NUTZUNGSBEDINGUNGEN MEINE DIGITALEN SCHLÜSSEL

Artikel 1 - Geltungsbereich dieser Nutzungsbedingungen

Diese Nutzungsbedingungen regeln das Verfahren, das von der Föderalbehörde für die elektronische Registrierung, Identifikation und Authentifizierung von Endbenutzern angeboten wird, ungeachtet dessen, ob diese Bürger sind oder nicht. Mittels dieses Verfahrens können sich Endbenutzer für einen sicheren Zugang zu elektronischen Behördendiensten und eine sichere elektronische Kommunikation mit den Behörden registrieren.

Dennoch ist es möglich, dass einige öffentliche Instanzen weiterhin andere Systeme für elektronische Benutzerverwaltung in Anspruch nehmen.

Artikel 2 - Zugang zum Verfahren

Der Endbenutzer hat Zugang zum Verfahren, ohne dass jedoch gewährleistet wird, dass der Zugang zum Verfahren und den angebotenen Diensten jederzeit garantiert und frei von Fehlern und technischen Störungen ist.
Der Zugang zum Verfahren kann jederzeit gänzlich oder teilweise blockiert werden (unter anderem für Wartungszwecke). Sofern berechtigterweise möglich, wird der Endbenutzer im Vorhinein über eine derartige Unterbrechung informiert.
Der Endbenutzer hat erst Zugang zu bestimmten von der Behörde angebotenen Diensten, nachdem er das geltende Verfahren für die Registrierung, Identifikation und Authentifizierung verfolgt hat.
Dabei wird der Endbenutzer:
· sich mit vorliegenden Nutzungsbedingungen einverstanden erklären;
· eine korrekte E-Mailadresse mitteilen.

Der Endbenutzer ist dazu verpflichtet, die ihn betreffenden Daten nötigenfalls anzupassen, sodass diese jederzeit aktuell und korrekt sind.

Artikel 3 - Verwendung digitaler Schlüssel

Der Zugang des Endbenutzers zu bestimmten auf elektronischem Wege angebotenen Diensten erfordert die Verwendung digitaler Schlüssel (eID-Kartenleser, drahtloser eID-Kartenleser, Sicherheitscode mittels mobiler App/SMS/Token und Benutzername und Passwort, …).
Diese digitalen Schlüssel und die damit verbundenen Daten sind strikt persönlich und nicht übertragbar.
Jeder Endbenutzer ist für die gute Aufbewahrung, Sicherung, Geheimhaltung und Verwaltung seiner digitalen Schlüssel und der damit verbundenen Daten verantwortlich.

Der Endbenutzer ist für die Wahl eines sicheren Passwortes oder eines anderen geheimen Codes verantwortlich.
Wenn ein Endbenutzer feststellt, dass er den Benutzernamen, das Passwort, den Token oder einen anderen digitalen Schlüssel verloren hat oder dass ein Dritter diese ohne Erlaubnis nutzt oder wenn er einen derartigen Verlust oder eine derartige unzulässige Nutzung vermutet,

muss er unverzüglich alle nötigen Maßnahmen treffen, um den digitalen Schlüssel zu deaktivieren, wie dies unter anderem in Artikel 6 vorgeschrieben ist.

Im Fall einer Verriegelung seines digitalen Schlüssels muss der Endbenutzer einen neuen beantragen.

Artikel 4 - Nutzung der E-Mailadresse
Der Endbenutzer ist für die Wahl der E-Mailadresse verantwortlich, die er mitgeteilt hat. Er erklärt, dass ihm diese E-Mailadresse gehört und dass Dritte diese nicht ohne seine Zustimmung nutzen können.

Der Endbenutzer bestätigt, diese Adresse regelmäßig zu verwenden.

Artikel 5 - Anwendung des Verfahrens
Jeder Endbenutzer ist verpflichtet:
1. vollständige, genaue, wahre und nicht-irreführende Informationen bereitzustellen;

2. die durch Gesetze, Vorschriften, Dekrete, Verordnungen oder Erlässe der föderalen, regionalen, lokalen oder internationalen Behörden vorgeschriebenen Bestimmungen zu befolgen;

3. auf die Manipulation der gelieferten Informationen, ungeachtet auf welche Weise und mit welcher Technik, zu verzichten.

Artikel 6 - Verfahren bei Verlust oder Änderung eines digitalen Schlüssels oder eines Bestandteils eines digitalen Schlüssels

Bei Verlust oder Diebstahl einer Identitätskarte ist der Inhaber dazu verpflichtet, dies so schnell wie möglich beim Bevölkerungsdienst seiner Gemeinde oder der nächstgelegenen Polizeidienststelle zu melden oder Kontakt mit dem Dienst DocStop der FÖD Innere Angelegenheiten aufzunehmen.

Falls ein Endbenutzer sein Smartphone oder Handy verliert oder wenn dieses gestohlen wird, ist er dazu verpflichtet, dies so schnell wie möglich bei seinem Serviceprovider zu melden. Darüber hinaus muss er in "Meine digitalen Schlüssel" die betreffenden Schlüssel löschen (Sicherheitscode mittels mobiler App und/oder Sicherheitscode mittels SMS).

Falls ein Endbenutzer eine neue Handynummer verwenden möchte, ist er dazu verpflichtet, zuerst in "Meine digitalen Schlüssel" den Schlüssel "Sicherheitscode mittels SMS" für die alte Nummer zu löschen.

Falls ein Endbenutzer sein MYDIGIPASS-Konto kündigt, ist er dazu verpflichtet, in "Meine digitalen Schlüssel" den Schlüssel "Drahtloser eID-Kartenleser" zu löschen.

Falls ein Endbenutzer seinen Token verliert, muss er diesen deaktivieren und kann er mittels "Meine digitalen Schlüssel" einen neuen Token anfordern. Bei einem neuen Antrag wird das System einen neuen Token generieren, der per Post an die offizielle Adresse des Endbenutzers gesendet wird, gemäß den Angaben des Nationalregisters. Der alte Token wird so schnell wie möglich deaktiviert und kann ab diesem Zeitpunkt nicht mehr verwendet werden.

Artikel 7 - Schutz der persönlichen Privatsphäre
Die Behörde sorgt für Ihre Privatsphäre und handelt dabei stets in Übereinstimmung mit den Bestimmungen des belgischen Datenschutzgesetzes *(Gesetz vom 8. Dezember 1992 zum Schutz der Privatsphäre im Hinblick auf die Verarbeitung von Personendaten)*.
Durch Anwendung dieses Registrierungsverfahrens erteilt der Endbenutzer unmissverständlich seine Zustimmung zur Verwendung seiner Personendaten. Er anerkennt, dass die Verarbeitung dieser Personendaten relevant und notwendig ist, um eine korrekte und sichere Identifikation und Authentifizierung zu ermöglichen, sodass eine sichere Benutzerverwaltung und eine elektronische Kommunikation zwischen dem Endbenutzer und der Behörde möglich werden.
Der Endbenutzer erteilt ausdrücklich die Zustimmung, seine Nationalregisternummer im System zu speichern und erklärt, dass das Speichern dieser Nummer notwendig und relevant für die gute Funktion des Systems ist. FOD Beleid en Ondersteuning – DG Digitale Transformatie verfügt zu diesem Zweck über die nötigen Bevollmächtigungen, ausgestellt vom sektoriellen Ausschuss des Nationalregisters.
Einige Identifikationsdaten werden im Reichsregister oder im BIS-Register abgerufen. FOD Beleid en Ondersteuning – DG Digitale Transformatie verfügt diesbezüglich über die nötigen Vollmachten.
FOD Beleid en Ondersteuning – DG Digitale Transformatie ist für die Verarbeitung dieser Personendaten verantwortlich und beaufsichtigt die Vertraulichkeit und Sicherheit der Daten.
FOD Beleid en Ondersteuning – DG Digitale Transformatie ist für die Beantwortung von Fragen über den Schutz von Personendaten verantwortlich. Die vom Endbenutzer eingegebenen Personendaten werden mittels dem SSL-Protokoll über Internet gesendet. Die Personendaten werden nur anderen Behörden zur Verfügung gestellt, die den Dienst verwenden, um Endbenutzer zu identifizieren, authentifizieren und Zugang zu ihren Online-Diensten zu

erteilen. Der Dienst kann von den anderen Behörden nur verwendet werden, wenn sie über die nötigen Vollmachten des sektoriellen Ausschusses des Nationalregisters verfügen.

Der Endbenutzer hat stets das Recht, die Verarbeitung der von ihm eingegebenen Personendaten zu beenden, indem er sich abmeldet.

Die Datenschutz-Prüfungskette sorgt dafür, dass Anmeldungen und Anmeldeversuche zur Einhaltung der gesetzlichen Verpflichtung rekonstruiert werden können (Artikel 16§4 des Gesetzes vom 8. Dezember 1992), um die Personendaten ausreichend zu schützen.

Für die Anwendung "Anmeldung bei der Online-Behörde" nutzt FOD Beleid en Ondersteuning – DG Digitale Transformatie Cookies zur Verbesserung der Leistungen der Website, funktionelle Cookies für die Benutzerfreundlichkeit und vorübergehende Sitzungscookies, die für die Authentifizierung während der Sitzung erforderlich sind. Sie können die Cookies ablehnen, aber dann werden einige Bestandteile unserer Websites nicht oder nicht optimal funktionieren.

Notwendige Cookies

Diese Cookies sind unverzichtbar, um Ihre Identität auf sichere Weise zu kontrollieren und Ihnen auf Basis davon Zugang zu den Anwendungen zu gewähren, zu denen Sie Zugang wünschen.

Funktionelle Cookies

Die funktionellen Cookies sind Cookies, die die Funktion von Websites und die Benutzerfreundlichkeit verbessern. FOD Beleid en Ondersteuning – DG Digitale Transformatie verwendet Cookies, um Ihre Sprachpräferenzen zu speichern.

Cookies für Website-Leistungen

FOD Beleid en Ondersteuning – DG Digitale Transformatie verwendet "Load balancing"-Cookies. Diese werden bei Websites verwendet, die häufig besucht werden und dienen dazu, die Lasten der Anfragen über mehrere, gesonderte Netzwerke und Server zu verteilen.

Mittels den Browser-Einstellungen kann man Cookies ablehnen.

Artikel 8 - Definitionen

Zum Zweck dieser Nutzungsbedingungen werden die nachfolgenden Begriffe wie folgt beschrieben:

- **Registrierung** - Der Prozess, bei dem sich eine Person - unter Einhaltung eines vorgeschriebenen Verfahrens - in einer Liste aufnehmen lässt und dadurch bekanntgibt, dass sie einen bestimmten Dienst in Anspruch nehmen möchte.
- **Identifikation** - Ein Prozess, der verwendet wird, um die Identität einer bestimmten Person festzustellen.
- **Authentifizierung** - Prozess, der verwendet wird, um die Identität einer bestimmten Person zu bestätigen. Eine Person kann beispielsweise durch die Erteilung bestimmter vertraulicher Daten, die nur ihr bekannt sind (z.B. ein selbst gewähltes Passwort) bestätigen, dass sie sehr wohl die Person ist, die sie zu sein behauptet.