1 april 2026

Gebruikersreglement voor de toegang tot en het gebruik van het informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid door ondernemingen en hun lasthebbers

Artikel 1. - Toepassingsgebied

Dit gebruikersreglement regelt de toegang tot en het gebruik van het Informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid (hierna Informatiesysteem genoemd) en de daardoor aangeboden Diensten door ondernemingen en hun lasthebbers.

Artikel 2. – Verplichting tot aanduiding van een Hoofdtoegangsbeheerder

Elke onderneming die toegang wil hebben tot het Informatiesysteem en er gebruik van wil maken, moet één en slechts één Hoofdtoegangsbeheerder aanduiden.

Artikel 2 bis - Definities

Onder "Elektronische Identiteitskaart" in de zin van dit gebruikersreglement wordt begrepen de elektronische identiteitskaart bedoeld in de artikelen 6 en volgende van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen waarop de identiteits- en de handtekeningscertificaten zijn geactiveerd.

Onder toegangsbeheerder of lokale beheerder wordt (worden) in dit reglement de natuurlijke perso(o)n(en) verstaan die binnen de onderneming aangesteld wordt (worden) door de daartoe bevoegde persoon teneinde het gebruikers- en toegangsbeheer op zijn (hun) niveau te verzekeren, ongeacht of deze perso(o)n(en) nu optreedt (optreden) als Hoofdtoegangsbeheerder, als co-Hoofdtoegangsbeheerder, als (co-)Toegangsbeheerder (co-) Lokale beheerder)).

Artikel 3. – Aangeboden diensten en beschikbare kanalen

De aangeboden Diensten zijn toegankelijk via verschillende kanalen.

1. Via de portaalsite van de sociale zekerheid (www.socialezekerheid.be):

a) elke gebruiker heeft toegang tot de toepassingen zoals voor hem aangeduid in de tabel in "BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid";
b) elke curator die is aangeduid als Toegangsbeheerder (Lokale Beheerder) of elke Gebruiker die door deze curator is aangeduid heeft toegang tot de toepassingen zoals voor hem aangeduid in de tabel in "BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid";
c) elke Gebruiker die door de Hoofdtoegangsbeheerder van een onderneming is aangeduid als Toegangsbeheerder (Lokale Beheerder) heeft toegang tot de toepassingen zoals voor hem

aangeduid in de tabel in “BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid”;

d) elke Gebruiker die door de Toegangsbeheerder (Lokale Beheerder) van een onderneming is aangeduid heeft toegang tot die toepassingen waartoe hij door de Toegangsbeheerder (Lokale Beheerder) van een onderneming gemachtigd is, zonder dat deze toegang echter ruimer kan zijn dan de toegang van de Toegangsbeheerder (Lokale Beheerder) zelf;

e) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

2. Via de portaalsite van de federale overheid (www.belgium.be):

   a) elke gebruiker heeft toegang tot de toepassingen zoals voor hem aangeduid in de tabel in “BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid”;

   b) elke Gebruiker die door een onderneming is aangeduid als Toegangsbeheerder (Lokale Beheerder) heeft toegang tot de toepassingen zoals voor hem aangeduid in de tabel in “BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid”;

   c) elke Gebruiker die door de Toegangsbeheerder (Lokale Beheerder) van een onderneming is aangeduid en beschikt over het repertoriumnummer van de lastgever heeft toegang tot de toepassingen zoals voor hem aangeduid in de tabel in “BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid”, en dit voor de personen voor wie hij over een mandaat beschikt om deze toepassingen voor hun rekening en in hun naam te gebruiken en waarvan hij dit mandaat ter beschikking heeft gesteld van de Gewestelijke Directie van de Directe Belastingen die bevoegd is voor het belastingkantoor van de lastgever;

   d) elke Gebruiker die door de Toegangsbeheerder (Lokale Beheerder) van een onderneming is aangeduid en, en met betrekking tot de toepassingen vermeld in punt 3c), beschikt over het repertoriumnummer van de lastgever, heeft toegang tot die toepassingen waartoe hij door de Toegangsbeheerder (Lokale Beheerder) van een onderneming gemachtigd is, zonder dat deze toegang echter ruimer kan zijn dan de toegang van de Toegangsbeheerder zelf;

   e) elke Gebruiker die door een onderneming is aangeduid als Toegangsbeheerder (Lokale Beheerder) of die door de Toegangsbeheerder (Lokale Beheerder) van een onderneming is aangeduid, en die beschikt over een Gebruikersnaam, een Paswoord, een Private Sleutel en een gekwalificeerd Certificaat in de zin van artikel 2, 4° van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, of een ander type certificaat vermeld in de lijst van aanvaarde certificaten op de portaalsite van de sociale zekerheid, heeft daarenboven toegang tot de toepassingen zoals voor hem aangeduid in de tabel in “BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid”.

   f) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau

voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

3. Via de portaalsite eGezondheid (www.ehealth.fgov.be):

   a) heeft elke Gebruiker toegang tot de toepassingen zoals voor hem aangeduid in de tabel in "BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid";

   b) heeft elke gemachtigd gebruiker, afhankelijk van zijn hoedanigheid, toegang tot de toepassingen zoals voor hem aangeduid in de tabel in "BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid";

   c) heeft elke gemachtigd gebruiker , toegang tot de toepassingen zoals voor hem aangeduid in de tabel in "BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid";

   d) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

4. Via bestandsoverdracht overeenkomstig (S)FTP of andere aanvaarde kanalen, kan elke Gebruiker die door een onderneming is aangeduid als Toegangsbeheerder (Lokale Beheerder) of die door een Toegangsbeheerder is aangeduid, en die beschikt over een Gebruikersnaam, een Paswoord, een Private Sleutel en een gekwalificeerd Certificaat in de zin van artikel 2, 4° van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, of een ander type certificaat vermeld in de lijst van aanvaarde certificaten op de portaalsite van de sociale zekerheid, waaronder het geactiveerd handtekeningscertificaat van de Elektronische Identiteitskaart , "Dimona-aangiften", "DmfA - Multifunctionele aangifte", "DmfA voor provinciale en plaatselijke besturen", "Wijzigingen van een RSZ-aangifte (DMFA)", "Wijzigen van een DmfAPPL-aangifte" en " ASR - Aangifte sociale risico's" verrichten.

De inhoud van de Diensten en de toegang tot deze Diensten kunnen ten allen tijde worden gewijzigd.

Specifieke gebruiksvoorwaarden voor de aangeboden diensten kunnen als bijlage bij dit gebruikersreglement worden gespecificeerd.

Artikel 4. - Toegang tot het Informatiesysteem

De Gebruiker heeft toegang tot het Informatiesysteem, zonder dat evenwel gewaarborgd wordt dat de toegang tot het Informatiesysteem en de geboden Diensten te allen tijde is verzekerd, vrij is van fouten of technische storingen.

De toegang tot het Informatiesysteem en de Diensten die via het systeem worden geleverd kan te allen tijde geheel of gedeeltelijk worden afgesloten (o.m. voor onderhoudsdoeleinden). Waar redelijkerwijze mogelijk zal de Gebruiker van dergelijke onderbreking op voorhand op de hoogte worden gebracht.

De Gebruiker is verantwoordelijk voor het voorzien in en het onderhoud van de Terminal die nodig is voor het gebruik van het Informatiesysteem. De aanbieders van het Informatiesysteem zijn niet verantwoordelijk voor de Terminal en het gebruik dat ervan wordt gemaakt, en zijn niet gehouden tot het bieden van enige ondersteuning dienaangaande.

Artikel 5. - Het gebruik van de Gebruikersnaam en het Paswoord

Een Gebruiker die door een onderneming is aangeduid als Hoofdtoegangsbeheerder kan in afzonderlijke zendingen via Eranova, het Contactcentrum van de openbare instellingen van sociale zekerheid, een Gebruikersnaam en Paswoord ontvangen. Een gebruiker die niet door een onderneming is aangeduid als Hoofdtoegangsbeheerder ontvangt zijn Gebruikersnaam en Paswoord van de Toegangsbeheerder (Lokale Beheerder) van zijn onderneming.

De Gebruikersnaam en het Paswoord zijn strikt persoonlijk en niet overdraagbaar.

Elke gebruiker dient het Paswoord dat hij van het Contactcentrum van de openbare instellingen van sociale zekerheid of van een Toegangsbeheerder (Lokale Beheerder) ontvangen heeft zo snel mogelijk na de ontvangst en in elk geval bij het eerste gebruik ervan te wijzigen. Elke Gebruiker dient nadien zijn Paswoord te wijzigen op regelmatige tijdstippen.

Een veilig paswoord is samengesteld uit 15 tekens en bevat alfanumerieke karakters en symbolen, geplaatst in een volgorde die niet makkelijk kan worden geraden. Elke gebruiker dient ervoor te zorgen dat het gekozen Paswoord voldoet aan deze eisen. Elke Gebruiker is zelf aansprakelijk in de gevallen waarin een Paswoord, dat niet volgens deze regels is samengesteld, wordt achterhaald en / of misbruikt.

Elke Gebruiker dient zorgvuldig om te gaan met zijn Gebruikersnaam en Paswoord en is tot geheimhouding ervan gehouden. Elke Gebruiker is aansprakelijk voor elk al dan niet geoorloofd gebruik ervan, met inbegrip van elk gebruik door derden.

Indien een gebruiker kennis heeft van verlies van zijn Gebruikersnaam en / of Paswoord of van elk ongeoorloofd gebruik door derden van zijn Gebruikersnaam en / of Paswoord, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen.

Elke Gebruiker die door een onderneming is aangeduid als Hoofdtoegangsbeheerder is er onder meer toe gehouden dit verlies of ongeoorloofde gebruik onmiddellijk te melden aan het Contactcentrum van de openbare instellingen van sociale zekerheid, Eranova (02/511.51.51 of via de portaalsite van de sociale zekerheid (www.socialezekerheid.be)). Zo spoedig mogelijk na de ontvangst van deze melding en binnen de grenzen van de redelijkheid, worden alle mogelijke inspanningen geleverd om de Gebruikersnaam en het Paswoord van de Gebruiker te wijzigen.

Elke Gebruiker die niet door een onderneming is aangeduid als Hoofdtoegangsbeheerder is er onder meer toe gehouden dit verlies of ongeoorloofd gebruik onmiddellijk te melden aan de

Hoofdtoegangsbeheerder of Toegangsbeheerder(Lokale Beheerder) van wie hij zijn Gebruikersnaam en Paswoord ontvangen heeft. Deze moet zo spoedig mogelijk na de ontvangst van deze melding en binnen de grenzen van de redelijkheid, alle mogelijke inspanningen leveren om de Gebruikersnaam inactief te maken en/of het Paswoord van de Gebruiker te wijzigen.

Elke Gebruiker blijft aansprakelijk voor alle (rechtstreekse of onrechtstreekse) schade ontstaan door het (al dan niet geoorloofd) gebruik van zijn Gebruikersnaam en / of Paswoord dat heeft plaatsgevonden vóór het tijdstip waarop de Gebruikersnaam en het Paswoord geïnactiveerd werden.

In geval van blokkering van zijn Gebruikersnaam en / of Paswoord dient de Gebruiker die door een onderneming is aangeduid als Toegangsbeheerder (Lokale Beheerder) een nieuwe Gebruikersnaam en een nieuw Paswoord aan te vragen bij Eranova, het Contactcentrum van de openbare instellingen van sociale zekerheid, waarna een nieuwe Gebruikersnaam en een nieuw Paswoord worden verstrekt.

Artikel 5 bis. - Het gebruik van de digitale sleutels

De toegang van de Gebruiker tot bepaalde langs elektronische weg aangeboden diensten vereist het gebruik van digitale sleutels (zoals eID kaartlezer, beveiligingscode op basis van TOTP (Time-based One-time password) via mobiele app of SMS, gebruikersnaam en wachtwoord, (mobiele) sleutels aangeboden in het kader van diensten erkend conform het KB van 22 oktober 2017 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen).

Deze digitale sleutels en de gegevens eraan verbonden zijn strikt persoonlijk en niet overdraagbaar.

Elke eindgebruiker is verantwoordelijk voor de goede bewaring, beveiliging, geheimhouding en beheer van zijn digitale sleutels en gegevens eraan verbonden.

De eindgebruiker is verantwoordelijk voor de keuze van een veilig wachtwoord of andere geheime code.

Indien een eindgebruiker kennis heeft van het verlies van zijn gebruikersnaam, wachtwoord of ander digitale sleutel, of van elk ongeoorloofd gebruik ervan door derden, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen om de digitale sleutel te deactiveren.

In geval van vergrendeling van zijn digitale sleutel, dient de eindgebruiker een nieuwe aan te vragen.

De digitale sleutels worden aangewend in het kader van CSAM (zie https://www.csam.be). Het aanmaken en gebruik daarvan worden ook geregeld in de gebruikersovereenkomst van CSAM. Sommige digitale sleutels zijn niet beschikbaar gesteld voor elke toepassing.

Artikel 6. - Gebruik van het Informatiesysteem

Met betrekking tot het gebruik van het Informatiesysteem en de via dit systeem verleende Diensten, is elke Gebruiker ertoe gehouden:

1. volledige, accurate, waarachtige en niet-misleidende informatie te verstrekken;
2. de door wet, reglement, decreet, ordonnantie of besluit van de federale, regionale, lokale of internationale overheid voorgeschreven bepalingen te respecteren;
3. zich te onthouden van het manipuleren van de geleverde informatie, op welke wijze dan ook of met gebruik van eender welke techniek;
4. via het Informatiesysteem geen gegevens, berichten of documenten te versturen op eender welke wijze, hetzij gegevens of documenten via het Informatiesysteem op te laden:
   a) waarbij de rechten (waaronder persoonlijkheidsrechten of intellectuele eigendomsrechten) van derden of van de aanbieders van het Informatiesysteem worden geschonden;
   b) waarvan de inhoud onwettig, schadeberokkenend, lasterlijk, gewelddadig, obsceen of onterend is of waarbij de privacy van derden wordt geschonden;
   c) waarvan het gebruik of het bezit door de Gebruiker bij wet of bij overeenkomst verboden is;
   d) die virussen of instructies bevatten die schade kunnen toebrengen aan de aanbieders van het Informatiesysteem en/of het Informatiesysteem en/of de via het Informatiesysteem verleende Diensten in het gedrang zouden kunnen brengen of verstoren.

Artikel 7. - Gebruik van het certificaat

De toegang van de Gebruiker tot bepaalde Diensten vereist hetzij het gebruik van een Elektronische Identiteitskaart, hetzij, bovenop het gebruik van een Gebruikersnaam en een Paswoord, het gebruik van een Private Sleutel en van een gekwalificeerd Certificaat in de zin van artikel 2, 4° van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, of een ander type certificaat vermeld in de lijst van aanvaarde certificaten op de portaalsite van de sociale zekerheid.

Eenzelfde Certificaat kan worden gebruikt voor de authenticatie en voor het plaatsen van een elektronische handtekening, bedoeld in artikel 1322, tweede lid, van het Burgerlijk Wetboek Echter, indien de toegang tot de aangeboden Diensten gebeurt via een Elektronische Identiteitskaart, wordt de authenticatie gerealiseerd door het identiteitscertificaat van de Kaart en wordt de elektronische handtekening aangebracht via het handtekeningscertificaat van de Kaart.

Zodra de gegevens voor het aanmaken van een handtekening samengesteld zijn, is de certificaathouder alleen verantwoordelijk voor de vertrouwelijkheid van deze gegevens. Wanneer er twijfel bestaat over het behoud van de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening of wanneer de in het certificaat opgenomen gegevens niet meer met de werkelijkheid overeenstemmen, dient de houder het certificaat te laten herroepen. Wanneer een certificaat vervalt of herroepen wordt, mag de houder na de vervaldatum van het certificaat of na herroeping geen gebruik meer maken van de overeenkomstige gegevens voor het aanmaken van een handtekening om deze gegevens te ondertekenen of te laten certificeren door een andere certificatiedienstverlener.

Elke Gebruiker dient derhalve zorgvuldig om te gaan met de Private Sleutel en het Certificaat evenals het eventuele Paswoord dat nodig is om de Private Sleutel en het Certificaat te

gebruiken. De Gebruiker is aansprakelijk voor elk al dan niet ongeoorloofd gebruik ervan, met inbegrip van elk gebruik door derden. De Gebruiker dient de Private Sleutel en het Certificaat te bewaren op een veilige drager, bij voorkeur op een processorchipkaart die de Private Sleutel niet kan exporteren.

Het Informatiesysteem is in staat Certificaten en types te valideren die zijn uitgereikt door de certificatie-autoriteiten opgenomen in de lijst gepubliceerd op de portaalsite van de sociale zekerheid (www.socialezekerheid.be). Certificaten uitgereikt door andere certificatie-autoriteiten kunnen enkel worden aanvaard nadat de nodige technische aanpassingen zijn aangebracht aan het Informatiesysteem die het mogelijk maken om deze Certificaten te valideren. De Gebruiker die de vaste wil heeft om een gekwalificeerd Certificaat in de zin van artikel 2, 4° van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten te gebruiken dat is uitgereikt door een andere certificatie-autoriteit dan deze vermeld op de portaalsite van de sociale zekerheid, kan dit met gebruik van zijn Gebruikersnaam en Paswoord melden via het daartoe bestemde formulier op de portaalsite van de sociale zekerheid. Binnen de grenzen van de redelijkheid en voorzover de betrokken certificatie-autoriteit alle nodige medewerking verleent, zullen de nodige inspanningen worden gedaan opdat het Informatiesysteem ook Certificaten van de vermelde certificatie-autoriteit kan valideren. Zodra dit het geval is, is het gebruik van Certificaten van de vermelde certificatie-autoriteit mogelijk.

Artikel 8. - Gebruik van elektronische handtekening en bewijs (gebruikers met certificaat)

De berichten verstuurd via het Informatiesysteem, door de Gebruiker die beschikt hetzij over een gekwalificeerd Certificaat in de zin van artikel 2, 4° van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, of een ander type certificaat vermeld in de lijst van aanvaarde certificaten op de portaalsite van de sociale zekerheid, hetzij over een Elektronische Identiteitskaart, worden voorzien van een elektronische handtekening, bedoeld in artikel 1322, tweede lid, van het Burgerlijk Wetboek.

De Gebruiker erkent uitdrukkelijk dat alle berichten die worden verstuurd via het Informatiesysteem en die voorzien zijn van voornoemde elektronische handtekening dezelfde wettelijke bewijskracht hebben als een onderhandse akte in de zin van het Burgerlijk Wetboek.

De Gebruiker erkent uitdrukkelijk dat alle informatie betreffende berichten die door de aanbieders van het Informatiesysteem op een duurzame en niet te wijzigen manier opgeslagen wordt, wettelijke bewijskracht heeft als een onderhandse akte in de zin van het Burgerlijk Wetboek, tot bewijs van het tegendeel.

De Gebruiker erkent uitdrukkelijk als de zijne de handtekening die geplaatst is op basis van de private sleutel en het hem verleende certificaat, behalve in geval van misbruik, verlies, of diefstal, voor zover de daartoe voorziene procedure wordt nageleefd.

Artikel 9. - Controleplicht van de Gebruiker

De Gebruiker is verantwoordelijk voor de controle van de inhoud van de door hem via het Informatiesysteem verstuurde berichten en voor de opvolging daarvan naar aanleiding van

berichten die door de aanbieders van het Informatiesysteem aan de Gebruiker worden verstuurd, en die betrekking hebben op de (het) door de Gebruiker verstuurde bericht(en).

De materiële fout(en) in een door de Gebruiker verstuurd bericht, in een ontvangstmelding die daarop betrekking heeft of in eender welk ander bericht of document dat op de Gebruiker betrekking heeft en dat toegankelijk is via het Informatiesysteem, word(t)(en) op verzoek van de Gebruiker via een daartoe voorziene rechtzettingsprocedure verbeterd.

Artikel 10. - Intellectuele eigendomsrechten

De Gebruiker erkent en aanvaardt dat het Informatiesysteem, de Dienstverlening en de software die in verband met het Informatiesysteem en de Dienstverlening is ontwikkeld, beschermd worden door intellectuele eigendomsrechten (auteursrecht, merkenrecht, octrooirecht, enz.), waarvan de aanbieders van het Informatiesysteem (of haar licentieverstrekkers) de houder(s) zijn.

De Gebruiker verkrijgt een niet-exclusief recht om het Informatiesysteem te gebruiken voor de in het gebruikersreglement beschreven doeleinden. Behoudens uitdrukkelijke toestemming is het de Gebruiker niet toegelaten om op welke wijze ook het Informatiesysteem geheel of gedeeltelijk te kopiëren (op welke manier of op welke drager dan ook), aan te passen, te vertalen, te verkopen, te verhuren, uit te lenen, mede te delen aan het publiek, noch afgeleide werken van voormelde elementen te creëren.

Artikel 10bis. – Vrije licenties

Wanneer het Informatiesysteem en de diensten een vrije software gebruiken of ter beschikking stellen, is de licentie die bij deze software hoort van toepassing op de gebruiker.

Naast de regels die in de licentie van de vrije software in kwestie zijn opgenomen, zijn de volgende onafhankelijke en aanvullende bepalingen inzake de aansprakelijkheid van de beheerders, de administrators, de medewerkers en het personeel van het Informatiesysteem (hierna “het Informatiesysteem” genoemd) en de garantie die zij bieden, van toepassing op de gebruiker.

Wanneer het Informatiesysteem een vrije software aanpast, stelt het alles in het werk om ervoor te zorgen dat deze correct door de gebruiker kan worden aangewend, zonder echter in dit opzicht enige resultaatsverbintenis aan te gaan.

De gebruiker van zijn kant verbindt zich ertoe de software die ter zijn beschikking is gesteld zo adequaat en correct mogelijk te gebruiken en, desgevallend, alle nuttige informatie die kan bijdragen tot het oplossen van problemen m.b.t. het gebruik van de software, aan het Informatiesysteem te verschaffen.

Aangezien de software in kwestie vrij kan worden gebruikt, zal het Informatiesysteem in geen geval, behalve bij schriftelijke vermelding, aansprakelijk kunnen worden gesteld voor elke vorm van schade, direct of indirect, secundair of bijkomstig, materieel of immaterieel, veroorzaakt door de gebruiker of derden, voortkomend uit het gebruik van de software of uit de onmogelijkheid om deze te gebruiken.

Artikel 11 - Overgangsmaatregelen

Voor het ogenblik kan het handtekeningscertificaat van de Elektronische Identiteitskaart slechts gebruik worden via het systeem van bestandsoverdracht overeenkomstig (S)FTP, aan de hand van MQSeries of andere aanvaarde kanalen; het laat niet toe om toegang te hebben tot en gebruik te maken van de Diensten die op de portaalsite van de sociale zekerheid en op de portaalsite van de federale overheid worden aangeboden, behalve voor wat betreft het gebruik van de toepassing “elektronisch formulier voor toegangsaanvraag”.

Artikel 12 – Autenticatiemiddelen en zekerheidsniveaus

Authenticatiemiddelen worden gebruikt om de identiteit van een gebruiker betrouwbaar vast te stellen en zijn cruciaal voor digitale veiligheids- en toegangscontrole. De Federal Authentication Service (FAS) van de FOD BOSA biedt hiervoor verschillende middelen aan, die bijvoorbeeld door de KSZ en het eHealth-platform gebruikt worden om burgers en professionals veilig toegang te geven tot gevoelige toepassingen.

Het betrouwbaarheidsniveau (of zekerheidsniveau) van een authenticatiemiddel – hoe zeker het is dat iemand werkelijk is wie hij beweert te zijn – wordt volgens Europese regelgeving aangeduid als laag, substantieel of hoog. De FAS specificeert dit niveau ook met een cijfer (het FAS-authenticatieniveau) voor meer nauwkeurigheid.

De FOD BOSA publiceert een overzicht van de beschikbare middelen:

Betrouwbaarheidsniveau	FAS Authenticatieniveau	Authenticatiemiddel
Hoog	500	eID
		eIDAS4 High
	490	MyGov.be Hoog (met PIN)
	450	Itsme Hoog (met PIN)
Substantieel	400	eIDAS Substantieel
		Itsme Substantieel (met vingerafdruk)
		MyGov.be Substantieel (met vingerafdruk)
		TOTP (via Authenticator App)
		TOTP (via mail)
		TOTP (via SMS)
Laag	200	Username / Password

BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Toepassingen toegankelijk voor elke Gebruiker zoals omschreven in artikel 3.1.a		
Dimona (Niet-beveiligd)	Voor deze toepassingen is geen digitale sleutel vereist	
Aangifte van werken		
Elektronisch formulier voor toegangsaanvraag		
Publieke raadpleging van het werkgevers-repertorium		
Werkgever Identificatie (WIDE) – niet beveiligd		
Inhoudingsplicht		
Minnelijk afbetalingsplan		
Toepassingen toegankelijk voor curatoren zoals omschreven in artikel 3.1.b		
eCUR	Ja	Ja
Werkgever Identificatie (WIDE)		
Toepassingen toegankelijk voor toegangsbeheerders (lokale beheerders) en voor Gebruikers door hen aangeduid zoals omschreven in artikel 3.1.c en artikel 3.1.d		
“Raadpleging van de e-Box”,	Ja	Ja
“Dimona (Beveiligd)”,		
“DmfA - Multifunctionele aangifte”,		
“DmfA voor provinciale en plaatselijke besturen”,		
“ASR - Aangifte sociale risico's (indienen en wijzigen)”		
“Beveiligde raadpleging van het werkgeversrepertorium”		
“Consultatie Vakantiebestand”,		
“Limosa - Meldingsplicht”,		
“Toegangsbeheer voor Ondernemingen en Organisaties”,		

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Toepassingen toegankelijk voor toegangsbeheerders (lokale beheerders) en voor Gebruikers door hen aangeduid zoals omschreven in artikel 3.1.c en artikel 3.1.d		
“Ecaro”,	Ja	Ja
“Trillium”,		
“Werkgever identificatie (WIDE)”,		
“Capelo - Aanvullingen bij het Loopbaan Dossier”,		
“Capelo - Historische Gegevens”,		
“Student@work”,		
“DestHa – beheer van verzendingsregels”,		
“Consultatie facturen werkgevers”,		
“Checkinatwork”,		
“Horeca@work”,		
“Publiato”,		
“Aangifte van werken - FRONTEND”,		
“Inhoudingsplicht”,		
“FollowIt”		
“Beheer en historiek van mandaten van sociale zekerheid (Mahis)”,	Nee	Ja
“DB2P”,		
“Publieke mandatarissen”,		
“Werken in het buitenland”		
“Wijziging van een RSZ-aangifte (DMFA)”		
“Wijzigen van een DmfAPPL-aangifte”		
Registreren (beveiligd)		
Werken in het buitenland - Zelfstandigen		
Green@work		
Rina		
BelgianIDpro		
Vrijstelling sociale bijdragen zelfstandigen		
ContactData		
CareerPro Documents		
“Tijdelijke werkloosheid en validatieboek”		
“Dossier Loopbaanonderbreking en tijdskrediet”		
Verenigingswerk	Nee	Ja
Working in the Arts – Amateurkunstenvergoeding	Nee	Ja
Check In and Out at Work	Nee	Ja
Chaman: beheer van technische kanalen	Nee	Ja
CareerPro Federal Learning Account	Nee	Ja
Flexi at work	Nee	Ja
Burgermandaten	Nee	Ja
Burgergegevens raadplegen	Nee	Ja
Inzetbaarheidsbevorderende maatregelen	Ja	Ja
Gezondheidstoezicht op zwangere werkneemsters	Nee	Ja

BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Opvragen van informatie van de ondernemingen”	Voor deze toepassingen is geen digitale sleutel vereist	
Toepassingen toegankelijk tot Toegangsbeheerder (Lokale Beheerder) en door hen aangeduide Gebruikers zoals omschreven in de artikelen 3.2.b en 3.2.d		
“Opvragen van informatie van mijn onderneming”	Ja	Ja
“Woonwerkverkeersenquête”		
“Vigilis (e-loket)“		
“e-Notification“		
“De Unieke Startersaangifte (DEUS)”		
Toepassingen toegankelijk tot Toegangsbeheerder (Lokale Beheerder) en door hen aangeduide Gebruikers zoals omschreven in de artikelen 3.2.c en 3.2.d		
“Tax-on-web” (TOW)	Ja	Ja
“Raadpleging van de Tax-on-web-aangifte”		
Toepassingen toegankelijk tot Toegangsbeheerder (Lokale Beheerder) en door hen aangeduide Gebruikers zoals omschreven in artikel 3.2.e		
“Belcotax-on-web”	Nee	Ja
“PLDA – Paperless Douane en Accijnzen”.		

BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Toepassingen toegankelijk voor elke gebruiker zoals omschreven in artikel 3.3.a		
"Authentieke Bron Implanteerbare Medische Hulpmiddelen	Voor deze toepassingen is geen digitale sleutel vereist	
Pharma formulary		
" en "Healthdata.be Data Reporting"		
Centraal reservatiesysteem COV19 (via reservatiecode)		
Toepassingen toegankelijk voor elke gemachtigd gebruiker afhankelijk van zijn hoedanigheid zoals omschreven in artikel 3.3.b		
"BHOD - beschikbaarheidshonoraria"	Ja	Ja
"CEBAM Digital Library for Health / DCLH / EBMPRACTICENET",		
"E-loket Zorg en Gezondheid",	Nee	Ja
"WebWachtMailer"		
"eHealth Web Application for File Exchange for Batch applications (WebFX)";		
"eTCT - Feedback aan de ziekenhuizen over de door hen verstrekte zorg en de kost ervan",		
UPPAD		
"BINC (Begeleiding in Cijfers) - Online registratiesysteem voor de private voorzieningen uit de sector Bijzondere Jeugdzorg",		
"Platform Welzijn en Gezondheid";		
"Interface for communication on experiments between sponsors, ethics committees and the competent authority (ICE-SEC)",		
Toepassingen toegankelijk voor elke gemachtigd gebruiker zoals omschreven in artikel 3.3.c		
"Elektronische gegevensuitwisseling voor het Vlaams Agentschap Zorg & Gezondheid (VESTA)",	Nee	Ja
"Kankerregistratie",		
"Technische Cel via het web (eTCT)",		
"Elektronische geboorteaangifte (eBirth)",		
"Raadplegen van de verzekerbaarheid van een persoon",		
"Doorsturen van facturen derde betaler",		
"eBox Update Info",		
"Project on Cancer of the Rectum, online applicatie voor de registratie van rectumkanker (PROCARE DATA ENTRY)"		
"Medic-e intern - Elektronische invoer en raadpleging van de evaluatie van de personen met een handicap";		
"Tool for Administrative Reimbursment Drugs Information Sharing " (TARDIS),	Nee	Ja
"ODEA"		

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Toepassingen toegankelijk voor elke gemachtigd gebruiker zoals omschreven in artikel 3.3.c		
"Raadpleging van de wilsverklaring inzake euthanasie - eutha-consult",	Nee	Ja
"ORTHOpedic Prosthesis Identification Data - Electronic Registry - ORTHOpride®",		
"Project on cancer of the rectum - Central Image Repository (PROCARE RX)",		
"Qermid(c)Pacemakers-Quality Electronic Registration of Medical Implant Devices",		
"SMUREG",		
"Medico-Administratieve Stromen – Thuisverpleging (MEDADM-INF)",		
"ZNA - Zorgportaal – SARAi",		
"Registratie van Therapeutische Projecten (TherPro – PatientRegistration)",		
"BHOD - beschikbaarheidshonoraria",		
"QermidDefibrilateur-Quality Electronic Registration of Medical Implant Devices",		
"eHealthBox",		
"QermidEndoprothèses-Quality Electronic Registration of Medical Implant Devices",		
"QermidPacemakers-Quality Electronic Registration of Medical Implant Devices",		
"QermidTuteurs Coronaires-Quality Electronic Registration of Medical Implant Devices",		
"Registratiemodule van de Belgische Virtuele Tumorbank",		
"Catalogus van de Belgische Virtuele Tumorbank",		
"CIVARS – Chapter IV Agreement Requesting System",		
"Web Application Metahub",		
"Raadpleging van medische kaart",		
"TDI - Registratie Module van de "Treatment Demand Indicator"",		
"eShop - Online bestelling getuigschriften voor verstrekte hulp (Medattest)",		
"BNMDR - Belgian NeuroMuscular Disease Registry", "eHealthConsent",		
"Moduledatabank Jeugdhulp Vlaanderen",		
"Authentieke bron geneesmiddelen",		
"Insisto - Informaticasysteem Intersectorale Toegangspoort",		
"Raadpleging van het recht GMD",		
PCR Prescription validation		
"DOMINO",		

	UID/PWD +toekomstige (Laag)	eID ITSME MyGov.be X509 cert TOTP eIDAS +toekomstige (Substantieel & Hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Toepassingen toegankelijk voor elke gemachtigd gebruiker zoals omschreven in artikel 3.3.c		
"Centraal Traceringsregister",	Nee	Ja
"eTarif",		
"eHealthOCC",		
"Statistiek Jongerenwelzijn",		
"GKB2.0 - Gemeenschappelijk KlantenBestand",		
"PARIS (Prescription & Autorisation Requesting Information System)",		
"BelRAI",		
"eHealth API portal"		
eHealthCreaBis		
BelRAI Vlaanderen		
Corona Vaccination - App voor aangifte van patiënten met zeldzame/complexe aandoeningen		
Corona Test prescription & Consultation		
MyRIZIV		
Heracles		
MediPrima		
Software Register - officieel en gedeeld kadaster van gezondheidssoftware	Nee	Ja

Bijlage 4 - Gebruik van de authentieke bron geneesmiddelen door softwareontwikkelaars

1.Inleiding

Het eHealth-platform stelt via zijn portaalsite de Authentieke Bron Geneesmiddelen ter beschikking.

De Authentieke Bron Geneesmiddelen bevat gegevens komende van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG) en het Rijksinstituut voor ziekte- en invaliditeitsverzekering (RIZIV).

2. Terbeschikkingstelling aan softwareontwikkelaars

Softwareontwikkelaars die erkende of geregistreerde softwarepakketten voor zorgverleners ontwikkelen, kunnen de Authentieke Bron Geneesmiddelen in zijn geheel via de portaalsite van het eHealth-platform downloaden.

De modaliteiten voor de terbeschikkingstelling van eventuele updates zullen worden gepubliceerd op de portaalsite van het eHealth-platform.

3. Gebruik van de Authentieke Bron Geneesmiddelen

De softwareontwikkelaars mogen de Authentieke Bron Geneesmiddelen uitsluitend gebruiken voor de integratie ervan in hun erkende of geregistreerde softwarepakketten voor zorgverleners.

Met uitzondering van de eventuele kost van de technische integratie van de Authentieke Bron Geneesmiddelen in de softwarepakketten, is het de softwareontwikkelaars verboden om een vergoeding te bekomen voor de terbeschikkingstelling van de inhoud van de Authentieke Bron Geneesmiddelen aan de gebruikers van de softwarepakketten.

De inhoud van de Authentieke Bron Geneesmiddelen mag op geen enkele wijze worden aangewend voor publicitaire of commerciële doeleinden door de softwareontwikkelaars of door derden.

De intellectuele rechten of auteursrechten voor de gegevens opgenomen in de Authentieke Bron Geneesmiddelen behoren exclusief toe aan de partijen die de gegevens aan de Authentieke Bron Geneesmiddelen hebben verstrekt, zijnde onder andere het FAGG en het RIZIV.

Het is de softwareontwikkelaars verboden de gegevens die opgenomen zijn in de Authentieke Bron Geneesmiddelen te wijzigen door de inhoud, geheel of gedeeltelijk, te verwijderen of te wijzigen.

Het is de softwareontwikkelaars toegestaan om de Authentieke Bron Geneesmiddelen te verrijken met andere gegevens doch uitsluitend onder hun eigen verantwoordelijkheid en met uitdrukkelijke vermelding hiervan aan de gebruikers.

4. Verantwoordelijkheden

Het FAGG, het RIZIV, het eHealth-platform en elke andere bij de samenstelling en terbeschikkingstelling van de Authentieke Bron Geneesmiddelen betrokken partij, stellen alles

in het werk voor een correcte samenstelling en terbeschikkingstelling van de Authentieke Bron Geneesmiddelen, zonder echter enige resultaatsverbintenis op dat vlak aan te gaan.

Het FAGG, het RIZIV, het eHealth-platform en elke andere bij de samenstelling en terbeschikkingstelling van de Authentieke Bron Geneesmiddelen betrokken partij, zijn volledig vrijgesteld van eender welke aansprakelijkheid voor het concrete gebruik van de informatie die beschikbaar is in de Authentieke Bron Geneesmiddelen. Ze kunnen in geen geval aansprakelijk worden gesteld voor eender welke vorm van schade, direct of indirect, secundair of bijkomstig, materieel of immaterieel, veroorzaakt bij de gebruiker of derden, voortkomend uit het gebruik van de Authentieke Bron Geneesmiddelen of de onmogelijkheid om het te gebruiken.

5. Inbreuken en schadevergoeding

Voor iedere inbreuk op de gebruiksvoorwaarden is de betrokken softwareontwikkelaar een schadevergoeding van € 50.000 verschuldigd aan het FAGG, het RIZIV en het eHealth-platform ten gezamenlijke titel.

Indien het eHealth-platform, het FAGG of het RIZIV een inbreuk op één of meerdere van voorliggende gebruiksvoorwaarden door een softwareontwikkelaar vaststelt, zal het de betrokken softwareontwikkelaar hiervan inlichten. De softwareontwikkelaar is er vervolgens toe gehouden om het gebruik van de Authentieke Bron Geneesmiddelen onmiddellijk en onherroepelijk te staken, en dit op straffe van een bijkomende schadevergoeding van € 5.000 aan voormelde partijen per dag dat de softwareontwikkelaar in gebreke blijft.