

## **GEBRUIKSVORWAARDEN MIJN DIGITALE SLEUTELS**

### **Artikel 1 - Toepassingsgebied van deze gebruiksvoorwaarden**

Deze gebruiksvoorwaarden regelen de procedure die door de federale overheid wordt aangeboden voor de elektronische registratie, identificatie en authenticatie van eindgebruikers, al dan niet burgers. Via deze procedure kunnen eindgebruikers zich registreren met het oog op een veilige toegang tot elektronische diensten van de overheid en een veilige elektronische communicatie met de overheid.

Niettemin blijft het mogelijk dat sommige publieke instanties beroep doen op andere systemen voor elektronisch eindgebruikersbeheer.

### **Artikel 2 - Toegang tot de procedure**

De eindgebruiker heeft toegang tot de procedure zonder dat evenwel gewaarborgd wordt dat de toegang tot de procedure en de aangeboden diensten ten allen tijde verzekerd is en vrij is van fouten of technische storingen.

De toegang tot de procedure kan te allen tijde geheel of gedeeltelijk worden afgesloten (onder meer voor onderhoudsdoeleinden). Voor zover redelijkerwijze mogelijk zal de eindgebruiker van dergelijke onderbreking op voorhand op de hoogte worden gebracht.

De eindgebruiker heeft slechts toegang tot bepaalde diensten aangeboden door de overheid nadat hij de procedure voor registratie, identificatie en authenticatie die van toepassing is, heeft gevolgd.

Daarbij zal de eindgebruiker:

- zich akkoord verklaren met onderhavige gebruiksvoorwaarden;
- een correct e-mail adres meedelen.

De eindgebruiker is ertoe gehouden de gegevens die hem betreffen zo nodig aan te passen, zodat deze op elk moment actueel en correct zijn.

### **Artikel 3 - Gebruik van digitale sleutels**

De toegang van de eindgebruiker tot bepaalde langs elektronische weg aangeboden diensten vereist het gebruik van digitale sleutels (eID kaartlezer, draadloze eID kaartlezer, beveiligingscode via mobiele app/SMS/token en gebruikersnaam en wachtwoord, ...).

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, token 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 zoals voorgeschreven onder andere in artikel 6.

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

**Artikel 4 - Gebruik van het e-mailadres**

De eindgebruiker is verantwoordelijk voor de keuze van het e-mailadres dat hij heeft meegedeeld. Hij verklaart dat dit e-mailadres hem toebehoort en dat derden er geen gebruik van kunnen maken zonder zijn toestemming.

De eindgebruiker bevestigt dit adres regelmatig te gebruiken.

**Artikel 5 - Gebruik van de procedure**

Elke eindgebruiker is ertoe gehouden om:

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.

**Artikel 6** - Procedure in geval van verlies of wijziging van een digitale sleutel of een onderdeel van een digitale sleutel

In geval van verlies of diefstal van een identiteitskaart, is de titularis ertoe gehouden zo snel mogelijk aangifte te doen bij de bevolkingsdienst van zijn gemeente of de dichtstbij zijnde politiedienst, of contact op te nemen met de dienst DocStop van de FOD Binnenlandse Zaken.

In geval een eindgebruiker zijn smartphone of GSM verliest, of deze gestolen wordt, is hij ertoe gehouden zo snel mogelijk aangifte te doen bij zijn service provider. Daarnaast dient hij in "Mijn digitale sleutels" de betreffende sleutels te verwijderen (beveiligingscode via mobiele app en/of beveiligingscode via SMS).

In geval een eindgebruiker een nieuw Gsm-nummer wenst te gebruiken, is hij ertoe gehouden eerst in "Mijn digitale sleutels" de sleutel "beveiligingscode via SMS" voor het oude nummer te verwijderen.

In geval een eindgebruiker zijn MYDIGIPASS account opzegt, is hij ertoe gehouden in "Mijn digitale sleutels" de sleutel "draadloze eID kaartlezer" te verwijderen.

In geval een eindgebruiker zijn token verliest, dient hij het te deactiveren en kan hij een nieuw token aanvragen via "Mijn digitale sleutels". In geval van een nieuwe aanvraag, zal het systeem een nieuw token genereren dat per traditionele post zal worden verstuurd naar het officiële adres van de eindgebruiker, zoals opgenomen in het Rijksregister. Het oude token zal zo snel mogelijk gedeactiveerd worden en zal vanaf dan niet meer bruikbaar zijn.

**Artikel 7** - Bescherming van de persoonlijke levenssfeer

Def overheid draagt zorg voor uw privacy en handelt hierbij steeds in overeenstemming met de bepalingen van de Belgische privacywet (*Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*).

Door gebruik te maken van deze registratieprocedure geeft de eindgebruiker ondubbelzinnig zijn toestemming voor het gebruik van zijn persoonsgegevens. Hij erkent dat het verwerken van deze persoonsgegevens relevant en noodzakelijk is om een correcte en veilige identificatie en authenticatie toe te laten zodat een veilig gebruikersbeheer en een elektronische communicatie tussen de eindgebruiker en de overheid mogelijk worden.

De eindgebruiker geeft uitdrukkelijk de toestemming om zijn rijksregisternummer op te slaan in het systeem en erkent dat het bewaren van dit nummer noodzakelijk en relevant is voor de goede werking van het systeem. FOD Beleid en Ondersteuning – DG Digitale Transformatie beschikt daartoe over de nodige machtigingen uitgereikt door het Sectoraal comité van het Rijksregister.

Sommige identificatiegegevens worden geconsulteerd in het Rijksregister of in het BIS-register. FOD Beleid en Ondersteuning – DG Digitale Transformatie beschikt daartoe over de nodige machtigingen.

FOD Beleid en Ondersteuning – DG Digitale Transformatie is verantwoordelijk voor de verwerking van deze persoonsgegevens en ziet toe op de vertrouwelijkheid en de veiligheid van de gegevens. FOD Beleid en Ondersteuning – DG Digitale Transformatie is verantwoordelijk voor het beantwoorden van vragen betreffende de bescherming van persoonsgegevens. De persoonsgegevens die de eindgebruiker ingeeft, worden verzonden over het internet via het SSL protocol. De persoonsgegevens worden slechts ter beschikking gesteld aan andere overheidsdiensten die gebruik maken van de dienst om eindgebruikers te identificeren, authentifieren en toegang te verlenen tot hun online diensten. De dienst kan

slechts gebruikt worden door de andere overheidsdiensten indien zij over de nodige machtigingen uitgereikt door het Sectoraal comité van het Rijksregister beschikken.

De eindgebruiker heeft steeds het recht om de verwerking van de door hem ingegeven persoonsgegevens stop te zetten door zich uit te schrijven.

De privacy audit trail zorgt er voor dat aanmeldingen en pogingen tot aanmeldingen kunnen worden gereconstrueerd ter naleving van de wettelijke verplichting (artikel 16§4 van de Wet van 8 december 1992) om de persoonsgegevens afdoende te beveiligen.

FOD Beleid en Ondersteuning – DG Digitale Transformatie maakt gebruik van cookies om de prestaties van de website te verbeteren, functionele cookies voor de gebruiksvriendelijkheid en tijdelijke sessiecookies noodzakelijk voor de authenticatie tijdens de sessie. Je kunt de cookies weigeren, maar dan zullen sommige onderdelen van onze websites niet of niet optimaal werken.

Noodzakelijke cookies

Deze cookies zijn onmisbaar om op een veilige manier jouw identiteit te controleren en je op basis daarvan toegang te geven tot de toepassingen waartoe je toegang wenst te bekomen.

Functionele cookies

De functionele cookies zijn cookies die het functioneren van de websites en de gebruiksvriendelijkheid verbeteren. FOD Beleid en Ondersteuning – DG Digitale Transformatie gebruikt cookies om jouw taalvoorkeur te onthouden.

Cookies voor websiteprestaties

FOD Beleid en Ondersteuning – DG Digitale Transformatie gebruikt load balancing cookies. Ze worden gebruikt bij websites die veel worden bezocht en dienen om de lasten van de aanvragen te verdelen over meerdere, aparte netwerken en servers.

Via de browserinstellingen kan men cookies weigeren.

### **Artikel 8 - Definities**

Voor de doeleinden van deze gebruiksvoorwaarden worden de onderstaande begrippen als volgt omschreven:

- **Registratie** - Het proces waarbij een persoon zich - via het doorlopen van een voorgeschreven procedure - in een lijst laat opnemen, en daardoor te kennen geeft dat hij/zij gebruik wil maken van een bepaalde dienst.
- **Identificatie** - Een proces dat wordt gebruikt om de identiteit van een bepaalde persoon vast te stellen.
- **Authenticatie** - Proces dat gebruikt wordt om de identiteit van een bepaalde persoon te bevestigen. Een persoon kan bijvoorbeeld door het verschaffen van bepaalde vertrouwelijke gegevens die enkel aan hem/haar bekend zijn (bijv. een zelf gekozen wachtwoord) bevestigen dat hij/zij wel degelijk de persoon is die hij/zij beweert te zijn.