

Privacyverklaring Inkoper.io

Laatst bijgewerkt: 7 februari 2025

Deze Privacyverklaring (ook 'Privacybeleid' genoemd) beschrijft Onze beleidslijnen en procedures over de verzameling, het gebruik en de openbaarmaking van Uw informatie wanneer U de Dienst gebruikt en informeert U over Uw privacyrechten en hoe de wet U beschermt. We gebruiken Uw Persoonlijke gegevens om de Dienst te leveren en te verbeteren. Door de Dienst te gebruiken, stemt U in met de verzameling en het gebruik van informatie in overeenstemming met dit Privacybeleid.

1. Algemene informatie

1.1 Persoonsgegevens

"*Persoonsgegevens*" betreft elke vorm van informatie die betrekking heeft op een geïdentificeerde of identificeerbare persoon. Voor de doeleinden van de AVG betekent Persoonsgegevens elke informatie met betrekking tot U zoals een naam, een identificatienummer, locatiegegevens, online indicator of één of meer factoren specifiek voor de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit.

1.2 Juridisch

Naast dit Privacybeleid is uw gebruik van onze Diensten ook onderworpen aan andere juridische documentatie zoals de Algemene voorwaarden, beschikbaar op onze website (www.inkoper.io).

2. Interpretatie en Definities

2.1 Interpretatie

De woorden waarvan de eerste letter met een hoofdletter is geschreven hebben betekenissen gedefinieerd onder de volgende voorwaarden. De volgende definities zullen dezelfde betekenis hebben, ongeacht of ze in enkelvoud of meervoud staan.

2.2 Definities

- *Applicatie* betekent de Diensten en Service van inkoper.io geleverd door de Leverancier, door U te benaderen via e-mail. De Applicatie biedt inkoop en juridisch advies op het gebied van aanbestedingsrecht.
- *Bedrijf* (verwezen als "het Bedrijf", "Wij", "Ons" of "Onze" in deze Overeenkomst) verwijst naar inkoper.io, in oprichting, adres en KvK-nummer zullen op een later tijdstip worden verstrekt. Voor het doel van de AVG is het Bedrijf de Verwerkingsverantwoordelijke.
- *Land* verwijst naar Nederland.
- *Verwerkingsverantwoordelijke*, voor de doeleinden van de AVG (Algemene Verordening Gegevensbescherming), verwijst naar het Bedrijf als de rechtspersoon die alleen of

gezamenlijk met anderen de doeleinden en middelen van de verwerking van Persoonsgegevens bepaalt.

- *Apparaat* betekent elke desktop.
- *Dienst* verwijst naar de Applicatie.
- *Dienstverlener* betekent elke natuurlijke of rechtspersoon die de gegevens namens het Bedrijf verwerkt. Het verwijst naar externe bedrijven of personen die door het Bedrijf in dienst zijn genomen om de Dienst te vergemakkelijken, om de Dienst namens het Bedrijf te leveren, om diensten te verrichten die verband houden met de Dienst of om het Bedrijf te assisteren bij het analyseren van hoe de Dienst wordt gebruikt. Voor het doel van de AVG worden Dienstverleners beschouwd als Gegevensverwerkers.
- *Gebruiksgegevens* verwijst naar gegevens die automatisch worden verzameld door gebruik van de Dienst.
- *U* betekent de persoon die toegang heeft tot of gebruik maakt van de Dienst, of het bedrijf, of andere rechtspersoon namens welke zo'n persoon toegang heeft tot of gebruik maakt van de Dienst, zoals van toepassing. Onder de AVG (Algemene Verordening Gegevensbescherming) kunt U worden aangeduid als de betrokkene of als de gebruiker, aangezien u de persoon bent die de Dienst gebruikt.

3. Verzameling, Gebruik en Beveiliging van Uw Persoonsgegevens

3.1 Persoonsgegevens

Tijdens het gebruik van Onze Dienst, kunnen wij U vragen Ons bepaalde persoonlijk identificeerbare informatie te verstrekken die gebruikt kunnen worden om contact met u op te nemen of u te identificeren. Het gaat hierbij om de volgende soorten persoonsgegevens:

- Voornaam en achternaam
- E-mailadres
- Bankrekeningnummer
- Functietitel
- Organisatienaam van Uw werkgever (indien van toepassing)
- Eventueel door U geleverde data

3.2 Gebruik van Uw Persoonsgegevens

Het Bedrijf kan Persoonsgegevens gebruiken voor de volgende doeleinden:

- Om onze Dienst te leveren, te onderhouden en te updaten.
 - Wij gebruiken de bovenstaand genoemde persoonsgegevens om onze dienstverlening aan U te kunnen uitvoeren.
- Om contact met u op te nemen.

- Mogelijk willen Wij met U contact opnemen, dit kan bijvoorbeeld om U te helpen wanneer de dienst niet naar behoren werkt, maar kan ook om commerciële doeleinden gebeuren. Tevens nemen wij contact met U op om feedback over onze dienst te vragen of om U meer informatie te verschaffen over onze dienst.
- Voor bedrijfsoverdrachten.
 - Wij kunnen Uw persoonsgegevens gebruiken om een fusie, overname, herstructurering of verkoop van een deel of al onze activa of passiva te evalueren of uit te voeren.

Uw persoonsgegevens kunnen in de volgende situaties worden gedeeld:

- Met Dienstverleners.
 - Wij kunnen uw persoonsgegevens delen met dienstverleners om het gebruik van onze dienst te monitoren en analyseren, voor betalingsverwerking of om contact met u op te nemen.
- Voor bedrijfsoverdrachten.
 - Wij kunnen Uw persoonsgegevens gebruiken om een fusie, overname, herstructurering of verkoop van een deel of al onze activa of passiva te evalueren of uit te voeren.
- Met uw toestemming.
 - Met Uw toestemming kunnen wij Uw persoonsgegevens delen.
- Indien vereist door de wet en soortgelijke bekendmakingen.
 - Wij kunnen uw Persoonsgegevens inzien, bewaren en openbaar maken als wij van mening zijn dat dit vereist of gepast is om: (i) te voldoen aan wetshandavingsverzoeken en juridische procedures, zoals een gerechtelijk bevel of dagvaarding; (ii) reageren op uw verzoeken; of (iii) de rechten, eigendommen of veiligheid van u, onze of anderen te beschermen.

3.3 Beleid inzake gegevensinbreuken

Het Bedrijf doet er alles aan om haar systemen en de website te beveiligen tegen ongeoorloofd gebruik en verlies of diefstal van persoonsgegevens. Het is onmogelijk om elk ongeoorloofd gebruik en elk accidenteel verlies van persoonsgegevens volledig uit te sluiten.

Als toezichthouder wordt de Autoriteit Persoonsgegevens binnen de wettelijke termijn geïnformeerd als er sprake is van een datalek, als dit ernstig is. Als er sprake is van een datalek, wordt dit direct aan de betrokkenen gemeld indien er sprake is van een hoog risico voor de bescherming van persoonsgegevens en de privacy van de betrokkenen. Elk datalek wordt door ons gedocumenteerd.

3.4 Bewaring van Uw Persoonsgegevens

Het Bedrijf bewaart uw Persoonsgegevens slechts zo lang als nodig is voor de doeleinden uiteengezet in dit Privacybeleid. We zullen uw persoonlijke gegevens bewaren en gebruiken voor zover dit nodig is om te voldoen aan onze wettelijke verplichtingen (bijvoorbeeld als we uw gegevens moeten

bewaren om te voldoen aan de toepasselijke wetgeving), geschillen op te lossen en onze overeenkomsten en ons beleid af te dwingen.

Het Bedrijf bewaart Gebruiksgegevens ook voor interne analysedoeleinden. Gebruiksgegevens worden over het algemeen voor een kortere periode bewaard, behalve wanneer deze gegevens worden gebruikt om de veiligheid te versterken of om de functionaliteit van Onze Dienst te verbeteren, of als Wij wettelijk verplicht zijn deze gegevens voor langere tijd te bewaren.

3.5 Overdracht van Uw Persoonsgegevens

Uw informatie, inclusief Persoonsgegevens, wordt verwerkt binnen de grenzen van de Europese Unie. Dit betekent dat uw gegevens niet worden overgedragen naar computers die zich buiten de Europese Unie bevinden. Het Bedrijf zal alle stappen ondernemen die redelijkerwijs nodig zijn om ervoor te zorgen dat uw gegevens veilig en in overeenstemming met dit Privacybeleid worden behandeld.

3.6 Openbaarmaking van Uw Persoonsgegevens

- Zakelijke transacties

Als het bedrijf betrokken is bij een fusie, overname of verkoop van activa of passiva, kunnen uw persoonlijke gegevens worden overgedragen. Wij zullen u hiervan op de hoogte stellen voordat uw persoonlijke gegevens worden overgedragen en onderworpen worden aan een ander privacybeleid.

- Wettelijke verplichting

Onder bepaalde omstandigheden kan het Bedrijf verplicht zijn om uw Persoonsgegevens openbaar te maken als dit wettelijk verplicht is of als reactie op geldige verzoeken van overheidsinstanties (bijvoorbeeld een rechtbank of een overheidsinstantie).

Het Bedrijf kan uw Persoonsgegevens openbaar maken als het te goeder trouw van mening is dat een dergelijke actie noodzakelijk is om:

- Te voldoen aan een wettelijke verplichting
- De rechten of eigendom van het bedrijf te verdedigen of beschermen
- Mogelijke misstanden in verband met de Dienst te voorkomen of onderzoeken
- De persoonlijke veiligheid van gebruikers van de dienst of het publiek te beschermen

3.7 Beveiliging van Uw Persoonsgegevens

Het Bedrijf beschouwt de bescherming van zijn gegevens, inclusief Uw persoonsgegevens, van groot belang. Daarom hebben wij verschillende organisatorische en technische maatregelen genomen, waaronder:

Onderstaande beschrijving geeft een overzicht van de belangrijkste beveiligingsmaatregelen die Het Bedrijf heeft getroffen om persoonsgegevens te beschermen. Hiertoe worden de voornaamste principes van de ISO 27001 norm toegepast als richtsnoer voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens.

1. Beveiligingsbeleid en organisatie

- Toewijzing van verantwoordelijkheden: De directie heeft formele eindverantwoordelijkheid voor informatiebeveiliging. Daarnaast is er een aangewezen coördinator die toezicht houdt op de naleving van de beveiligingsrichtlijnen.
- Beveiligingsbeleid: Er gelden interne richtlijnen voor correct gebruik van systemen, omgang met gegevens en verantwoordelijkheden van medewerkers.

2. Classificatie van gegevens

- Classificatie: Persoonsgegevens en andere gevoelige informatie worden geclassificeerd op basis van vertrouwelijkheid. Waar passend wordt encryptie ingezet voor opslag en/of overdracht.
- Verwijdering en dataminimalisatie: Verouderde en niet langer noodzakelijke data worden periodiek gewist of geanonimiseerd volgens interne richtlijnen en wettelijke verplichtingen.

3. Toegangsbeveiliging

- Autorisatiemodel: Medewerkers krijgen alleen toegang op basis van hun functie ("least privilege"). Toegang tot productie-omgevingen en gevoelige data is beperkt en wordt waar mogelijk gelogd.
- Sterke authenticatie: Wachtwoorden moeten voldoen aan minimale complexiteitseisen en worden regelmatig gewijzigd. Er is voor kritieke systemen waar mogelijk Multi-Factor Authentication (MFA) ingesteld.
- Gebruikersbeheer: Uitdiensttredende medewerkers of externe contractanten verliezen direct hun toegang.

4. Cryptografie en databeveiliging

- Encryptie: Data in transit worden, waar redelijkerwijs mogelijk, versleuteld. Gevoelige data in rust worden op afgeschermd systemen opgeslagen met encryptie.
- Sleutelbeheer: Encryptiesleutels worden versleuteld en centraal beheerd. Uitsluitend geautoriseerde medewerkers hebben toegang tot deze sleutels.

5. Fysieke beveiliging

- Toegangscontrole: Kantoor- en serverruimtes zijn alleen toegankelijk voor geautoriseerd personeel.
- Bescherming tegen externe risico's: Er zijn basismaatregelen tegen brand, waterschade en stroomuitval getroffen.

6. Operationele beveiliging en netwerkomgeving

- Patch management: Besturingssystemen, middleware, frameworks en applicaties worden up-to-date gehouden met de nieuwste beveiligingspatches en updates.
- Malwarebescherming: Alle bedrijfsapparaten zijn voorzien van antivirussoftware of endpoint-beveiligingsoplossingen en worden periodiek gescand.
- Monitoring en logging: Kritieke systemen en applicaties worden gemonitord; relevante gebeurtenissen worden gelogd en beveiligd opgeslagen. Logs worden periodiek geanalyseerd op verdachte activiteiten.
- Back-ups: Er worden periodieke back-ups gemaakt van kritieke systemen en data. Deze back-ups worden getest.

7. Ontwikkeling en onderhoud

- Veilig ontwikkelproces: Het Bedrijf volgt, voor zover van toepassing, veilige ontwikkelrichtlijnen. Code wordt vóór implementatie gereviewd en geautomatiseerde tests worden uitgevoerd.
- Scheiding omgevingen: Er is een duidelijke scheiding tussen ontwikkel-, test- en productieomgevingen. Productie persoonsgegevens worden niet gebruikt in testomgevingen zonder dat deze geanonimiseerd zijn.

- Release management: Nieuwe releases en updates worden getest en gedocumenteerd; er is een rollback-procedure om bij fouten terug te schakelen naar een stabiele versie.

8. Incidentmanagement en datalekken

- Procedure: Er is een interne procedure voor het melden, registreren, onderzoeken en evalueren van incidenten en datalekken.
- Meldplicht: Bij (vermoeden van) een datalek dat risico's inhoudt voor de rechten en vrijheden van betrokkenen, meldt de Verwerker het incident binnen de wettelijke termijnen bij de verwerkingsverantwoordelijke en de toezichthouder (indien nodig).

10. Bewustwording en training

- Security awareness: Medewerkers volgen periodiek awareness-sessies over informatiebeveiliging.
- Geheimhoudingsverplichtingen: Alle medewerkers en ingehuurd krachten ondertekenen een geheimhoudingsverklaring.

Het Bedrijf streeft naar continue verbetering van zijn beveiliging op basis van risicoanalyses, interne controles en best practices. De beveiliging van Uw Persoonsgegevens is belangrijk voor ons, maar geen enkele methode van verzending via internet of methode van elektronische opslag is 100% veilig. Terwijl we streven naar volledige bescherming van Uw Persoonsgegevens, kunnen we de absolute veiligheid ervan niet garanderen omdat wij hiervoor ook afhankelijk zijn van andere serviceproviders zoals hieronder verder uiteengezet.

4. Gedetailleerde informatie over de verwerking van uw persoonsgegevens

De serviceproviders die wij gebruiken, kunnen toegang hebben tot uw persoonlijke gegevens. Deze externe leveranciers verzamelen, bewaren, gebruiken, verwerken en dragen informatie over Uw activiteit op onze dienst over in overeenstemming met hun eigen privacybeleid.

4.1 Communicatieproviders

Wij kunnen Uw e-mailadres, voor- en achternaam en organisatienaam van Uw werkgever gebruiken om direct (via e-mail contact) of indirect (via onze website) met U te communiceren. Dit contact kan als doel verbetering of het faciliteren van Onze dienst hebben. We kunnen deze persoonsgegevens delen met de volgende communicatiedienstverleners om contact faciliteren.

- ActiveCampaign: privacybeleid is te bekijken op: <https://www.activecampaign.com/legal/privacy-policy>
- Make.com: privacybeleid is te bekijken op: <https://www.make.com/en/privacy-notice>
- Wordpress: privacybeleid is te bekijken op <https://nl.wordpress.org/about/privacy/>

4.2 Infrastructuuraanbieder

We gebruiken de externe dienst OpenAI om ons te voorzien van de digitale infrastructuur van ons bedrijf. We kunnen Uw functietitel en e-mailadres delen met OpenAI.

- Meer informatie over hun beveiligingsmaatregelen is te vinden op: <https://openai.com/policies/privacy-policy>

4.3 Juridische basis voor de verwerking van persoonsgegevens onder de AVG

We kunnen de persoonsgegevens verwerken onder de volgende voorwaarden:

- Toestemming: U heeft uw toestemming gegeven voor de verwerking van persoonsgegevens voor een of meer specifieke doeleinden.
- Uitvoering van een contract: Het verstrekken van persoonsgegevens is noodzakelijk voor de uitvoering van een overeenkomst met U en/of voor eventuele precontractuele verplichtingen daarvan.
- Wettelijke verplichtingen: De verwerking van persoonsgegevens is noodzakelijk om te voldoen aan een wettelijke verplichting waaraan het bedrijf onderhevig is.
- Vitale belangen: De verwerking van persoonsgegevens is noodzakelijk om Uw vitale belangen of die van een andere natuurlijke persoon te beschermen.
- Openbare belangen: De verwerking van persoonsgegevens heeft betrekking op een taak die wordt uitgevoerd in het openbaar belang of in de uitoefening van een officiële autoriteit die aan het bedrijf is verleend.
- Legitieme zakelijke belangen: zoals effectief en efficiënt beheer en beheer van de werking van ons bedrijf; naleving van interne beleidslijnen en procedures; het monitoren van het gebruik van onze auteursrechtelijk beschermde materialen; het mogelijk maken van snelle en gemakkelijke toegang tot informatie over onze diensten; het sturen van e-mailupdates over onze diensten, nieuws, aankomende evenementen en andere marketing- of promotiematerialen.

In elk geval zal het Bedrijf U graag helpen om de specifieke juridische basis te verduidelijken die van toepassing is op de verwerking, en in het bijzonder of het verstrekken van persoonsgegevens een wettelijke of contractuele verplichting is, of een vereiste die nodig is om een contract aan te gaan.

4.4 Uw rechten onder de AVG

Het Bedrijf verbindt zich ertoe de vertrouwelijkheid van uw persoonsgegevens te respecteren en te garanderen dat U Uw rechten kunt uitoefenen. Neem contact op met de contactpersoon om Uw rechten uit te oefenen. U heeft het recht onder dit Privacybeleid, en volgens de wet als U zich binnen de EU bevindt, om:

- Toegang aanvragen tot Uw Persoonsgegevens. Het recht om toegang te krijgen tot, bij te werken of de informatie die we over U hebben te verwijderen.
- Correctie aanvragen van de persoonsgegevens die we over U hebben. U heeft het recht om eventuele onvolledige of onjuiste informatie die we over U hebben te laten corrigeren.
- Bezwaar maken tegen de verwerking van uw persoonsgegevens. Dit recht bestaat wanneer we vertrouwen op een legitiem belang als de juridische basis voor onze verwerking en er is iets met betrekking tot Uw specifieke situatie, waardoor U bezwaar wilt maken tegen onze verwerking van uw persoonsgegevens op deze grond. U heeft ook het recht om bezwaar te maken wanneer we uw persoonsgegevens verwerken voor marketing doeleinden.

- Verzoek tot wissen van Uw persoonsgegevens. U heeft het recht om ons te vragen persoonsgegevens te verwijderen of te verwijderen wanneer er geen goede reden is voor ons om deze te blijven verwerken.
- Verzoek tot overdracht van Uw persoonsgegevens. Wij zullen U, of een door U gekozen derde partij, Uw persoonsgegevens verstrekken in een gestructureerd, algemeen gebruikt, machineleesbaar formaat. Let op: dit recht is alleen van toepassing op geautomatiseerde informatie waarvoor U aanvankelijk toestemming heeft gegeven voor ons gebruik of waarbij we de informatie hebben gebruikt om een contract met U uit te voeren.
- Uw toestemming intrekken. U heeft het recht om Uw toestemming voor het gebruik van Uw Persoonsgegevens in te trekken. Als U Uw toestemming intrekt, kunnen we U mogelijk geen toegang geven tot bepaalde specifieke functionaliteiten van de dienst.

4.5 Uitoefening van uw AVG-gegevensbeschermingsrechten

U kunt Uw rechten op toegang, rectificatie, annulering en verzet uitoefenen door contact met ons op te nemen. Houd er rekening mee dat we U kunnen vragen om uw identiteit te verifiëren voordat we op dergelijke verzoeken reageren. Als U een verzoek indient, zullen we ons best doen om zo snel mogelijk op U te reageren. Als U van mening bent dat Uw rechten worden geschonden, heeft U het recht om een klacht in te dienen bij de toezichthoudende autoriteit. Dit is de Autoriteit Persoonsgegevens. U kunt de klacht per post indienen of via de website van de Autoriteit Persoonsgegevens. De volgende informatie is van toepassing per post. Autoriteit Persoonsgegevens Postbus 93374 2509 AJ Den Haag

We willen U erop wijzen dat we het op prijs stellen als u eerst een klacht bij ons indient (zie contactgegevens). We lossen de klacht graag samen met U op.

5. Privacy van Kinderen

Onze Dienst is niet gericht op personen jonger dan 18 jaar. We verzamelen niet bewust persoonlijke identificeerbare informatie van iemand onder de leeftijd van 18 jaar. Als U een ouder of voogd bent en U zich bewust bent dat uw kind ons persoonlijke gegevens heeft verstrekt, neem dan contact met ons op. Als we ons ervan bewust worden dat we persoonlijke gegevens hebben verzameld van iemand onder de leeftijd van 18 jaar zonder verificatie van ouderlijke toestemming, nemen we stappen om die informatie van onze servers te verwijderen.

6. Links naar andere websites

Onze Dienst kan links bevatten naar andere websites die niet door ons worden beheerd. Als U op een link van derden klikt, wordt U doorverwezen naar de site van die derde partij. We adviseren U dringend om het Privacybeleid van elke site die u bezoekt te bekijken. Wij hebben geen controle over en nemen geen verantwoordelijkheid voor de inhoud, het privacybeleid of de praktijken van websites of diensten van derden.

7. Wijzigingen in dit Privacybeleid

We kunnen ons Privacybeleid van tijd tot tijd bijwerken. We zullen U op de hoogte stellen van eventuele wijzigingen door het nieuwe Privacybeleid op deze pagina te plaatsen. We updaten de "Laatst bijgewerkt" datum bovenaan dit Privacybeleid zodra er een wijziging heeft plaatsgevonden. We adviseren U om dit Privacybeleid periodiek te herzien op eventuele wijzigingen. Wijzigingen in dit Privacybeleid zijn effectief wanneer ze op deze pagina worden geplaatst.

8. Contact

Als U vragen heeft over dit Privacybeleid, kunt U contact met ons opnemen via e-mail:
timo@martoconsul.com