegevens krijgen wij?

Exit

Welke onderdelen kunnen we exporteren, in welk formaat en met welke termijnen voor wissen?

Bewijs

Welke auditsporen en maatregelen kunnen jullie voor onze toepassing aantonen?

De verwerkersovereenkomst beschrijft informatieverstrekking en audits. Bescherm bij een audit gegevens van andere klanten en de vertrouwelijke beveiligingsinformatie van leveranciers. Een eventuele geheimhoudingsovereenkomst legt vertrouwelijkheid vast; zij bewijst op zichzelf geen technische veiligheid.

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

12 · VEILIGHEID & DATA

Veelgestelde vragen en contact

Is mijn data echt van mij?

Je bedrijfsgegevens blijven van jou. Rechten van betrokken personen blijven gelden. Het eigendom of de gebruiksrechten van software, ontwerpen en materiaal van derden worden afzonderlijk geregeld.

Kunnen jullie technisch nergens bij?

Noodzakelijke ondersteuning en beveiliging kunnen beperkte, gelogde toegang voor bevoegde medewerkers vereisen. De belofte is gecontroleerde toegang en geheimhouding, niet dat toegang technisch onmogelijk is.

Staat alles in Europa?

Nee. De leveranciers en locaties verschillen per dienst. Het gepubliceerde beleid benoemt ook verwerking buiten de EER en de bijbehorende doorgiftemechanismen.

Wordt mijn invoer gebruikt om AI-modellen te trainen?

De gepubliceerde verwerkersovereenkomst beschrijft uitsluiting van training bij de genoemde modeldiensten. Controleer voor jouw gekozen configuratie de actuele afspraken. Sleutels gaan volgens de sleutelbelofte nooit naar een AI-model.

Hebben jullie ISO 27001 of SOC 2?

Het gepubliceerde beveiligingsbeleid zegt dat SocialNow deze certificeringen niet heeft. Dit document is geen vervangende certificering.

Kan ik weg zonder mijn gegevens te verliezen?

Je kunt gegevens laten teruggeven of wissen volgens de verwerkersovereenkomst. Plan de export vóór sluiting en maak aparte afspraken voor een eventuele migratie.

Is veiligheid voor 100% gegarandeerd?

Nee. Risico's worden beperkt met technische maatregelen, werkafspraken en controle. Daarom publiceren wij zowel maatregelen als grenzen en het incidentproces.

Contact

Beveiliging en kwetsbaarheden: security@socialnow.nl. Privacy, gegevens en verzoeken: privacy@socialnow.nl. Algemeen: hello@socialnow.nl. SocialNow, Amstelstraat 43G, 1017 DA Amsterdam. De actuele contact- en bedrijfsgegevens staan op de website.

[Veiligheid](#) · [Juridische documenten](#)

BIJLAGE A

Beveiliging · beleidsuittreksel

Onderstaande tekst komt uit de gepubliceerde beleidsbron. Dit is een gedateerde selectie voor naslag. De actuele online tekst en jouw overeenkomst blijven leidend. Deze bijlage is geen onafhankelijk auditbewijs.

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

De uitgangspunten

Zo min mogelijk bewaren. Wat er niet is, kan niet uitlekken. Wij vragen geen gegevens die wij niet nodig hebben en bewaren niets langer dan waarvoor wij het hebben.

Eén werkruimte is een grens. Elk verzoek wordt per verzoek gecontroleerd op werkruimte en rol; er is geen scherm waarin per ongeluk de gegevens van een andere klant kunnen verschijnen.

Een sleutel die je ons geeft is van jou. Sleutels voor Odoo, Meta, Google of je socialkanalen worden versleuteld opgeslagen, nooit teruggetoond, nooit in een logregel geschreven en nooit naar een AI-model gestuurd.

Toegang van een beheerder is tijdelijk en laat een spoor na. Er is geen permanente beheerderssessie in een klantomgeving.

Toegang

Accountlogin loopt via Google Firebase. Of tweestapsverificatie wordt afgedwongen hangt af van de gebruikte inlogroute en het accountbeleid. Het centrale beheerportaal ondersteunt passkeys en een tijdcode. Dit is geen garantie dat elke rechtstreekse app-login een tweede factor vraagt.

Wil een beheerder een klantomgeving openen, dan gebeurt dat met een briefje dat twee minuten geldig is, dat alleen dat ene systeem opent en dat door dat systeem zelf wordt beoordeeld. Het briefje zelf komt nergens in een logboek; de uitgifte wel, met wie, welk systeem en wanneer.

Rechten worden per werkruimte toegekend. Vertrekt iemand, dan wordt zijn toegang ingetrokken; in het OS doe je dat zelf onder Team.

Versleuteling

Al het verkeer loopt over TLS. Wie op http binnenkomt wordt doorgestuurd naar https.

Gegevens staan versleuteld op de opslag van onze leveranciers.

Geheimen staan uitsluitend in de omgeving van de hostingleverancier. Ze staan niet in de broncode en niet in een configuratiebestand dat meegaat in versiebeheer.

Toezicht

Handelingen met gevolgen – toegang verlenen, een systeem openen, een sleutel wijzigen – komen in een auditspoor.

Fouten en waarschuwingen worden centraal verzameld. Persoonsgegevens worden daar niet in meegeschreven.

De bereikbaarheid en de inlogbeveiliging van elk klantsysteem worden doorlopend automatisch gecontroleerd. Serveert een systeem zijn startpagina zonder inlog, dan staat dat als alarm op het beheerscherm.

Als er toch iets misgaat

Wij melden een inbreuk in verband met persoonsgegevens binnen 24 uur na ontdekking bij de betrokken klant, met wat er is gebeurd, wat het vermoedelijk raakt, wat wij hebben gedaan en bij wie je terecht kunt. Dat is korter dan de 72 uur die de AVG jou geeft, zodat jij je eigen afweging kunt maken met tijd over.

Wij houden een register bij van inbreuken, ook van die welke niet gemeld hoefden te worden.

Wij melden niet namens jou bij de toezichthouder, tenzij je ons daar schriftelijk om vraagt. Jij bent de verwerkingsverantwoordelijke; die melding is jouw beslissing.

Een kwetsbaarheid melden

Vind je iets, meld het dan op security@socialnow.nl, of lees eerst <https://socialnow.nl/security.txt>. Beschrijf wat je vond, waar, en hoe je het kunt laten zien. Een schermafbeelding of een kort stappenplan helpt.

Wat je van ons mag verwachten: binnen drie werkdagen een reactie van een mens, een inschatting van de ernst binnen tien werkdagen, en bericht wanneer het verholpen is. Meld je verantwoord en misbruik je niet wat je gevonden hebt, dan doen wij geen aangifte en stellen wij je niet aansprakelijk. Wil je genoemd worden bij de oplossing, dan doen wij dat graag.

Wat wij van jou vragen: geen gegevens van anderen inzien, kopiëren, wijzigen of verwijderen; geen dienst platleggen; geen social engineering, phishing of fysieke toegang; geen geautomatiseerd scannen dat het systeem belast; en het lek niet delen voordat het verholpen is. Kom je onbedoeld bij gegevens van anderen, stop dan en meld dat erbij.

Wij betalen geen beloning. Wat wij wel doen is snel antwoorden en snel oplossen.

Contact

Kwetsbaarheden: security@socialnow.nl. Privacy en gegevens: privacy@socialnow.nl. Alles daarbuiten: hello@socialnow.nl.

BIJLAGE B

Algemene voorwaarden · beleidsuittreksel

Onderstaande tekst komt uit de gepubliceerde beleidsbron. Dit is een gedateerde selectie voor naslag. De actuele online tekst en jouw overeenkomst blijven leidend. Deze bijlage is geen onafhankelijk auditbewijs.

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

15. Auteursrecht en intellectueel eigendom

Opdrachtnemer behoudt de rechten die hem op grond van de Auteurswet toekomen. Verstrekte stukken, ontwerpen, software en andere resultaten zijn uitsluitend bestemd voor gebruik door opdrachtgever en mogen zonder toestemming niet worden verveelvoudigd, openbaar gemaakt of aan derden verstrekt. Opdrachtnemer mag de kennis die hij door de werkzaamheden opdoet voor andere doeleinden gebruiken, zolang geen vertrouwelijke informatie bij derden terechtkomt. Opdrachtgever stemt ermee in dat zijn logo, de gemaakte ontwerpen en zijn ervaringen herkenbaar voor promotie worden gebruikt, tenzij die gevoelige of vertrouwelijke informatie bevatten; opdrachtgever kan daar bezwaar tegen maken, waarna opdrachtnemer de publicatie niet plaatst of waar mogelijk verwijdt.

17. SocialNow OS: account, gegevens en verbetering

SocialNow OS is de online omgeving op app.socialnow.nl waarin opdrachtgever zijn website, klanten, content en advertenties beheert. Wie een account aanmaakt gaat akkoord met deze voorwaarden en met het privacybeleid op socialnow.nl/privacy.

Noodzakelijke ondersteuning en beveiliging geven bevoegde medewerkers beperkte, gelogde toegang. Vrijwillige gebruiksmeting en afzonderlijke gemaskeerde schermopnames vragen toestemming die onder Account kan worden ingetrokken. Een account aanmaken geeft geen algemene toestemming om bedrijfsinhoud voor eigen productontwikkeling te gebruiken. Zie socialnow.nl/privacy.

SocialNow verkoopt deze gegevens nooit, deelt ze nooit met andere klanten en gebruikt ze nooit voor advertenties van derden. Gegevens van gekoppelde bronnen zoals Odoo, Meta en Google worden alleen gelezen voor de eigen werkruimte van opdrachtgever; de sleutels die opdrachtgever invoert worden versleuteld bewaard en niet getoond.

Opdrachtgever blijft eigenaar van zijn gegevens en kan zijn account op elk moment verwijderen onder Account in het OS. Toegang wordt gesloten en verwijdering wordt afgehandeld volgens het privacybeleid; wettelijke bewaarplichten blijven gelden.

Het OS wordt geleverd zoals het is en wordt voortdurend doorontwikkeld. SocialNow geeft geen garantie op ononderbroken beschikbaarheid en mag functies wijzigen of beëindigen. Opdrachtgever gebruikt het OS niet voor illegale doeleinden, spam of misbruik van gekoppelde platformen en houdt zich aan de voorwaarden van die platformen.

BIJLAGE C

Verwerkersovereenkomst · beleidsuittreksel

Onderstaande tekst komt uit de gepubliceerde beleidsbron. Dit is een gedateerde selectie voor naslag. De actuele online tekst en jouw overeenkomst blijven leidend. Deze bijlage is geen onafhankelijk auditbewijs.

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

3. Geheimhouding

Iedereen die bij ons toegang heeft tot jouw gegevens is tot geheimhouding verplicht, schriftelijk of op grond van de wet. Dat geldt voor medewerkers, voor ingeschakelde specialisten en voor de beheerders van onze systemen.

Toegang wordt alleen gegeven aan wie hem voor zijn werk nodig heeft, en wordt ingetrokken zodra dat niet meer zo is. Beheerderstoegang tot een klantomgeving verloopt via een kortlevende, gelogde sessie; die toegang staat in een auditspoor dat wij bewaren.

De geheimhouding blijft gelden na afloop van deze overeenkomst en na het einde van een dienstverband of opdracht.

4. Beveiliging

Wij nemen passende technische en organisatorische maatregelen als bedoeld in artikel 32 AVG, rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doeleinden van de verwerking, en met de risico's voor de betrokkenen.

De maatregelen die wij op dit moment treffen staan beschreven in bijlage B. Die bijlage is een momentopname: wij mogen maatregelen vervangen door maatregelen die minstens zo beschermend zijn, en zullen het beschermingsniveau niet verlagen.

Jij bent zelf verantwoordelijk voor de beveiliging aan jouw kant: sterke wachtwoorden of passkeys, tweestapsverificatie waar die beschikbaar is, het tijdig intrekken van toegang van vertrokken teamleden, en het zorgvuldig omgaan met de sleutels die je in het OS invoert.

5. Subverwerkers

Je geeft ons algemene toestemming om subverwerkers in te schakelen. De subverwerkers die wij nu gebruiken staan in bijlage C, met per partij waarvoor wij hem gebruiken en waar de gegevens staan.

Wij leggen elke subverwerker dezelfde verplichtingen op als wij tegenover jou hebben, in een schriftelijke overeenkomst. Komt een subverwerker die verplichtingen niet na, dan blijven wij tegenover jou volledig aansprakelijk.

Willen wij een subverwerker toevoegen of vervangen, dan melden wij dat minstens dertig dagen van tevoren per e-mail en op socialnow.nl/verwerkersovereenkomst. Heb je binnen die termijn een redelijk bezwaar dat de bescherming van persoonsgegevens betreft, dan zoeken wij samen naar een

oplossing; komen wij daar niet uit, dan mag je de betrokken dienst opzeggen zonder opzegkosten, tegen terugbetaling van het vooruitbetaalde deel.

Partijen die jij zelf koppelt – je eigen Odoo, je eigen Meta-account, je eigen Google-property, je eigen socialkanalen – zijn geen subverwerkers van ons. Jij hebt met die partijen een eigen verhouding; wij lezen en schrijven daar alleen met de sleutel die jij ons geeft, en alleen binnen jouw werkruimte.

6. Rechten van betrokkenen

Krijgt een betrokkene bij ons een verzoek binnen dat eigenlijk voor jou bedoeld is – inzage, rectificatie, wissing, beperking, overdraagbaarheid of bezwaar – dan voeren wij dat niet zelf uit. Wij sturen het door naar jou en laten de betrokkene weten dat wij dat hebben gedaan.

Wij helpen je om zulke verzoeken te beantwoorden, met passende technische en organisatorische maatregelen en voor zover dat redelijkerwijs mogelijk is. In het OS kun je gegevens zelf inzien, aanpassen, exporteren en verwijderen; lukt dat niet, dan doen wij het op jouw verzoek.

Wij brengen voor deze hulp geen kosten in rekening, tenzij het gaat om herhaalde of buitensporige verzoeken die substantieel werk vragen; in dat geval melden wij de kosten vooraf.

7. Datalekken, DPIA en voorafgaande raadpleging

Ontdekken wij een inbreuk in verband met persoonsgegevens, dan melden wij dat zonder onredelijke vertraging en in elk geval binnen 24 uur na ontdekking bij jou, zodat jij binnen de 72 uur van artikel 33 AVG je eigen afweging kunt maken. Wij melden nooit zelf bij de toezichthouder namens jou, tenzij je ons daar schriftelijk om vraagt.

Onze melding bevat, voor zover bekend: wat er is gebeurd en wanneer, welke categorieën en hoeveel betrokkenen en records het vermoedelijk betreft, de waarschijnlijke gevolgen, de maatregelen die wij hebben genomen of voorstellen, en een contactpunt. Wat op dat moment nog niet bekend is, leveren wij na zodra wij het weten.

Wij houden een intern register bij van inbreuken, ook van die welke niet gemeld hoefden te worden, met de feiten, de gevolgen en de genomen maatregelen.

Moet jij een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren of de toezichthouder vooraf raadplegen, dan leveren wij de informatie over onze verwerking die je daarvoor nodig hebt.

8. Einde: teruggeven of wissen

Bij het einde van je account of opdracht kies jij wat er met de gegevens gebeurt: teruggeven in een gangbaar bestandsformaat, of wissen. Laat je binnen dertig dagen na het einde niets weten, dan wissen wij.

Wissen betekent bij ons: uit de actieve systemen binnen dertig dagen, en uit de back-ups zodra die volgens hun eigen cyclus aflopen, uiterlijk na negentig dagen. Zolang een gegeven nog in een back-up staat, wordt het niet meer gebruikt en niet meer getoond.

Wat een wet ons verplicht te bewaren, bewaren wij. Dat is in de praktijk de factuuradministratie, zeven jaar op grond van de Algemene wet inzake rijksbelastingen. Die gegevens worden alleen nog voor dat doel gebruikt.

Op jouw verzoek bevestigen wij het wissen schriftelijk.

9. Informatie en audit

Wij stellen je alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit artikel 28 AVG worden nagekomen, en werken mee aan audits, waaronder inspecties, door jou of door een door jou gemachtigde controleur.

In de praktijk beantwoorden wij vragenlijsten en leveren wij op verzoek een overzicht van onze maatregelen, ons subverwerkersregister en onze auditsporen. Wil je een audit ter plaatse of door een externe partij, dan kondig je die minstens dertig dagen van tevoren aan, vindt hij plaats tijdens kantooruren, verstoort hij onze dienstverlening niet, en is de controleur tot geheimhouding gehouden. Ten hoogste één audit per kalenderjaar is voor onze rekening; een volgende audit in hetzelfde jaar, of een audit die geen tekortkoming aantoont, komt voor jouw rekening tegen ons gebruikelijke uurtarief.

Bij een audit tonen wij nooit gegevens van andere klanten. Waar het maar even kan werken wij met geanonimiseerde of geaggregeerde bewijsstukken.

10. Doorgifte buiten de EER

Wij bewaren en verwerken jouw gegevens bij voorkeur binnen de Europese Economische Ruimte. De regio verschilt per dienst. PostHog gebruikt de EU-regio; de huidige Vercel-appfuncties draaien in de Verenigde Staten. Onze dienstverlening is daarom niet uitsluitend Europees.

Is doorgifte naar een derde land onvermijdelijk – dat speelt bij een aantal Amerikaanse leveranciers van modellen en infrastructuur – dan doen wij dat alleen op basis van een geldig mechanisme uit hoofdstuk V AVG: een adequaatheidsbesluit van de Europese Commissie, of de standaardcontractbepalingen (uitvoeringsbesluit (EU) 2021/914), aangevuld met een beoordeling van de omstandigheden in dat land en met aanvullende maatregelen waar die nodig zijn, zoals versleuteling onderweg en in rust en het zo klein mogelijk houden van wat er heen gaat.

Per subverwerker staat in bijlage C waar de gegevens staan en welk mechanisme geldt. Wijzig dat, dan werken wij die bijlage bij volgens artikel 5.

Bijlage A: gegevens en betrokkenen

Categorieën betrokkenen waarvan wij namens jou gegevens verwerken:

- jouw teamleden en de gebruikers van jouw werkruimte
- jouw klanten, leads en relaties, zoals ze in jouw Odoo of in het CRM staan
- mensen die reageren op je berichten, advertenties of formulieren
- bezoekers van de websites die wij voor je bouwen of beheren, voor zover jij daar gegevens verzamelt

Soorten persoonsgegevens:

- naam, functie, bedrijf, e-mailadres, telefoonnummer en adres
- correspondentie: berichten, reacties, e-mails en gespreksverslagen die jij in het OS zet of laat binnenkomen
- commerciële gegevens: offertes, orders, facturen, bedragen en statussen uit jouw Odoo
- accountgegevens: inlognaam, rol, taal, tijdstempels van gebruik
- technische gegevens: IP-adres, apparaat en browser, voor zover die bij een handeling worden vastgelegd
- beeld en tekst die jij aanlevert of laat maken en waarin mensen herkenbaar kunnen zijn

Bijzondere categorieën persoonsgegevens als bedoeld in artikel 9 AVG en strafrechtelijke gegevens als bedoeld in artikel 10 horen niet in SocialNow OS. Zet je ze er toch in, dan doe je dat op eigen verantwoordelijkheid en buiten de bedoeling van deze overeenkomst; wij treffen voor zulke gegevens geen aanvullende maatregelen omdat wij er niet op rekenen dat ze er zijn.

Bijlage B: beveiligingsmaatregelen

Toegang en identiteit:

- inloggen op je account gaat via een identiteitsdienst met tweestapsverificatie; beheerderstoegang van SocialNow gaat via een passkey en een tijdgebonden code
- toegang van een beheerder tot een klantomgeving verloopt via een briefje dat twee minuten geldig is en alleen dat ene systeem opent; het briefje zelf wordt nooit gelogd, de uitgifte wel
- rechten worden per werkruimte toegekend en bij vertrek ingetrokken

Versleuteling en sleutels:

- al het verkeer loopt over TLS; HTTP-verkeer wordt afgedwongen doorgestuurd naar HTTPS
- gegevens staan versleuteld op de opslag van onze leveranciers
- sleutels die jij invoert voor Odoo, Meta, Google of je socialkanalen worden versleuteld opgeslagen, nooit teruggetoond en nooit in logregels geschreven
- geheimen staan uitsluitend in de omgeving van de hostingleverancier, niet in de broncode

Scheiding en afscherming:

- elke klant heeft een eigen werkruimte; verzoeken worden per verzoek gecontroleerd op werkruimte en rol
- voor klanten met een eigen systeem draait een eigen omgeving met eigen geheimen, gescheiden van de andere
- de beheeromgeving is niet publiek bereikbaar en staat op noindex
- een strikt Content Security Policy beperkt welke scripts, stijlen en verbindingen een pagina mag gebruiken

Logging en detectie:

- handelingen met gevolgen – toegang verlenen, een systeem openen, een sleutel wijzigen – komen in een auditspoor met wie, wat en wanneer
- foutmeldingen en waarschuwingen worden centraal verzameld; persoonsgegevens worden daarin niet meegeschreven
- de bereikbaarheid en de inlogbeveiliging van elk klantsysteem worden doorlopend automatisch gecontroleerd

Continuïteit:

- opslag en herstel verlopen volgens de mogelijkheden van de gebruikte leverancier; frequentie, bewaartermijn en herstelbaarheid worden per gegevensbron vastgelegd
- de code staat in versiebeheer; elke publicatie is herleidbaar tot een commit en kan worden teruggedraaid
- voor publicatie draait een geautomatiseerde testsuite; een rode suite betekent niet publiceren

Organisatie:

- wie toegang heeft is een korte, bekende kring, allemaal onder geheimhouding
- nieuwe leveranciers worden beoordeeld op waar zij gegevens opslaan en op welke voorwaarden
- er is een vaste route voor het melden van kwetsbaarheden: security@socialnow.nl

Deze lijst beschrijft wat er op 19 september 2026 staat. Wij vervangen een maatregel alleen door een maatregel die minstens zo beschermend is.

Bijlage C: subverwerkers

Infrastructuur en opslag:

- Vercel Inc. (Verenigde Staten; regio afhankelijk van de dienst, appfuncties momenteel VS): hosting van het OS en de API
- Google Ireland Limited / Google LLC: Firebase voor de opslag van werkruimten en accounts
- Hostinger International Ltd (Litouwen): hosting van websites, domeinen en e-mail

Identiteit en communicatie:

- Google Ireland Limited: inloggen met een Google-account
- Hostinger International Ltd: verzending van e-mail vanuit het OS, waaronder inlogcodes

Metten:

- PostHog Inc., EU-datacentrum in Frankfurt: meten van gebruik van het OS, alleen na toestemming van de gebruiker, zonder schermopnames

Modellen voor tekst en beeld, alleen voor wat jij laat maken:

- Google Ireland Limited / Google LLC: Gemini voor tekst en beeld
- OpenAI Ireland Ltd: modellen voor tekst en beeld
- Anthropic PBC (Verenigde Staten): modellen voor tekst
- Higgsfield: beeld en film
- Bij al deze partijen is contractueel uitgesloten dat jouw invoer wordt gebruikt om hun modellen te trainen.

Publiceren op sociale kanalen:

- Zernio: het koppelen aan en publiceren op jouw eigen socialkanalen, met de sleutel die jij zelf aansluit

Wij hebben met elk van deze partijen een verwerkersovereenkomst of gelijkwaardige voorwaarden. Bij partijen buiten de EER berust de doorgifte op de standaardcontractbepalingen van de Europese Commissie, en waar van toepassing op het EU-VS Data Privacy Framework.

Deze lijst geldt op 19 september 2026. Wijzigingen worden dertig dagen vooraf aangekondigd volgens artikel 5.

BIJLAGE D

Bronnen, versie en onderhoud

Versie 1.0, samengesteld op 13 oktober 2026. De hoofdstukken zijn uitleg op basis van de hieronder genoemde publieke bronnen. De brondata is bewaard naast het opmaakschrift zodat deze uitgave reproduceerbaar is. De oorspronkelijke beleidsdatums staan bij de uittreksels. Controleer veranderingen in diensten en beleid voordat je dit document als inkoopbewijs gebruikt.

Bron: [Algemene voorwaarden](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Privacybeleid](#) · Laatst bijgewerkt: 20 september 2026

Bron: [Beveiliging](#) · Laatst bijgewerkt: 19 september 2026

Bron: [Verwerkersovereenkomst](#) · Laatst bijgewerkt: 19 september 2026

[Veiligheid en sleutelbelofte](#)

[Responsible disclosure](#)

[AP: beveiliging van persoonsgegevens](#)

[AP: verwerkersovereenkomst](#)

[AP: melding van een datalek](#)

Wat deze versie niet toevoegt

Geen nieuwe garantie, nieuw serviceniveau, gewijzigde overdracht van intellectuele eigendomsrechten of wijziging van een ondertekende overeenkomst. Geen aanspraak op niet-bestaande certificeringen en geen claim dat iedere verwerking uitsluitend in de EU plaatsvindt.

Wanneer bijwerken

Bij een wijziging van leverancier, regio, inlogroute, AI-configuratie, bewaartermijn, exportmogelijkheid of contractueel beleid. Werk eerst de onderliggende beleidsbron bij en maak daarna een nieuwe versie van dit handboek. Gebruik voor nieuwe afspraken altijd de actuele overeenkomsten.