

## **Benutzerordnung betreffend den Zugang zum Informationssystem der föderalen Behörde und der öffentlichen Einrichtungen der sozialen Sicherheit und die Nutzung dieses Systems durch Unternehmen und ihre Bevollmächtigten**

### **Artikel 1 - Anwendungsbereich**

Diese Benutzerordnung regelt den Zugang zum Informationssystem der föderalen Behörde und der öffentlichen Einrichtungen der sozialen Sicherheit (hiernach Informationssystem genannt) und zu den dadurch angebotenen Dienstleistungen, und die Nutzung dieses Systems durch Unternehmen und ihre Bevollmächtigten.

### **Artikel 2 – Verpflichtung zur Bestimmung eines lokalen Verwalters**

Jedes Unternehmen, das auf das Informationssystem zugreifen und dieses nutzen möchte, muss einen einzigen lokalen Verwalter bestimmen.

### **Artikel 2 bis - Definition**

Mit „Elektronischem Personalausweis“ im Sinne dieser Benutzerordnung ist der elektronische Personalausweis im Sinne der Artikel 6ff des Gesetzes vom 19. Juli 1991 über die Bevölkerungsregister und die Personalausweise und zur Abänderung des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen gemeint, auf dem die Identitäts- und Signaturzertifikate aktiviert wurden.

### **Artikel 3 – Angebotene Dienstleistungen und verfügbare Kanäle**

Die angebotenen Dienstleistungen sind über verschiedene Kanäle zugänglich.

1. Über den vokal Server kann jeder Benutzer eine Dimona-Meldung vornehmen.
2. Über die Portalsite der Sozialen Sicherheit ([www.soziale-sicherheit.be](http://www.soziale-sicherheit.be))
  - a) hat jeder Benutzer Zugang zu den Anwendungen „Dimona“, „Entsendungsanträge“ (Gotot), „Arbeitsmeldungen“, die „Einbehaltungspflicht 30bis“, das „elektronische Formular für den Zugangsantrag“ und die „öffentliche Abfrage des Arbeitgeberrepertorium“;
  - b) hat jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde und über einen Benutzernamen und ein Kennwort verfügt, Zugang zur Anwendung „Routing Consult“;

- c) hat jeder Konkursverwalter, der zum lokalen Verwalter bestimmt wurde, oder jeder Benutzer, der durch diesen Konkursverwalter bestimmt worden ist und über einen Benutzernamen und ein Kennwort verfügt, Zugang zur Anwendung „WEBCUR“;
- d) hat jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde und über einen Benutzernamen und ein Kennwort verfügt, entweder nach dem Eingeben dieses Benutzernamens und dieses Kennworts oder ohne dass er diese eingibt, wenn er einen elektronischen Personalausweis benutzt, Zugang zu den Anwendungen „Abfrage der E-Box“, „Personalbestand“, „LSS-Meldung (DmfA)“, „LSSPLV-Meldung (DmfAPLV)“, „Meldung Sozialrisiken (MSR)“, „Abfrage Arbeitsmeldungen“, „Vorübergehende Arbeitslosigkeit und Validierungsbuch“, „Gesicherte Abfrage des Arbeitgeberrepertoriums“, „Beiträge für die öffentlichen Mandate“, Routing-Regeln“ und „Abfrage des Urlaubsbestands“;
- e) hat jeder Benutzer, der durch den lokalen Verwalter eines Unternehmens bestimmt wurde und entweder über einen Benutzernamen sowie ein Kennwort oder über einen elektronischen Personalausweis verfügt, Zugang zu den Anwendungen, zu denen er durch den lokalen Verwalter eines Unternehmens ermächtigt wurde, ohne dass diese Zugangsmöglichkeiten die des lokalen Verwalters überschreiten;
- f) hat jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde oder der durch den lokalen Verwalter eines Unternehmens bestimmt wurde und der entweder über einen Benutzernamen, ein Kennwort, einen Privatschlüssel und ein qualifiziertes Zertifikat im Sinne von Artikel 2,4° des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste oder einen anderen Zertifikatstyp verfügt, der in der Liste der akzeptierten Zertifikate auf der Portalsite der sozialen Sicherheit angegeben wurde, oder über einen elektronischen Personalausweis verfügt, außerdem Zugang zu den Anwendungen „Änderung einer LSS-Meldung (DmfA)“ oder „Änderung einer LSSPLV-Meldung (DmfAPLV)“.

### 3. Über die Portalsite der föderalen Behörde ([www.belgium.be](http://www.belgium.be))

- a) hat jeder Benutzer Zugang zu den Anwendungen „Abfragen von Informationen der Unternehmen“;
- b) hat jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde und über einen Benutzernamen sowie ein Kennwort verfügt, Zugang zu den Anwendungen „Abfragen von Informationen meines Unternehmens“, „Umfrage zum Verkehr zwischen dem Wohnort und dem Ort des Arbeitsplatzes“, „Fonds Online“, „Vigilis (e-Schalter)“ und „Die Eindeutige Startermeldung“ (DEUS);
- c) hat jeder Benutzer, der durch den lokalen Verwalter eines Unternehmens bestimmt wurde und über einen Benutzernamen, ein Kennwort und das Verzeichnisnummer des Auftraggebers verfügt, Zugang zu den Anwendungen „Tax-on-web“ (TOW) und „Abfrage der Tax-on-web-Meldung“ für die Personen, für die er über eine Vollmacht verfügt, um diese Anwendungen auf ihre Rechnung und in ihrem Namen zu verwenden und von denen er dieses Mandat der regionalen Direktion der direkten Steuern zur Verfügung gestellt hat, die für das Finanzamt des Auftraggebers befugt ist;

- d) hat jeder Benutzer, der durch den lokalen Verwalter eines Unternehmens bestimmt wurde und über einen Benutzernamen sowie ein Kennwort und in Bezug auf die Anwendungen im Sinne von Punkt 3c) über die Verzeichnisnummer des Auftraggebers verfügt, Zugang zu den Anwendungen, zu denen er durch den lokalen Verwalter eines Unternehmens ermächtigt wurde, ohne dass diese Zugangsmöglichkeiten die des lokalen Verwalters überschreiten;
  - e) hat jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde oder der durch den lokalen Verwalter eines Unternehmens bestimmt wurde und der entweder über einen Benutzernamen, ein Kennwort, einen Privatschlüssel und ein qualifiziertes Zertifikat im Sinne von Artikel 2, 4° des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste oder einen anderen Zertifikatstyp verfügt, der in der Liste der akzeptierten Zertifikate auf der Portalsite der Sozialen Sicherheit angegeben wurde, außerdem Zugang zu den Anwendungen „Belcotax-on-web“ und „PLDA – Paperless Douane en Accijnzen“.
4. Über Dateiübertragung gemäß (S)FTP, anhand von MQSeries oder anderen akzeptierten Kanälen kann jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde oder der durch einen lokalen Verwalter bestimmt wurde und der über einen Benutzernamen, ein Kennwort, einen Privatschlüssel und ein qualifiziertes Zertifikat im Sinne von Artikel 2, 4°, des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste oder einen anderen Zertifikatstyp verfügt, der in der Liste der akzeptierten Zertifikate auf der Portalsite der sozialen Sicherheit angegeben wurde, darunter das aktivierte Signaturzertifikat des elektronischen Personalausweises, Dimona-Meldungen, LSS-Meldungen (DmfA), LSSPLV-Meldungen (DmfAPLV), Entsendungsanträge (Gotot), Änderungen einer LSS-Meldung (DmfA), Änderungen einer LSSPLV-Meldung (DmfAPLV) und Meldungen von Sozialrisiken (MSR) vornehmen.

Der Inhalt der Dienstleistungen und der Zugang zu diesen Dienstleistungen können jederzeit geändert werden.

#### **Artikel 4 - Zugang zum Informationssystem**

Der Benutzer hat Zugang zum Informationssystem, ohne dass jedoch gewährleistet ist, dass der Zugang zum Informationssystem und den angebotenen Dienstleistungen jederzeit gesichert oder frei von Fehlern oder technischen Störungen ist.

Der Zugang zum Informationssystem und den angebotenen Dienstleistungen kann jederzeit ganz oder teilweise (u.a. zu Wartungszwecken) gesperrt werden. Wenn dies redlicherweise möglich ist, wird der Benutzer über eine derartige Unterbrechung im Voraus informiert.

Der Benutzer ist für die Bereitstellung und Wartung des Terminals verantwortlich, der zur Nutzung des Informationssystems erforderlich ist. Die Anbieter des Informationssystems sind nicht für den Terminal und dessen Nutzung verantwortlich und sind nicht verpflichtet, diesbezüglich irgendeine Unterstützung zu bieten.

## **Artikel 5 - Nutzung des Benutzernamens und des Kennwortes**

Ein Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde, erhält den Benutzernamen und das Kennwort in separaten Sendungen über Eranova, das Contact-Center der öffentlichen Einrichtungen der sozialen Sicherheit. Ein Benutzer, der nicht durch ein Unternehmen zum lokalen Verwalter bestimmt wurde, erhält den Benutzernamen und das Kennwort vom lokalen Verwalter eines Unternehmens.

Der Benutzername und das Kennwort sind strikt persönlich und nicht übertragbar.

Jeder Benutzer muss das Kennwort, das er vom Contact-Center der öffentlichen Einrichtungen der sozialen Sicherheit oder von einem lokalen Verwalter empfangen hat, möglichst schnell nach dem Empfang und auf jeden Fall bei der erstmaligen Nutzung ändern. Jeder Benutzer muss nachträglich sein Kennwort regelmäßig ändern.

Ein sicheres Kennwort besteht aus 15 Zeichen und enthält alphanumerische Zeichen und Symbole in einer Reihenfolge, die nicht leicht erraten werden kann. Jeder Benutzer muss dafür sorgen, dass das ausgewählte Kennwort diesen Anforderungen entspricht. Jeder Benutzer ist selbst für die Fälle haftbar, in denen ein Kennwort, das nicht gemäß diesen Regeln zusammengestellt wird, herausgefunden und/oder missbraucht wird.

Jeder Benutzer muss sorgfältig mit seinem Benutzernamen und Kennwort umgehen und ist diesbezüglich zur Geheimhaltung verpflichtet. Jeder Benutzer ist haftbar für jede diesbezügliche (un-)erlaubte Nutzung, einschließlich jeder Nutzung durch Dritte.

Wenn ein Benutzer Kenntnis vom Verlust seines Benutzernamens und/oder Kennworts oder von jeder unerlaubten Nutzung durch Dritte seines Benutzernamens und/oder Kennworts hat oder einen derartigen Verlust bzw. unerlaubte Nutzung vermutet, muss er unverzüglich alle erforderlichen Maßnahmen ergreifen.

Jeder Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde, ist unter anderem dazu verpflichtet, diesen Verlust oder diese unerlaubte Nutzung unverzüglich dem Contact-Center der öffentlichen Einrichtungen der Sozialen Sicherheit Eranova zu melden (unter der Rufnummer 02-511.51.51 oder über die Portalsite der sozialen Sicherheit ([www.sociale-sicherheit.be](http://www.sociale-sicherheit.be))). Möglichst bald nach Eingang dieser Meldung und sofern dies redlich ist, werden alle möglichen Anstrengungen unternommen, um den Benutzernamen und das Kennwort des Benutzers zu inaktivieren.

Jeder Benutzer, der nicht durch ein Unternehmen zum lokalen Verwalter bestimmt wurde, ist unter anderem dazu verpflichtet, diesen Verlust oder diese unerlaubte Nutzung unverzüglich dem lokalen Verwalter zu melden, von dem er diesen Benutzernamen und dieses Kennwort erhalten hat. Dieser muss möglichst bald nach Eingang dieser Meldung und sofern dies redlich ist, alle möglichen Anstrengungen unternehmen, um den Benutzernamen und das Kennwort des Benutzers zu inaktivieren.

Jeder Benutzer bleibt haftbar für den gesamten (direkten oder indirekten) Schaden, der durch die (erlaubte oder unerlaubte) Nutzung seines Benutzernamens und/oder Kennworts entsteht, die vor dem Zeitpunkt erfolgte, zu dem der Benutzername und das Kennwort inaktiviert wurden.

Im Falle einer Sperrung seines Benutzernamens und/oder Kennworts muss der Benutzer, der durch ein Unternehmen zum lokalen Verwalter bestimmt wurde, schriftlich einen neuen Benutzernamen und ein neues Kennwort bei Eranova, dem Contact-Center der öffentlichen Einrichtungen der sozialen Sicherheit beantragen, wonach er einen neuen Benutzernamen und ein neues Kennwort erhält.

## **Artikel 6 - Nutzung des Informationssystems**

In Bezug auf die Nutzung des Informationssystems und der über dieses System angebotenen Dienstleistungen ist jeder Benutzer dazu verpflichtet:

1. vollständige, akkurate, wahre und eindeutige Informationen zu erteilen;
2. die kraft Gesetz, Ordnung, Erlass, Verfügung oder Beschluss der föderalen, regionalen, lokalen oder internationalen Behörde vorgeschriebenen Bestimmungen zu respektieren;
3. die erteilten Informationen nicht zu manipulieren, wie auch immer oder mit welcher Technik auch immer;
4. über das Informationssystem keine Daten, Berichte oder Dokumente auf irgendwelche Weise zu versenden, bzw. Daten oder Dokumente über das Informationssystem zu senden:
  - a) bei denen die Rechte (worunter Persönlichkeitsrechte oder geistige Eigentumsrechte) von Dritten oder der Anbieter des Informationssystems verletzt werden;
  - b) deren Inhalt illegal, schädigend, verleumderisch, gewalttätig, obszön oder entehrend ist oder durch welche die Privatsphäre Dritter verletzt wird;
  - c) deren Nutzung oder Besitz durch den Benutzer kraft Gesetz oder durch Vertrag untersagt ist;
  - d) die Viren oder Anweisungen enthalten, welche den Anbietern des Informationssystems und/oder dem Informationssystem Schaden zufügen könnten und/oder die die per Informationssystem angebotenen Dienstleistungen beeinträchtigen oder stören könnten.

## **Artikel 7 - Nutzung des Zertifikats**

Um auf bestimmte Dienstleistungen zugreifen zu können, muss der Benutzer entweder über einen elektronischen Personalausweis oder, zusätzlich zu einem Benutzernamen und Kennwort über einen Privatschlüssel und ein qualifiziertes Zertifikat gemäß Art. 2, 4°, des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste oder einen anderen Zertifikatstyp verfügen, der in der Liste der akzeptierten Zertifikate auf der Portalsite der sozialen Sicherheit angegeben wurde.

Dieses Zertifikat kann auch für die Authentifizierung und das Setzen einer elektronischen Signatur im Sinne von Art.1322, Abs. 2 des Zivilgesetzbuchs verwendet werden. Wenn der Zugang auf die angebotenen Dienstleistungen aber über einen elektronischen Personalausweis erfolgt, wird die Authentifizierung durch das Identitätszertifikat der Karte vorgenommen und wird die elektronische Signatur über das Signaturzertifikat der Karte angebracht.

Sobald die Daten zur Erstellung der Signatur zusammengestellt sind, ist nur der Zertifikatsinhaber für die Vertraulichkeit dieser Daten verantwortlich. Wenn Zweifel über den Erhalt der Vertraulichkeit der Daten zum Erstellen einer Signatur besteht oder die im Zertifikat aufgenommenen Daten nicht mehr der Realität entsprechen, muss der Inhaber das Zertifikat widerrufen lassen. Wenn ein Zertifikat ungültig oder widerrufen wird, darf der Inhaber nach dem Fälligkeitsdatum des Zertifikats oder nach dem Widerruf die entsprechenden Daten zum Erstellen einer Signatur nicht mehr benutzen, um diese Daten zu unterzeichnen oder durch einen anderen Zertifizierungsdienstleister zertifizieren zu lassen.

Jeder Benutzer muss deshalb sorgfältig mit dem Privatschlüssel und dem Zertifikat sowie mit dem Kennwort umgehen, das gegebenenfalls erforderlich ist, um den Privatschlüssel und das Zertifikat zu benutzen. Der Benutzer ist haftbar für jede diesbezügliche (un-) erlaubte Nutzung, einschließlich jeder Nutzung durch Dritte. Der Benutzer muss den Privatschlüssel und das Zertifikat auf einem sicheren Träger aufbewahren, vorzugsweise auf einer Prozessor-Chipkarte, die den Privatschlüssel nicht exportieren kann.

Das Informationssystem kann Zertifikate und Typen validieren, die durch Zertifizierungsbehörden ausgestellt wurden, die auf der Liste der Portalsite der sozialen Sicherheit ([www.sociale-veiligheid.be](http://www.sociale-veiligheid.be)) stehen. Zertifikate, die durch andere Zertifizierungsbehörden ausgestellt wurden, können nur angenommen werden, nachdem die benötigten technischen Anpassungen am Informationssystem vorgenommen wurden, um diese Zertifikate zu validieren. Der Benutzer, der fest entschlossen ist, ein qualifiziertes Zertifikat gemäß Art. 2, 4° des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste zu benutzen, das durch eine Zertifizierungsbehörde ausgestellt wurde, die nicht auf der Portalsite der Sozialen Sicherheit angegeben wird, kann dies unter Nutzung seines Benutzernamens und Kennwortes über das dazu bestimmte Formular auf der Portalsite der sozialen Sicherheit melden. Sofern dies redlich ist und sofern die beteiligte Zertifizierungsbehörde die benötigte Mitarbeit gewährt, werden die erforderlichen Anstrengungen unternommen, damit das Informationssystem auch Zertifikate der genannten Zertifizierungsbehörde anerkennen kann. Sobald dies der Fall ist, können die Zertifikate der genannten Zertifizierungsbehörde benutzt werden.

### **Artikel 8 - Nutzung der elektronischen Signatur und Beweis (Benutzer mit Zertifikat)**

Berichte, die durch das Informationssystem versandt werden, werden durch den Benutzer, der entweder über ein qualifiziertes Zertifikat gemäß Art. 2, 4° des Gesetzes vom 9. Juli 2001 zur Festlegung bestimmter Regeln in Bezug auf rechtliche Rahmenbedingungen für elektronische Signaturen und Zertifizierungsdienste oder einen anderen Zertifikatstyp verfügt, der in der Liste der angenommenen Zertifikate auf der Portalsite der sozialen Sicherheit angegeben wurde, oder über einen elektronischen Personalausweis verfügt, mit einer elektronischen Signatur im Sinne von Art.1322, Abs. 2 des Zivilgesetzbuchs versehen.

Der Benutzer erkennt ausdrücklich an, dass alle Berichte, die über das Informationssystem versandt werden und mit der oben genannten elektronischen Signatur versehen sind, die gleiche gesetzliche Beweiskraft wie eine privatschriftliche Urkunde im Sinne des Zivilgesetzbuchs haben.

Der Benutzer erkennt ausdrücklich an, dass alle Informationen über Berichte, die durch die Anbieter des Informationssystems auf dauerhafte und nicht zu ändernde Weise gespeichert

werden, die gleiche gesetzliche Beweiskraft wie eine privatschriftliche Urkunde im Sinne des Zivilgesetzbuchs haben, bis das Gegenteil nachgewiesen wurde.

Der Benutzer erkennt ausdrücklich die Signatur als die seinige an, die anhand des Privatschlüssels und des ihm gewährten Zertifikats geleistet wurde, außer im Falle eines Missbrauchs, Verlustes oder Diebstahls, sofern das dazu vorgesehene Verfahren nicht eingehalten wird.

### **Artikel 9 - Kontrollpflicht des Benutzers**

Der Benutzer ist verantwortlich für die Kontrolle des Inhalts der durch ihn über das Informationssystem versandten Berichte und für die betreffende Betreuung anlässlich von Berichten, die durch die Anbieter des Informationssystems an den Benutzer gesandt werden und die sich auf den/die durch den Benutzer versandten Bericht(e) beziehen.

Der/die materielle(n) Fehler in einem vom Benutzer versandten Bericht, in einer Empfangsmeldung, die sich darauf bezieht oder in jedem anderen Bericht oder Dokument, der bzw. das sich auf den Benutzer bezieht und der bzw. das über das Informationssystem zugänglich ist, wird bzw. werden auf Verlangen des Benutzers über ein dazu vorgesehenes Berichtigungsverfahren korrigiert.

### **Artikel 10 - Geistige Eigentumsrechte**

Der Benutzer erkennt an und akzeptiert, dass das Informationssystem, die Dienstleistungen und die Software, die im Zusammenhang mit dem Informationssystem und den Dienstleistungen entwickelt wurde, durch geistige Eigentumsrechte geschützt werden (Urheberrecht, Markenrecht, Patentrecht usw.), von denen die Anbieter des Informationssystems (oder seine Lizenzerteiler) der/die Inhaber sind.

Der Benutzer erhält ein nicht exklusives Recht, das Informationssystem zu den in der Benutzerordnung beschriebenen Zwecken zu benutzen. Vorbehaltlich der ausdrücklichen Genehmigung ist es dem Benutzer nicht gestattet, das Informationssystem wie auch immer ganz oder teilweise zu kopieren (wie auch immer oder auf welchem Träger auch immer), zu ändern, zu übersetzen, zu verkaufen, zu vermieten, auszuleihen, der Öffentlichkeit mitzuteilen bzw. abgeleitete Werke der oben genannten Elemente erzeugen.

### **Artikel 11 - Übergangsmaßnahmen**

Zur Zeit kann das Signaturzertifikat des elektronischen Personalausweises nur über das System der Dateiübertragung gemäß (S)FTP, anhand von MQSeries oder mittels sonstiger zugelassener Kanäle verwendet werden; es gestattet keinen Zugang auf bzw. keine Nutzung der Dienste, die auf der Portalsite der sozialen Sicherheit und der föderalen Portalsite angeboten werden, außer der Benutzung der Applikation „elektronische Formular für den Zugangsantrag“.