Benutzerordnung betreffend den Zugriff auf das Informationssystem der Föderalbehörde und der öffentlichen Einrichtungen der Sozialen Sicherheit und die Benutzung dieses Systems durch Unternehmen und ihre Bevollmächtigten

Artikel 1 – Anwendungsbereich

Diese Benutzerordnung regelt den Zugriff auf das Informationssystem der Föderalbehörde und der öffentlichen Einrichtungen der Sozialen Sicherheit (nachfolgend Informationssystem genannt) und auf die dadurch angebotenen Dienstleistungen und die Benutzung dieses Systems durch Unternehmen und ihre Bevollmächtigten.

Artikel 2 – Verpflichtung zur Bestimmung eines Hauptzugangsverwalters

Jedes Unternehmen, das auf das Informationssystem zugreifen und dieses benutzen möchte, muss nur einen einzigen Hauptzugangsverwalter bestimmen.

Artikel 2 bis – Definitionen

Mit „Elektronischem Personalausweis“ im Sinne dieser Benutzerordnung ist der elektronische Personalausweis im Sinne der Artikel 6 ff. 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.

Mit Zugangsverwalter oder lokalem Verwalter ist (sind) in dieser Benutzerordnung die natürliche(n) Person(en) gemeint, die innerhalb des Unternehmens dazu bestimmt wird (werden), die Benutzer- und Zugangsregelung auf ihrer Ebene zu gewährleisten, unabhängig davon, ob diese Person(en) nun als Hauptzugangsverantwortlicher, Haupt-(Mit-)Zugangsverwalter, als (Mit-)Zugangsverwalter Lokaler (Mit-)Verwalter auftritt (auftreten).

Artikel 3 – Angebotene Dienstleistungen und verfügbare Kanäle

Die angebotenen Dienstleistungen sind über verschiedene Kanäle zugänglich.

1. Über die Portalsite der Sozialen Sicherheit (www.soziale-sicherheit.be)
    a) hat jeder Benutzer Zugriff auf den Onlinediensten „Dimona (Nicht gesichert)“, „Entsendungsanträge“ (Gotot), „Meldung von Arbeiten“, „Elektronisches Formular für den Zugangsantrag“,„Öffentliche Abfrage des Arbeitgeberrepertoriums“, „Identifikation des Arbeitgebers (WIDE)“ und „Einbehaltungspflicht“;
    b) hat jeder Konkursverwalter, der zum Zugangsverwalter (Lokaler Verwalter) bestimmt wurde, oder jeder Benutzer, der durch diesen Konkursverwalter bestimmt wurde und entweder über einen Benutzernamen und ein Kennwort oder über einen elektronischen Personalausweis verfügt, Zugriff auf die Anwendungen „eCUR“ und „Identifikation des Arbeitgebers (WIDE)“;
    c) hat jeder Benutzer, der von der für die Zugriffe verantwortlichen Entität eines Unternehmens als Zugangsverwalter (lokaler Verwalter) angegeben wurde und der entweder über einen Benutzernamen und ein Passwort oder über einen elektronischen Personalausweis verfügt, Zugriff auf die Anwendungen „Abrufen der e-Box“, „Dimona (Gesichert)“, „Personalbestand”, „LSS-Meldung (DMFA)”, „LSSPLV-Meldung

(DmfAPPO)", „Meldung Sozialrisiken (MSR)", „Abrufen von Arbeitsmeldungen", „Vorübergehende Arbeitslosigkeit un Validierungsbuch", „Gesichertes Abrufen des Arbeitgeberrepertoriums", „Beiträge für öffentliche Mandate", „Routing Module", „Routing Consult", „COVA", „Limosa – Meldepflicht", „Zugangsverwaltung für Unternehmen und Organisationen", „Informationen in Zusammenhang mit Einstellungsmaßnahmen – Arbeitgeber", „Informationen in Zusammenhang mit Einstellungsmaßnahmen – Beauftragter", „UMOE – Erste Verbindung", „Ecaro", „Trillium", „Einstellungsmeldung – Artikel 17", „Arbeitgeber Identifikation (WIDE)", „Abfragen MSR-Nachfolgesystem", „Capelo – Ergänzungen zur Laufbahnakte", „Capelo – Historische Daten", „Student@work - 50days", „Verwaltung von Versandregeln des befugten Arbeitnehmers (DESTHA)", „UDDI Registry Social Security", „Pay IT", „Rx", „Vertragsmeldung", „Alcedo – Checkinatwork", „Horeca@work", „Publiato", „Meldung von Arbeiten – FRONTEND", „Einbehaltungspflicht", „FollowIt" und „Beschäftigungsmaßnahmen";

d) hat jeder Benutzer, der durch den Hauptzugangsverwalter durch ein Unternehmen zum Zugangsverwalter (Lokaler Verwalter) bestimmt wurde und über einen elektronischen Personalausweis verfügt, Zugriff auf die Anwendung „Verwaltung und Verlauf der Vollmachten der sozialen Sicherheit (Mahis)", „DB2P", „PMP-Online", „Gotot-grenzüberschreitende Beschäftigung" und "4. Weg – Soziale Notifizierung";

e) hat jeder Benutzer, der durch den Zugangsverwalter (Lokaler Verwalter) eines Unternehmens bestimmt wurde und entweder über einen Benutzernamen und ein Kennwort oder über einen elektronischen Personalausweis verfügt, Zugriff auf die Anwendungen, zu denen er durch den Zugangsverwalter (Lokaler Verwalter) eines Unternehmens ermächtigt wurde, ohne dass diese Zugriffsmöglichkeiten die des Zugangsverwalters (Lokalen Verwalters) überschreiten;

f) hat jeder Benutzer, der durch ein Unternehmen zum Zugangsverwalter (Lokalen Verwalter) bestimmt wurde oder der durch den Zugangsverwalter 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 09. 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 Zugriff auf den Onlinediensten „Änderung einer LSS-Meldung (DmfA)" oder „Änderung einer LSSPLV-Meldung (DmfAPLV)".

2. Über die Portalsite der Föderalbehörde (www.belgium.be)

a) hat jeder Benutzer Zugriff auf die Anwendung „Abfragen von Informationen der Unternehmen";

b) hat jeder Benutzer, der durch ein Unternehmen zum Zugangsverwalter (Lokalen Verwalter) bestimmt wurde und über einen Benutzernamen sowie ein Kennwort verfügt, Zugriff auf die Anwendungen „Abfragen von Informationen meines Unternehmens", „Umfrage zum Verkehr zwischen dem Wohnort und dem Ort des Arbeitsplatzes", „Vigilis (e-Schalter)", „e-Notification" und „Die Eindeutige Startermeldung" (DEUS);

c) hat jeder Benutzer, der durch den Zugangsverwalter (Lokalen Verwalter) eines Unternehmens bestimmt wurde und über einen Benutzernamen, ein Kennwort und die

Verzeichnisnummer des Auftraggebers verfügt, Zugriff auf die 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 Zugangsverwalter (Lokalen Verwalter) eines Unternehmens bestimmt wurde und über einen Benutzernamen sowie ein Kennwort und in Bezug auf den Onlinediensten im Sinne von Punkt 3c) über die Verzeichnisnummer des Auftraggebers verfügt, Zugriff auf den Onlinediensten, zu denen er durch den Zugangsverwalter (Lokalen Verwalter) eines Unternehmens ermächtigt wurde, ohne dass diese Zugriffsmöglichkeiten die des Zugangsverwalters überschreiten;

e) hat jeder Benutzer, der durch ein Unternehmen zum Zugangsverwalter (Lokalen Verwalter) bestimmt wurde oder der durch den Zugangsverwalter (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 Zugriff auf die Anwendungen „Belcotax-on-web” und „PLZA – Paperless Zoll und Akzisen“.

3. Über die Portalsite von eSanté (www.ehealth.fgov.be)

a) hat jeder Benutzer Zugriff auf die Anwendung „Authentische Quelle Implantierbare Medizinische Hilfsmittel“ und „Healthdata.be Data Reporting“;

b) hat jeder ermächtigte Benutzer, der, abhängig von seiner Eigenschaft, entweder über einen Benutzernamen und ein Kennwort oder über einen Benutzernamen, ein Kennwort und ein Bürgertoken verfügt, Zugriff auf die Anwendungen „Interface for communication on experiments between sponsors, ethics committees and the competent authority (ICE-SEC)“, „Medega“, „CEBAM Digital library for Health“; „eTCT – Feedback an die Krankenhäuser über die von ihnen erbrachte Pflegeleistung und deren Kosten“ und „BINC (Begeleiding in Cijfers) – Online-Registrierungssystem für private Einrichtungen der besonderen Jugendbetreuung“;

c) hat jeder ermächtigte Benutzer, der, abhängig von seiner Eigenschaft, über einen Benutzernamen, ein Kennwort und ein Bürgertoken verfügt, Zugriff auf die Anwendungen „E-loket Zorg en Gezondheid“, „WebWachtMailer“ und „eHealth Web Application for File Exchange for Batch applications (WebFX)“;

d) hat jeder ermächtigte Benutzer, der entweder über einen Benutzernamen, ein Kennwort und ein Bürgertoken oder über einen elektronischen Personalausweis verfügt, Zugriff auf die Anwendungen „Elektronischer Datenaustausch für die Flämische Agentur Pflege & Gesundheit (VESTA)“, „Krebsregistrierung“, „Technische Gruppe über das Web (eTCT)“, „Elektronische Geburtsmeldung (eBirth)“, „BelRAI“, „Konsultieren der Versicherbarkeit einer Person“, „Übermitteln von Rechnungen für Drittzahler“, „eBox Update Info“, „Project on Cancer of the Rectum, die Online-Antrag zur Registrierung von Rektumkrebs (PROCARE DATA ENTRY)“ und „Medic-e intern – Elektronische Eingabe und Abfrage der Evaluation von Personen mit Behinderung“;

e) hat jeder ermächtigte Benutzer, der über einen elektronischen Personalausweis

verfügt, Zugriff auf die Anwendungen „Tool for Administrative Reimbursment Drugs Information Sharing“ (TARDIS), „Patientenverfügung für Euthanasie – eutha-consult“, „ORTHOpedic Prosthesis Identification Data – Electronic Registry – ORTHOpride®“, „Project on cancer of the rectum – Central Image Repository (PROCARE RX)“, „Qermid(c)Pacemakers – Quality Electronic Register Medical Implant Device“, „SMUREG“, „Medizinisch-administrative Ströme – Heimpflege (MEDADM-INF)“, „ZNA - Pflegeportal – SARAi“, „Registrierung therapeutischer Projekte (TherPro – PatientRegistration)“, „Medega“, „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“, „Registrierungsmodul der Belgischen Virtuellen Tumorbank“, „Katalog der Belgischen Virtuellen Tumorbank“, „CIVARS – Chapter IV Agreement Requesting System“, „Web Application Metahub“, „Abfrage der medizinischen Karte“, „TDI – Registrierungsmodul des „Treatment Demand Indicator““, „eShop – Online-Bestellung Pflegebescheinigungen (Medattest)“, „BNMDR – Belgian NeuroMuscular Disease Registry“, „eHealthConsent“, „Moduldatenbank Jugendhilfe Flandern“, „Authentische Quelle Arzneimittel“, „INSISTO“, „Konsultation des AMA-Anspruchs“, „DOMINO“, „Zentrales Rückverfolgungsregister“, „eTarif“, „eHealthOCC“, „Statistik Wohlbefinden Jugendliche“ und „GKB2.0 – Gemeinsamer Kundenbestand“.

4. Über Dateiübertragung gemäß (S)FTP, anhand von MQSeries oder anderen akzeptierten Kanälen kann jeder Benutzer, der durch ein Unternehmen zum Zugangsverwalter (Lokalen Verwalter) bestimmt wurde oder der durch einen Zugangsverwalter 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 von und der Zugriff auf diese Dienstleistungen können jederzeit geändert werden. Besondere Benutzungsbedingungen für die angebotenen Dienste können als Anlage zur Benutzerordnung angegeben werden.

Artikel 4 – Zugriff auf das Informationssystem

Der Benutzer hat Zugriff auf das Informationssystem, jedoch ohne Gewähr, dass der Zugriff auf das Informationssystem und die angebotenen Dienstleistungen jederzeit gesichert oder frei von Fehlern oder technischen Störungen ist.

Der Zugriff auf das Informationssystem und die 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, das zur Benutzung des Informationssystems erforderlich ist. Die Anbieter des Informationssystems sind nicht für den Terminal und dessen Benutzung verantwortlich und sind nicht verpflichtet, diesbezüglich irgendeine Unterstützung zu bieten.

Artikel 5 – Gebrauch von Benutzername und Kennwort

Ein Benutzer, der durch ein Unternehmen zum Hauptzugangsverwalter bestimmt wurde, kann in separaten Sendungen über Eranova, das Contact-Center der öffentlichen Einrichtungen der sozialen Sicherheit, einen Benutzernamen und ein Kennwort erhalten. Ein Benutzer, der nicht durch ein Unternehmen zum Hauptzugangsverantwortlichen bestimmt wurde, erhält seinen Benutzernamen und das Kennwort vom Zugangsverwalter (Lokalen Verwalter) seines 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 Zugangsverwalter (Lokalen Verwalter) empfangen hat, möglichst schnell nach dem Empfang und auf jeden Fall bei der erstmaligen Nutzung ändern. Jeder Benutzer muss sein Kennwort danach 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 verantwortlich in Fällen, 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 Benutzung durch Dritte seines Benutzernamens und/oder Kennworts hat oder einen derartigen Verlust bzw. eine derartige unerlaubte Benutzung vermutet, muss er unverzüglich alle erforderlichen Maßnahmen ergreifen.

Jeder Benutzer, der durch ein Unternehmen zum Zugangsverwalter (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 (unter der Rufnummer 02-511.51.51 oder über die Portalsite der sozialen Sicherheit (www.sociale-zekerheid.be)) zu melden. 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 Zugangsverwalter (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) Benutzung seines Benutzernamens und/oder Kennworts entsteht, die vor dem Zeitpunkt erfolgte, zu dem der Benutzername und das Kennwort deaktiviert wurden.

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

Artikel 6 – Benutzung des Informationssystems

In Bezug auf die Benutzung 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 laden;
    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 den die Privatsphäre Dritter verletzt wird;
    c) deren Benutzung 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 - Benutzung 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 im Sinne von 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.

Ein derartiges Zertifikat kann gemäß Art. 1322 Abs. 2 des Zivilgesetzbuchs für die Authentifizierung und die Anbringung einer elektronischen Signatur verwendet werden. Erfolgt der Zugriff auf die angebotenen Dienstleistungen allerdings mit einem elektronischen Personalausweis, wird die Authentifizierung durch das Identitätszertifikat des Ausweises durchgeführt und die elektronische Signatur mit dem Signaturzertifikat des Ausweises 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 Benutzung, einschließlich jeder Benutzung 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-zekerheid.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. Falls ein Benutzer 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 ist, kann er dies unter Benutzung seines Benutzernamens und Kennworts 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 – Benutzung 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 Informationssystemzugänglich 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 10bis. – Freie Lizenzen

Wenn das Informationssystem und die Dienste eine freie Software benutzen oder zur Verfügung stellen, gilt die Lizenz, die zu dieser Software gehört, für den Benutzer.

Außer den Regeln, die in die Lizenz der betreffenden freien Software aufgenommen sind, gelten folgende unabhängigen und ergänzenden Bestimmungen bezüglich der Haftung der Verwalter, der Administratoren, der Mitarbeiter und des Personals des Informationssystems (im Folgenden „das Informationssystem“ genannt) und die Garantie, die sie bieten, für den Benutzer.

Wenn das Informationssystem eine freie Software anpasst, wird es die nötigen Maßnahmen ergreifen, um dafür zu sorgen, dass diese korrekt durch den Benutzer angewendet werden kann ohne jedoch diesbezüglich irgendeine Ergebnisverpflichtung einzugehen.

Der Benutzer verpflichtet sich seinerseits dazu, die Software, die ihm zur Verfügung gestellt wird, so zweckdienlich und korrekt wie möglich zu benutzen und gegebenenfalls dem Informationssystem alle nützlichen Informationen, die zur Lösung von Problemen in Bezug auf den Gebrauch der Software beitragen können, zu verschaffen.

Da die betreffende Software frei genutzt werden kann, kann das Informationssystem unter keinen Umständen, es sei denn, dies ist schriftlich angegeben, für irgendwelche direkten oder indirekten, sekundäre oder nachfolgende, materielle oder immaterielle Schäden, die sich aus dem Gebrauch der Software oder aus der Unmöglichkeit dieses Gebrauchs ergeben, haftbar gemacht werden.

Artikel 11 - Übergangsmaßnahmen

Zurzeit 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 Zugriff auf bzw. keine Nutzung der Dienste, die auf der Portalsite der sozialen Sicherheit und der föderalen Portalsite angeboten werden, außer der Benutzung der Anwendung „elektronisches Formular für den Zugriffsantrag“.

Anlage - Benutzung der authentischen Quelle Arzneimittel durch Softwareentwickler

1. Einleitung

Die eHealth-Plattform stellt ihre Portalsite „Authentische Quelle Arzneimittel“ zur Verfügung.

Die Authentische Quelle Arzneimittel umfasst Angaben der Föderalagentur für Arzneimittel und Gesundheitsprodukte (FAGG-AFMPS) und des Landesinstituts für Kranken- und Invalidenversicherung (LIKIV).

2. Zuverfügungstellung für Softwareentwickler

Softwareentwickler, die anerkannte oder registrierte Softwarepakete für Dienstleister entwickeln, können die Authentische Quelle Arzneimittel als Ganzes von der Portalsite der eHealth-Plattform herunterladen.

Die Modalitäten für die Zurverfügungstellung eventueller Updates wird auf der Portalsite der eHealth-Plattform veröffentlicht.

3. Benutzung der Authentischen Quelle Arzneimittel

Softwareentwickler dürfen die Authentische Quelle Arzneimittel ausschließlich zu deren Integration in ihre anerkannten oder registrierten Softwarepakete für Dienstleister benutzen.

Mit Ausnahme der eventuellen Kosten für die technische Integration der Authentischen Quelle Arzneimittel in die Softwarepakete ist es Softwareentwicklern verboten, für die Zurverfügungstellung des Inhalts der Authentischen Quelle Arzneimittel an Benutzer der Softwarepakete eine Entschädigung zu erhalten.

Der Inhalt der Authentischen Quelle Arzneimittel darf von den Softwareentwicklern oder von Dritten auf keinerlei Weise für werbliche oder kommerzielle Zwecke genutzt werden.

Die geistigen Eigentums- oder Urheberrechte über die in die Authentische Quelle Arzneimittel aufgenommenen Daten sind ausschließliches Eigentum der Parteien, die die Daten für die Authentische Quelle Arzneimittel bereitgestellt haben, unter anderem FAGG- AFMPS und LIKIV.

Es ist den Softwareentwicklern verboten, die in die Authentische Quelle Arzneimittel aufgenommenen Daten zu verändern, indem der Inhalt ganz oder teilweise gelöscht oder verändert wird.

Es ist Softwareentwicklern erlaubt, die Authentische Quelle Arzneimittel um andere Daten zu erweitern, jedoch nur unter ihrer eigenen Verantwortung und mit ausdrücklichem Hinweis an die Benutzer.

4. Verantwortlichkeiten

FAGG-AFMPS, LIKIV, die eHealth-Plattform und jede andere bei der Zusammensetzung und Zuverfügungstellung der Authentischen Quelle Arzneimittel beteiligte Partei unternehmen alles, um eine sachgerechte Zusammensetzung und Zuverfügungstellung der Authentischen Quelle Arzneimittel zu gewährleisten, jedoch ohne diesbezüglich eine Ergebnisverpflichtung einzugehen.

FAGG-AFMPS, LIKIV, die eHealth-Plattform und jede andere bei der Zusammensetzung und Zuverfügungstellung der Authentischen Quelle Arzneimittel beteiligte Partei übernehmen keinerlei Haftung für den sachgerechten Gebrauch der in der Authentischen Quelle Arzneimittel verfügbaren Informationen. Sie können auf keinen Fall für irgendwelche, vom Benutzer oder von Dritten verursachte, direkte oder indirekte, sekundäre oder nachfolgende, materielle oder immaterielle Schäden, die sich aus dem Gebrauch der Authentischen Quelle Arzneimittel oder aus der Unmöglichkeit dieses Gebrauchs ergeben, haftbar gemacht werden.

5. Verstöße und Schadensersatz

Für jeden Verstoß gegen die Benutzungsbedingungen schuldet der Softwareentwickler FAGG-AFMPS, LIKIV und der eHealth-Plattform zusammen einen Schadensersatz in Höhe von € 50.000.

Falls die eHealth-Plattform, FAGG-AFMPS, LIKIV einen Verstoß des Softwareentwicklers gegen eine oder mehrere Benutzungsbedingungen feststellen, setzen sie den Softwareentwickler davon in Kenntnis. Der Softwareentwickler ist dann verpflichtet, die Benutzung der Authentischen Quelle Arzneimittel unverzüglich und unwiderruflich einzustellen, und dies unter Androhung einer zusätzlichen Schadensersatzzahlung an die oben angegebenen Parteien in Höhe von € 5.000 für jeden Tag, den der Softwareentwickler in Verzug bleibt.