

Algemene Voorwaarden

Digidentity Identiteitsdiensten

Titel	Algemene Voorwaarden – Digidentity Identiteitsdiensten
Datum	25 maart 2019
Ingangsdatum	12 April 2019
Versie	2019-v1
Classificatie	Public

1. Over Digidentity

- a) Digidentity BV is een geregistreerde naamloze vennootschap in Nederland, met KvK-nummer 27322631, gevestigd aan de Waldorpstraat 17P, 2521 CA, Den Haag, Nederland.
- b) Als je vragen hebt over de dienstverlening, kan je onze website www.digidentity.eu bezoeken of contact met ons opnemen via:

Receptie: +31 (0)887 78 78 78

Service Desk NL: +31 (0)887 78 78 88

Service Desk UK: +44 (0)330 05 83 454

of

Nederlandstalige Service Desk: helpdesk@digidentity.eu

Engelstalige Service Desk: helpdesk@digidentity.co.uk

2. Contract & Toepassingsgebied

- a) Digidentity levert producten en diensten voor identiteitsbeheer en identiteitsverificatie. Digidentity is een Trust Service Provider voor de uitgifte en het beheer van EU gekwalificeerde en geavanceerde certificaten, email certificaten en servercertificaten.
- b) Dit zijn de Algemene Voorwaarden van Digidentity B.V. Deze Algemene Voorwaarden zijn van toepassing op alle producten en diensten van Digidentity.
- c) Deze Algemene Voorwaarden vormen de basis van de bindende overeenkomst tussen jou (persoon of organisatie) en Digidentity B.V. De Algemene Voorwaarden sluiten alle andere Algemene Voorwaarden uit. In aanvulling op deze Algemene Voorwaarden is het mogelijk dat je product specifieke voorwaarden moet accepteren. Indien van toepassing, maken wij deze specifieke voorwaarden tijdens het registratie/aanvraagproces beschikbaar.
- d) Deze Algemene Voorwaarden zijn van toepassing op alle aspecten van de relatie en het contract tussen jou en Digidentity, tenzij Digidentity uitdrukkelijk schriftelijk anders is overeengekomen. De onvoorwaardelijke aanvaarding en instemming met deze Algemene Voorwaarden zijn impliciet.
- e) Voordat je je kan registreren voor een product en/of service, moet je deze Algemene Voorwaarden lezen en expliciet mee akkoord gaan. Om deze Algemene Voorwaarden juridisch te accepteren, moet je de wettelijke leeftijd hebben bereikt in het land waar je woont. Dit betekent dat je juridisch een bindend contract kunt aangaan.

- f) De Algemene Voorwaarden blijven van toepassing ongeacht of het aanvraagproces en/of de verificatie van jouw identiteit succesvol is.
- g) Digidentity behoudt zich het recht voor deze Algemene Voorwaarden te allen tijde te wijzigen. De gewijzigde versie is van toepassing zodra Digidentity deze op de website heeft gepubliceerd. Nadat de Algemene Voorwaarden zijn gewijzigd, dien je deze lezen en accepteren bij het volgende gebruik van jouw account.
- h) Als je niet akkoord gaat met gewijzigde of herziene Algemene Voorwaarden van Digidentity, kan je de Digidentity Identity Services niet langer gebruiken. In dat geval kan je contact opnemen met de Servicedesk om jouw account te deactiveren. Je kan je account binnen 30 dagen na de-activatie opnieuw activeren door je aan te melden en de voorwaarden te accepteren. Na 30 dagen na de-activatie, word je account verwijderd.

3. Onze Diensten

- a) Wanneer je je registreert voor een product, moet je een account aanmaken. Het verificatieproces begint bij het starten van de registratie en omvat de validatie en verificatie van de documenten en gegevens die je en andere bronnen hebben verstrekt.
- b) Om het registratieproces te voltooien, moet je alle vereiste gegevens verstrekken. Als je niet alle vereiste gegevens verstrekt, is het niet mogelijk om jouw identiteit en/of organisatie te verifiëren en kunnen wij je het gewenste product niet leveren.
- c) Als het registratieproces succesvol is, zal Digidentity het product beschikbaar stellen via het gebruik van/of in jouw account en is het registratieproces voltooid.
- d) Als het registratieproces geen bevestiging en/of verificatie tot gevolg heeft, wordt de aanvraag afgewezen en wordt het product niet voor je beschikbaar gemaakt.
- e) De beslissing om aanvragen van producten en diensten van Digidentity goed of af te keuren blijft te allen tijde het recht van Digidentity B.V.

4. Producten

- a) Bij Digidentity kan je je registreren voor de producten op onze website, waarop deze Algemene Voorwaarden van toepassing zijn.

- b) Het gebruik van onze diensten wordt beschreven in deze Algemene Voorwaarden, product specifieke voorwaarden en onze Certificate Practice Statement (CPS).

5. Productgeldigheid

- a) Voor GOV.UK Verify-accounts is het noodzakelijk om de gebruikers opnieuw te valideren binnen 180 dagen na de eerste registratie. Als deze validatie succesvol is, vindt geen verdere validatie plaats en blijft het account actief tenzij een verzoek tot deactivatie of verwijdering is gedaan. Tijdens het verlengingsproces kunnen wij gebruikers van GOV.UK Verify vragen om een nieuw identiteitsbewijs te verstrekken.
- b) Voor eHerkenning geldt een eerste contractperiode van twaalf (12) maanden. Na verloop van twaalf (12) maanden verlengen wij het contract automatisch met twaalf (12) maanden en is het contract maandelijks opzegbaar.
- c) SSL/SBR-certificaten uit de PKI Private root zijn drie (3) jaar geldig. Zodra het certificaat is verlopen, is een nieuwe aanvraag vereist. Digidentity verlengt geen bestaande certificaten maar geeft een nieuw certificaat uit.
- d) SSL-certificaten uit de PKI publieke root zijn twee (2) jaar geldig. Zodra het certificaat is verlopen, is een nieuwe aanvraag vereist. Digidentity verlengt geen bestaande certificaten, maar geeft een nieuw certificaat uit.
- e) Voor eSGN-certificaten (gekwificeerd en geavanceerd) geldt een eerste contractperiode van twaalf (12) maanden. Na verloop van twaalf (12) maanden verlengen wij het contract automatisch met twaalf (12) maanden en is het contract maandelijks opzegbaar.
- f) Voor Beroepscertificaten geldt een eerste contractperiode van twaalf (12) maanden. Na verloop van twaalf (12) maanden verlengen wij het contract automatisch met twaalf (12) maanden en is het contract maandelijks opzegbaar.
- g) Accounts en/of contracten kunnen niet worden overgedragen. Aanvragers, persoonlijk of als organisatie, moeten zich voor hun eigen rekening registreren.

6. Kennisgeving aan Vertrouwende Partijen

- a) Digidentity adviseert vertrouwende partijen de geldigheid of intrekking van de certificaten verifiëren met behulp van de actuele intrekkingstatusinformatie.

- b) Digidentity adviseert vertrouwende partijen rekening houden met eventuele beperkingen van het gebruik van het certificaat die zijn beschreven in de Algemene Voorwaarden, de Certificate Practice Statement of in het certificaat.
- c) Digidentity adviseert Vertrouwende Partijen de voorzorgsmaatregelen te nemen die zijn voorgeschreven in overeenkomsten en andere documenten.
- d) Digidentity adviseert Vertrouwende Partijen de geldigheid van certificaten controleren via de volledige certificaatketen naar het vertrouwde root certificaat.

7. Verificatie Persoonsgegevens

- a) Om een account te registreren, vragen wij om bewijs om jouw identiteit vast te stellen. Het bewijsmateriaal dat je verstrekt, gebruiken wij om jouw persoonsgegevens te verifiëren. Het gevraagde bewijsmateriaal kan zijn:
 - i. Identiteitsdocument via de mobiele app - paspoort of nationale identiteitskaart
 - ii. Selfies via de mobiele app
 - iii. Transactie zonder kosten met een creditcard of betaalpas (voor GOV.UK Verify)
 - iv. Uw mobiele telefoonnummer
 - v. Persoonlijke identificatie door een Digidentity-vertegenwoordiger
 - vi. Emailadres
 - vii. Privé-adres (voor GOV.UK Verify)
 - viii. Geboortedatum
 - ix. Adresgeschiedenis (voor GOV.UK Verify)
 - x. Naam geschiedenis (voor GOV.UK Verify)
 - xi. Beroepsregistratienummer voor beroepscertificaten.
- b) Digidentity zal alleen de gegevens opvragen die nodig is om jouw identiteit te creëren en verifiëren.
- c) Digidentity is verplicht om periodiek uw bestaande gegevens te valideren bij de instanties die de gegevens beheren. Dit is nodig om te zorgen dat Digidentity beschikt over actuele en juiste gegevens met als door identiteitsverificatie uit te voeren.
- d) Elk afgegeven authenticatiecertificaat mag niet worden beschouwd als een vorm van een document voor wettelijke identificatie volgens de WID (Wet Identification - Nederlandse Identificatiecode).

Legale identificatie kan alleen worden aangetoond door het verstrekken van een erkend ID-document.

- e) Digidentity verifieert een aanvraag voor een beroepscertificaat bij de Nederlandse Beroepsorganisatie voor Accountants (NBA).

8. Verificatie Organisatiegegevens

- a) Als jouw registratie/aanvraag namens een organisatie is, of met toestemming van een organisatie zal Digidentity, indien van toepassing, de volgende gegevens opvragen;
 - i. Registratienummer van de Kamer van Koophandel (Nederlands KVK-nummer)
 - ii. Gegevens van het organisatieadres
 - iii. Organisatie emailadres
 - iv. Validatie van de Fully Qualified Domain Name (FQDN)
 - v. Controle van domeinnaam op zwarte lijst/phishing-lijst
 - vi. Kopie identiteitsdocument van eigenaar/directeur/wettelijke vertegenwoordiger
 - vii. Autorisatie voor de persoon die het certificaat aanvraagt
 - viii. Brief met bevestiging dat aanvrager voor de organisatie werkt
- b) Digidentity zal alleen de gegevens opvragen die nodig is om de identiteit van de organisatie en de wettelijke vertegenwoordiging te verifiëren.
- c) Digidentity zal geen certificaten en/of andere producten uitgeven als de organisatie zich in een faillissementsprocedure bevindt of niet langer bij de Kamer van Koophandel is geregistreerd.
- d) Digidentity geeft alleen certificaten uit aan wettelijke vertegenwoordiger(s) met de juiste machtigingen om namens een organisatie een contract aan te gaan.
- e) Als het register van de Kamer van Koophandel gezamenlijke wettelijke vertegenwoordiging vermeldt, zal Digidentity zonder uitzondering toestemming vragen aan alle wettelijke vertegenwoordigers die in het register zijn vermeld.
- f) Elk afgegeven authenticatiecertificaat mag niet worden beschouwd als een vorm van een document voor wettelijke identificatie volgens de WID. Wettelijke identificatie kan alleen worden aangetoond door erkend identiteitsdocument (paspoort of identiteitskaart).

9. Certificaatacceptatie

- a) Het certificaat wordt geacht te zijn aanvaard door de abonnee wanneer een periode van meer dan één (1) kalendermaand is verstreken zonder dat enige communicatie is ontvangen van de abonnee (persoon of organisatie), of dat het certificaat is gedownload, gebruikt en/of geïnstalleerd.

10. Deactiveren, verwijderen en intrekken

- a) Je kan je account op ieder gewenst moment deactiveren met de link "Deactiveer mijn account" in je account. Gedurende een periode van 30 dagen is de account gedeactiveerd zoals beschreven in onze Certificate Practice Statement. Je kan je account of de producten in het account niet gebruiken als de account gedeactiveerd is.

Je kan je account opnieuw activeren door binnen 30 dagen na deactivering, in te loggen. Als je het account niet binnen die 30 dagen opnieuw hebt geactiveerd, worden het account en alle persoonsgegevens verwijderd en worden alle aan uitgegeven certificaten ingetrokken. Records worden opgeslagen in overeenstemming met toepasselijke wet- en regelgeving.

- b) Je kan je account op ieder gewenst moment verwijderen met de link "Verwijder mijn account " in je account. Digidentity zal jouw account en persoonsgegevens permanent uit onze systemen verwijderen. Alle certificaten die aan je zijn uitgegeven, worden ingetrokken. Records worden opgeslagen in overeenstemming met toepasselijke wet- en regelgeving.
- c) Je kan certificaten zelf intrekken door je aan te melden bij jouw identiteitsaccount en op "Certificaten intrekken" te klikken. Vervolgens moet je je wachtwoord voor verificatie opgeven. Vervolgens zie je een overzicht van alle twee factor-authenticators en uw persoonlijke certificaten. U kunt het relevante certificaat intrekken door op "Smartcard verwijderen en certificaten intrekken" naast de bijbehorende smartcard te klikken. De intrekking gaat onmiddellijk in en u kunt uw certificaat niet langer gebruiken.
- d) Je kan een intrekking van je SSL/SBR-certificaat aanvragen door je aan te melden bij jouw SSL/SBR-account en te klikken op "Intrekken" naast het bijbehorende certificaat. De intrekking gaat onmiddellijk in en je kan uw certificaat niet langer gebruiken.
- e) Digidentity behoudt zich het recht voor om accounts met onmiddellijke ingang te deactiveren als enige reden is om aan te nemen of te vermoeden dat de verstrekte verificatie en/of validatie niet langer correct is, of onjuist, fout of frauduleus is zoals uiteengezet in de Certificate Practice Statement. Als je een account wilt hebben, moet je een nieuwe account aanvragen.

- f) Digidentity behoudt zich het recht voor om een certificaat in te trekken als een overtreding is van deze Algemene Voorwaarden of een contractuele overeenkomst, of als Digidentity ontdekt dat het certificaat is gebruikt, of zal worden gebruikt voor criminele activiteiten, waaronder phishing, fraude of voor de verspreiding van malware/virussen.
- g) Zodra een certificaat is ingetrokken of verlopen, mag je de bijbehorende private key is niet langer gebruiken.
- h) Digidentity zal elke frauduleuze activiteit doorverwijzen naar de relevante autoriteiten. Uit naam van de Identiteitsdienstverlening kunnen we verdachte activiteiten ook melden bij een relevante instantie of bevoegde autoriteit.
- i) Digidentity behoudt zich het recht voor om accounts met onmiddellijke ingang te deactiveren als de communicatie van een gebruiker naar Digidentity medewerkers beschouwd wordt als intimiderend, bedreigend of beledigend. Wat Digidentity betreft, maakt dit het onmogelijk om redelijke diensten te bieden ter ondersteuning van aanvragen voor een digitale identiteit. Digidentity zal de eventuele voortzetting van misbruik, dreigend of intimiderend gedrag melden aan de betreffende autoriteiten.

11. Onze Verplichtingen

- a) Digidentity zal de diensten leveren zoals beschreven op onze website en in overeenstemming met deze Algemene Voorwaarden, de Privacyverklaring en de Certificate Practice Statement. Digidentity zal alle contractuele verplichtingen uitvoeren. Deze verplichtingen zijn echter geen garantie voor een succesvol resultaat van uw aanvraag.
- b) Digidentity streeft naar een continue functionerende en toegankelijke dienst maar biedt geen garanties over de beschikbaarheid van de aangeboden diensten. Je accepteert het feit dat (tijdelijke) storingen kunnen optreden die de dienst in gevallen ontoegankelijk kunnen maken.
- c) Digidentity zal 24 uur per dag, 7 dagen per week de documentatie beschikbaar stellen. Mocht deze documentatie niet beschikbaar zijn, dan zal Digidentity trachten de beschikbaarheid binnen vier (4 uur) te herstellen.
- d) Digidentity behoudt zich het recht voor om de beschikbaarheid van de dienstverlening te beperken of volledig ontoegankelijk te maken gedurende een beperkte periode om onderhoud en/of implementatie van vereiste wijzigingen uit te voeren. Digidentity streeft deze geplande onbeschikbaarheid uit te voeren in perioden waarvan redelijkerwijs kan worden aangenomen dat deze zo min mogelijk gebruikers beïnvloeden, bijvoorbeeld buiten de kantooruren.

- e) Digidentity zal de dienstverlening leveren in overeenstemming met de gepubliceerde Privacyverklaring. Deze privacyverklaring is toegankelijk op de website. Digidentity zal zijn Privacyverklaring van tijd tot tijd bijwerken om veranderingen in de gegevensverwerking met betrekking tot de dienst weer te geven.

12. Uw Verplichtingen

- a) Je begrijpt dat identiteitsverificatie een proces is dat berust op persoonsgegevens, beschikbare documentatie en door jou verstrekte gegevens en uniek op jouw gegevens is gebaseerd. Je accepteert dat dit identiteitsverificatieproces niet gebaseerd kan zijn op andere gebruikerservaringen of eisen.
- b) Je zorgt en garandeert dat je alle redelijke maatregelen neemt om de controle over, het vertrouwelijk houden en beschermen van de private key die hoort bij de publieke sleutel van het SSL/SBR-certificaat. Als persoonlijke abonnee zorg je dat de private key onder jouw controle staat. Als organisatie (wettelijke abonnee) zorg je dat de private key onder controle van de organisatie staat.
- c) Je accepteert dat ongeoorloofd gebruik van de private key verboden is.
- d) Je verzekert en garandeert de installatie van het SSL/SBR-certificaat alleen op servers die toegankelijk zijn op de subjectAltName vermeld in het certificaat en om het certificaat alleen te gebruiken in overeenstemming met alle van toepassing zijnde wetten, overeenkomsten en de Algemene Voorwaarden.
- e) Je bent verplicht om elk vermoeden van misbruik, daadwerkelijk misbruik van of gevaar voor jouw certificaat aan Digidentity onverwijld te melden en onmiddellijk het certificaat in te trekken.
- f) Je bent verplicht Digidentity onverwijld op de hoogte te stellen als de private sleutel verloren is gegaan, gestolen is of mogelijk of daadwerkelijk is gecompromitteerd is, en om het gebruik van deze sleutel onmiddellijk en definitief te staken, met uitzondering van sleutelontcijfering.
- g) Je bent verplicht om Digidentity onverwijld op de hoogte te stellen als de controle over de private key is verloren door diefstal, compromitteren of verlies van de activeringsgegevens, bijvoorbeeld pincode.

- h) Je aanvaardt de verplichting om het sleutelpaar alleen te gebruiken in overeenstemming met de meegedeelde beperkingen. Je accepteert de verplichting om de private key alleen te gebruiken voor cryptografische functies binnen het beveiligde cryptografische apparaat.
- i) Je verzekert en garandeert dat alle verstrekte gegevens en documenten correct, volledig, nauwkeurig en up-to-date zijn en dat ze voldoen aan de eisen zoals Digidentity heeft gesteld tijdens het registratieproces en de aanvraag. Je werkt jouw online profiel bij als zich wijzigingen voordoen in de gegevens die je bij de registratie hebt opgegeven. Voor SSL/SBR-certificaten moet je Digidentity op de hoogte brengen van wijzigingen waardoor de gegevens in het certificaat onjuist worden. Je zal de instructies en eisen opvolgen voor elke overdracht van gegevens (via het onlineproces of via de mobiele/tablet-applicatie) die Digidentity aangeeft.
- j) Je stemt in om Digidentity onverwijld op de hoogte te stellen als je je zorgen maakt over beveiliging, beveiligingsproblemen of datalekken. Digidentity zal elk melding van deze gegevens behandelen als vertrouwelijk en zal de melding in overeenstemming met toepasselijke wet- en regelgeving behandelen om schade te beperken. Digidentity tracht beveiligingswaarschuwingen zo snel als redelijkerwijs mogelijk is op te lossen en onderneemt de nodige stappen om derden te informeren.
- k) Je accepteert de verplichting om Digidentity op de hoogte te stellen van enige overtreding van de Voorwaarden beschreven in artikelen 12,14 en 15, met een gedetailleerde beschrijving van een dergelijke overtreding en alle andere relevante gegevens. Je moet alle redelijke maatregelen nemen om verdere en/of voortdurende schendingen te voorkomen en je neemt alle redelijke maatregelen om schade die het gevolg is van een dergelijke overtreding te beperken.
- l) Je accepteert de verplichting om de factuur van Digidentity binnen veertien (14) dagen na de datum van afgifte van de factuur te betalen.

13. Beperkingen van het Gebruik van onze Website

- a) Het is verboden om inhoud van de website, producten, diensten of bijbehorende materialen van Digidentity te kopiëren, door te geven, te verkopen, te publiceren of winst te maken.
- b) Het is verboden om de website, producten of bijbehorende materialen van Digidentity te gebruiken op een manier die de website schade toebrengt of kan toebrengen of tot een aantasting van de prestaties, beschikbaarheid of toegankelijkheid van de website, producten of bijbehorende materialen kan leiden.
- c) Het is verboden om de Digidentity-website en bijbehorende materialen te gebruiken met behulp van een robot, spider of andere middelen.

14. Persoonsgegevens

- a) Je erkent dat Digidentity een identiteits-, authenticatie- en autorisatiedienst levert en je begrijpt dat Digidentity persoonsgegevens zal verwerken om een identiteit vast te stellen en om de juistheid van persoonsgegevens of documenten te verifiëren. Digidentity is de Controller zoals gedefinieerd in de EU Algemene Verordening Gegevensbescherming (AVG) en zal de persoonsgegevens met de nodige zorgvuldigheid behandelen, in overeenstemming met alle toepasselijke wetten voor gegevensbescherming, inclusief de AVG en deze Algemene Voorwaarden, tenzij anders is overeengekomen.
- b) Digidentity verwerkt persoonsgegevens om zijn taken uit hoofde van het contract met jou uit te voeren en om een directe relatie met jou aan te gaan en te onderhouden zoals aangegeven in de Privacyverklaring. Voor alle duidelijkheid: dit omvat het vergelijken en controleren van de gegevens met (openbare of andere) databases die voor dit doel beschikbaar zijn. Digidentity zal de persoonsgegevens niet verwerken voor andere doeleinden, tenzij de verwerking vereist is op basis van een wettelijke verplichting of een bevel van een rechtbank, of als je jouw toestemming hebt gegeven.
- c) Om haar taken uit hoofde van het contract uit te voeren, zal Digidentity op Vertrouwende Partijen beroep doen bij de verwerking van persoonsgegevens. Digidentity zal passende maatregelen nemen om te zorgen dat deze Vertrouwende Partijen de persoonsgegevens verwerken in overeenstemming met het doel en de toepasselijke wetgeving.

15. Vertrouwelijkheid

- a) Digidentity en jij zijn verplicht om alle redelijke maatregelen te nemen om vertrouwelijke gegevens of de identiteitsaccount te beschermen tegen ongeoorloofde toegang, verlies, beschadiging, wijziging of niet-geautoriseerde verwerking. In het geval dat een dergelijk probleem zich voordoet, moet u Digidentity onverwijld informeren over ongeautoriseerde toegang, verlies, beschadiging, wijziging of niet-geautoriseerde verwerking.

16. Bewaren van Gegevens

- a) Digidentity kan de volgende gegevens bewaren (zodra de registratie succesvol is) tijdens de levensduur van het account;
 - i. Naam
 - ii. Adres
 - iii. Geboortedatum

- iv. Identiteitsdocumentgegevens: naam, geboortedatum, nationaliteit, documentnummer, vervaldatum
- v. Mobiel telefoonnummer
- vi. Emailadres

Alle andere gegevens die tijdens de registratie zijn gebruikt voor verificatie, worden na veertien (14) dagen vernietigd.

- b) Nadat de verwijdering is bevestigd, archiveert Digidentity de accountgegevens gedurende zeven (7) jaar in een versleuteld bestand. Toegang tot het archief wordt alleen verleend aan bevoegd personeel en alleen verstrekt in het geval van levering van bewijs om bijvoorbeeld gerechtelijke procedures. Het archief blijft onder alle andere omstandigheden vergrendeld.
- c) Digidentity houdt een logboek bij van de gegevens die per account is ontvangen, waaronder de ontvangst van gegevens, de verwerking daarvan en het resultaat. Deze gebeurtenislogboeken worden voor dezelfde periode bewaard als de accountgegevens - zeven (7) jaar nadat de account is verwijderd.

17. Eigendomsrechten & Intellectuele eigendom

- a) Te allen tijde blijven alle intellectuele eigendomsrechten horende bij de identiteitsdienst of bijbehorende materialen eigendom van Digidentity, de licentienemer of onze leverancier.
- b) Jouw recht op gebruik van de identiteitsdienst of bijbehorende materialen geeft geen recht op intellectuele eigendomsrechten van de identiteitsdienst of bijbehorende materialen. Digidentity biedt enkel een niet-exclusief recht om de identiteitsdienst en/of bijbehorende materialen te gebruiken om uw identiteit te verifiëren en een account aan te maken. Uw gebruiksrechten zijn strikt persoonlijk en kunnen niet worden overgedragen aan een andere persoon.
- c) Het is verboden (een deel van) de identiteitsdienst, gegevens of bijbehorende materialen te gebruiken op een manier die zou leiden tot schending van intellectuele eigendomsrechten van Digidentity, de licentienemer of leveranciers.
- d) Digidentity behoudt zich het recht voor om alle nodige maatregelen te nemen om de intellectuele eigendomsrechten van henzelf, de licentienemer of leveranciers te beschermen. Deze maatregelen omvatten het beëindigen van het gebruik van de identiteitsdienst of bijbehorende materialen wanneer het contract afloopt. Het is verboden dergelijke maatregelen op enigerlei wijze te gebruiken, te verwijderen of te omzeilen.

18. Aansprakelijkheid

- a) Niets in deze Algemene Voorwaarden sluit onze aansprakelijkheid uit of beperkt deze ten aanzien van:
- i. inbreuk op de wet door Digidentity of haar onderaannemers,
 - ii. enig verlies, ongeoorloofde toegang tot of beschadiging van persoonsgegevens die in het bezit zijn van Digidentity of haar onderaannemers (inclusief eventuele inloggegevens die aan u zijn verstrekt),
 - iii. enig willekeurig opzet door Digidentity of zijn onderaannemers.
- b) Wij zijn niet verantwoordelijk jegens jou voor enig verlies of schade die je lijdt en die geen voor de hand liggend gevolg zijn van het overtreden van deze Algemene Voorwaarden. Wij zijn niet verantwoordelijk jegens jou voor verliezen die je lijdt als gevolg van gebeurtenissen buiten onze controle. Wij zijn niet aansprakelijk jegens jou voor verliezen die Digidentity niet direct heeft veroorzaakt.
- c) Je kan Digidentity niet aansprakelijk stellen voor schade die het gevolg is van gebeurtenissen buiten onze controle of die Digidentity niet rechtstreeks heeft veroorzaakt.
- d) Je kan Digidentity niet aansprakelijk stellen voor enige indirecte schade of schade die is/of wordt veroorzaakt omdat je geen gepaste maatregelen hebt getroffen of genomen om:
- i. schade direct te beperken nadat zich een schadelijke gebeurtenis heeft voorgedaan,
 - ii. verdere schade of latere schade als gevolg van de eerste gebeurtenis voorkomen,
 - iii. Digidentity onmiddellijk informeren over gebeurtenissen die schade zouden kunnen veroorzaken en/of relevante gegevens aan Digidentity zouden kunnen verschaffen.
- e) In alle gevallen is de aansprakelijkheid van Digidentity beperkt tot de gebruikelijke en voorzienbare schade. Je kan Digidentity niet aansprakelijk stellen voor bedrijfsschade na het gebruik van de identiteitsdienst in de hoedanigheid van consument.
- f) Je kan Digidentity nooit aansprakelijk stellen voor enige schade die voortvloeit uit:
- i. jouw ongeautoriseerd of oneigenlijk gebruik van de gegevens, de identiteitsdienst en/of gerelateerde materialen;

- ii. verstrekken van onjuiste en/of onvolledige gegevens, of het niet tijdig verstrekken van gegevens aan Digidentity;
- iii. het zelf verliezen van eigen gegevens;
- iv. jouw verzuim om zich te houden aan de verplichtingen in deze Algemene Voorwaarden of CPS, inclusief het niet meewerken aan de Algemene Voorwaarden.
- v. te late, onjuiste of onvolledige toegankelijkheid van de identiteitsdienst;
- vi. miscommunicatie of verlies van berichten en kennisgevingen die het gevolg zijn van het gebruik van een door u gekozen communicatiemiddel, of als gevolg van het disfunctioneren van door u gebruikt materiaal, inclusief onjuist functioneren van het internet;
- vii. gebruik van materialen die je hebt geselecteerd;
- viii. ongeautoriseerd gebruik, verlies of diefstal van inloggegevens die aan jou zijn verstrekt;
- ix. downtime of niet beschikbare online-tools van derden;
- x. jouw gebruikersnaam, wachtwoord of PIN code delen met een andere persoon.

19. Beperking van Vordering

- a) Je dient een vordering tot schadevergoeding tegen Digidentity in te dienen binnen een jaar nadat de schade is ontstaan.

20. Overmacht

- a) Digidentity is niet verplicht om een van de verplichtingen uit hoofde van het contract of de Algemene Voorwaarden na te komen in geval van overmacht. Onder overmacht wordt verstaan een gebeurtenis die buiten de redelijke controle van de getroffen partij valt en daarom, indien Digidentity geen acties kan uitvoeren die verband houden met, en niet beperkt tot;
 - i. Onjuist functionerend materiaal geleverd door gebruikers
 - ii. Wettelijke vereisten
 - iii. Stroomonderbreking, stroomuitval of andere onderbrekingen van elektriciteit
 - iv. Onjuiste werking van internet-, computer- en/of telecommunicatiemiddelen
 - v. Extreme weersomstandigheden, overstromingen, aardbevingen of andere natuurlijke of weersgerelateerde oorzaken;
 - vi. Staking, rellen of burgerlijke onrust
 - vii. Vuur of explosie
 - viii. Oorlog, opstand of openlijke militaire vijandelijkheden;
 - ix. Catastrofale epidemie of pandemie
 - x. Algemene vervoersproblemen

- xi. Extreme omstandigheden die de beschikbaarheid van Digidentity-medewerkers voor het uitvoeren van taken verminderen/ernstig beperken
- xii. Tegenstrijdige wetgeving of overheidsoptreden, verbod, embargo of boycot
- xiii. Terrorisme
- xiv. Falen van leveranciers

Digidentity neemt maatregelen om het risico van onderbreking van diensten te voorkomen, en heeft een bedrijfscontinuïteitsplan en een noodherstelplan.

21. Toepasselijke Wetten, Voorschriften en Audits

- a) Op het contract en de Algemene Voorwaarden is het Nederlandse recht van toepassing en zijn conform aan de Europese toepassingsrichtlijnen, in het bijzonder artikel 8 van het Europees Verdrag voor de Rechten van de Mens inzake privacywetten.
- b) Digidentity is gecontroleerd en goedgekeurd voor de uitgifte, het beheer en de intrekking van gekwalificeerde certificaten voor elektronische handtekeningen per Verordening nr. 910/2014 (EU), bekend als eIDAS.
- c) Digidentity wordt jaarlijks gecontroleerd op de vereisten van ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, CA/Browser Forum Baseline Requirements, CA/Browser Forum Network Security Requirements, PKI-overheid Programma van Eisen, Afsprakenstelsel eHerkenning, tScheme and ISO27001:2013. De huidige certificering kan worden bekeken via deze link:
<https://www.digidentity.eu/nl/home/#certifications>

22. Klachten

- a) Digidentity heeft een klachtenprocedure die beschikbaar is op:
<https://www.digidentity.eu/en/home/#complaints-procedure>
- b) Elk geschil dat een gebruiker en Digidentity niet in der minne kunnen schikken, wordt voorgelegd aan de bevoegde rechter van de plaats waar Digidentity een statutaire zetel heeft (Den Haag). Indien de toepasselijke Nederlandse of Europese wetgeving bepaalt dat een andere rechter ook bevoegd is, dan kan de zaak ook voor deze rechter worden gebracht. Indien de toepasselijke Nederlandse of Europese wetgeving bepaalt dat een andere rechter de exclusieve bevoegdheid heeft, dan kan de zaak alleen voor die rechter worden gebracht.

23. Garanties

- a) Digidentity voorziet niet in andere garanties, beloften en/of verbintenissen dan diegene die expliciet in de Algemene Voorwaarden voorzien zijn.

24. Slotbepalingen

- a) Mocht een bepaling van de Algemene Voorwaarden ongeldig of nietig worden verklaard, dan heeft dit geen invloed op de geldigheid van de andere bepalingen in de Algemene Voorwaarden. In een dergelijk geval zal Digidentity de Algemene Voorwaarden wijzigen met de bedoeling om hetzelfde doel te bereiken dat wordt gediend met de ongeldig of nietig verklaarde bepaling.

Definities

De volgende woorden hebben de volgende betekenis:

- **Gebruiker**

"Gebruiker", "je", "jou" of "jouw" in deze Algemene Voorwaarden verwijzen naar jou als gebruiker van de Identiteitsdienst.

- **Identiteitsdienst**

De service die we je bieden en die de verificatie van uw identiteit en/of de geldigheid van documenten of gegevens vereist. Als dit verificatie- en/of validatieproces resulteert in een bevestiging en/of validatie van de gegevens die je hebt verstrekt, maken we een identiteitsaccount voor uw persoonlijk gebruik.

- **Vertrouwende Partij**

De relevante derde partij die van u vereist dat u uw identiteit verifieert, zodat u zijn diensten kunt gebruiken, d.w.z. Overheidsafdelingen.

- **Contract**

De relatie tussen u en ons, beheerst door de Algemene Voorwaarden volgens artikel 1.

- **Algemene Voorwaarden**

Deze Algemene Voorwaarden zoals hier uiteengezet.

- **Identiteitsaccount**

Uw unieke profiel dat we u hebben verstrekt na identificatie en/of validatie van gegevens en documenten, ongeacht of de verificatie van uw identiteit al dan niet succesvol is.

- **Gegevens**

Alle gegevens die u ons hebt verstrekt of in verband met de Digidentity-service.

- **Licentiehouder**

De houder van een licentie voor intellectuele eigendomsrechten verbonden aan de identiteitsdienst.

- **Materialen**

Materialen verwijzen naar alle software, hardware, websites, database, ontwerpen, modellen, programma's, rapporten en andere identiteitsdiensten en materialen die wij of de vertrouwende partij hebben gebruikt in verband met de identiteitsdienst.

- **Schriftelijk**

Voor de huidige Algemene Voorwaarden verwijst de term "schriftelijk" naar elke schriftelijke communicatie, of dit nu op elektronische wijze is of per gewone post.