27. März 2024

Benutzerordnung für den Zugriff auf das Informationssystem des föderalen Dienstes 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 des föderalen Dienstes und der öffentlichen Einrichtungen der sozialen Sicherheit (hiernach Informationssystem genannt) und zu den dadurch angebotenen Diensten und die Benutzung dieses Systems durch Unternehmen und ihre Bevollmächtigten.

Artikel 2 – Verpflichtung zur Angabe eines Hauptzugangsverwalters

Jedes Unternehmen, das Zugriff auf das Informationssystem haben und dieses benutzen möchte, muss einen einzigen Hauptzugangsverwalter ernennen.

Artikel 2bis − Begriffsbestimmungen

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 in dem Unternehmen von der dazu befugten Person eingestellt wird (werden), um die Benutzer− und Zugriffsverwaltung auf ihrer Benutzerebene zu gewährleisten, und zwar unabhängig davon, ob diese Person(en) als Hauptzugangsverwalter für die Zugriffe, als für die Zugriffe mitverantwortlicher Hauptzugangsverwalter, als für die Zugriffe (mit-)verantwortlicher Zugangsverwalter oder als (mitverantwortlicher) lokaler Verwalter auftritt (auftreten).

Artikel 3 – Angebotene Dienste und zur Verfügung stehende Kanäle

Die angebotenen Dienste sind über verschiedene Kanäle zugänglich.

1. Über das Internetportal der sozialen Sicherheit (www.socialsecurity.be):

   a) jeder Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 1 − Anwendungen über das Internetportal des föderalen Dienstes“ aufgeführten Anwendungen;
   b) jeder Kurator, der als Zugangsverwalter (lokaler Verwalter) oder jeder von diesem Kurator ernannte Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 1 − Anwendungen über das Internetportal der sozialen Sicherheit“ aufgeführten Anwendungen;
   c) jeder Benutzer, der von einem Unternehmen als Hauptzugangsverwalter (lokaler Verwalter) angegeben wurde, hat Zugriff auf die in der Tabelle in „ANLAGE 1 − Anwendungen über das Internetportal der sozialen Sicherheit“ aufgeführten Anwendungen;
   d) jeder Benutzer, der von dem Zugangsverwalter (lokalen Verwalter) eines Unternehmens angegeben wurde, hat Zugriff auf diejenigen Anwendungen, für die er von dem

Zugangsverwalter (lokalen Verwalter) eines Unternehmens bevollmächtigt wurde, wobei dieser Zugriff jedoch auf keinen Fall über den des Zugangsverwalter (lokalen Verwalters) selbst hinausreicht;

e) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein.

f) Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

2. Über das Internetportal des föderalen Dienstes (www.belgium.be):

a) jeder Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes“ aufgeführten Anwendungen;

b) jeder Benutzer, der von einem Unternehmen als Zugangsverwalter (lokaler Verwalter) angegeben wurde, hat Zugriff auf die in der Tabelle in „ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes“ aufgeführten Anwendungen;

c) jeder Benutzer, der von dem Zugangsverwalter (lokalen Verwalter) eines Unternehmens angegeben wurde und über eine Verzeichnisnummer des Mandanten verfügt, hat Zugriff auf die in der Tabelle in „ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes“ aufgeführten Anwendungen für diejenigen Personen, für die er über ein Mandat verfügt, um diese Anwendungen für ihr Benutzerkonto und in ihrem Namen zu benutzen und wovon er dieses Mandat der Regionaldirektion der direkten Steuern, die für das Steueramt des Arbeitgebers zuständig ist, zur Verfügung gestellt hat;

d) jeder Benutzer, der von dem Zugangsverwalter (lokalen Verwalter) eines Unternehmens angegeben wurde und, in Bezug auf die unter Punkt 3c) genannten Anwendungen, über die Verzeichnisnummer des Mandanten verfügt, hat Zugriff auf diejenigen Anwendungen, für die er von dem Zugangsverwalter (lokalen Verwalter) eines Unternehmens bevollmächtigt wurde, wobei dieser Zugriff jedoch auf keinen Fall über den des Zugangsverwalters selbst hinausreicht;

e) jeder Benutzer, der von einem Unternehmen als Zugangsverwalter (lokaler Verwalter) angegeben wurde oder der von dem Zugangsverwalter (lokalen Verwalter) eines Unternehmens angegeben wurde und der gleichzeitig 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 über einen anderen Zertifikatstyp, der in der Liste akzeptierter Zertifikate auf dem Internetportal der sozialen Sicherheit verfügt, hat außerdem noch Zugriff auf die in der Tabelle in „ANLAGE 2 – Anwendungen über das Internetportal des föderalen

Dienstes“ für ihn aufgeführten Anwendungen;

f) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein.
g) Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

3. Über das Internetportal von eHealth (www.ehealth.fgov.be)

a) hat jeder Benutzer Zugriff auf die in der Tabelle in „ANLAGE 3 − Anwendungen über das Internetportal eHealth“ aufgeführten Anwendungen;
b) hat jeder autorisierte Benutzer, abhängig von seiner Eigenschaft, Zugriff auf die in der Tabelle in „ANLAGE 3 − Anwendungen über das Internetportal eHealth“ aufgeführten Anwendungen;
c) hat jeder autorisierte Benutzer Zugriff auf die in der Tabelle in „ANLAGE 3 − Anwendungen über das Internetportal eHealth“ aufgeführten Anwendungen;
d) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein. Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

4. Über die Datenübertragung über (S)FTP oder andere zugelassene Kanäle kann jeder Benutzer, der von einem Unternehmen als Zugangsverwalter (lokaler Verwalter) angegeben wurde oder der von einem Zugangsverwalter angegeben wurde und der gleichzeitig über einen Benutzernamen, ein Kennwort, einen Privatschlüssel und ein qualifiziertes Zertifikat im Sinne von Artikel 2, 4° des Gesetzes vom 9. Juli 2001 über die Festlegung bestimmter Regeln im Zusammenhang mit dem juristischen Rahmen für elektronische Signaturen und Zertifikatsdienste oder über einen anderen Zertifikatstyp, der in der Liste akzeptierter Zertifikate auf dem Internetportal der sozialen Sicherheit wie u. a. das aktivierte Signaturzertifikats des elektronischen Personalausweises verfügt, „Dimona- Meldungen“, „DmfA − Multifunktionelle Meldung“ und „DmfA für provinziale und lokale Verwaltungen“, „Änderungen einer LSS-Meldung (DMFA)“, „Änderungen einer DmfAPPL-Meldung“ und „MRS − Meldung sozialer Risiken“ durchführen.

Der Inhalt der Dienste und der Zugriff auf diese Dienste können jederzeit geändert werden. Spezielle Benutzungsbedingungen für die gebotenen Dienste können als Anlage zu dieser Benutzerordnung hinzugefügt werden.

Artikel 4 − Zugriff auf das Informationssystem

Der Benutzer hat Zugriff auf das Informationssystem, ohne dass jedoch gewährleistet ist, dass der Zugriff auf dieses System und die angebotenen Dienste jederzeit gesichert oder frei von Fehlern oder technischen Störungen ist. Der Zugriff auf das Informationssystem und die angebotenen Dienste kann jederzeit ganz oder teilweise (u. a. zu Wartungszwecken) gesperrt werden. Dort, wo es auf angemessene Weise möglich ist, muss der Benutzer im Vorfeld über eine solche

Sperrung informiert werden.

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 das Terminal und dessen Benutzung verantwortlich und sind nicht verpflichtet, diesbezüglich irgendeine Unterstützung zu bieten.

Artikel 5 − Benutzung des Benutzernamens und des Kennwortes

Ein Benutzer, der von einem Unternehmen als Hauptzugangsverwalter angegeben wurde, bekommt den Benutzernamen und das Kennwort in separaten Mitteilungen über Eranova, das Kontaktzentrum der öffentlichen Einrichtungen für soziale Sicherheit, zugesendet. Ein Benutzer, der von einem Unternehmen nicht als Hauptzugangsverwalter angegeben wurde, bekommt seinen Benutzernamen und das Kennwort von dem Zugangsverwalter (lokalen Verwalter) seines Unternehmens.

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

Jeder Benutzer muss das Kennwort, das er vom Kontaktzentrum der öffentlichen Einrichtungen für soziale Sicherheit oder von einem Zugangsverwalter (lokalen Verwalter) erhalten hat, möglichst schnell nach deren Erhalt und auf alle Fälle bei deren erster Benutzung ändern. Jeder Benutzer muss sein Kennwort danach auf regelmäßige Weise ändern.

Ein sicheres Kennwort besteht aus 15 alphanumerischen Zeichen und Symbolen in einer Reihenfolge, die nur schwierig zu erraten ist. Jeder Benutzer hat dafür zu sorgen, dass das gewählte Kennwort diese Anforderungen erfüllt. Jeder Benutzer ist selbst dafür haftbar, wenn ein Kennwort, das nicht gemäß diesen Regeln zusammengesetzt wurde, erraten und/oder missbraucht wird.

Jeder Benutzer muss sorgfältig mit seinem Benutzernamen und Kennwort umgehen und ist zu deren Geheimhaltung verpflichtet. Der Benutzer ist haftbar für jede diesbezügliche erlaubte Benutzung, einschließlich jeder Benutzung durch Dritte.

Wenn ein Benutzer seinen Benutzernamen und/oder sein Kennwort verloren hat oder merkt oder vermutet, dass diese ohne seine Genehmigung von Dritten verwendet werden, hat er unverzüglich alle erforderlichen Maßnahmen zu treffen.

Jeder Benutzer, der von einem Unternehmen als Hauptzugangsverwalter angegeben wurde, ist u. a. dazu angehalten, diesen Verlust oder die nicht genehmigte Benutzung unverzüglich dem Kontaktzentrum der öffentlichen Einrichtungen für soziale Sicherheit, Eranova, (02/511.51.51 oder über das Internetportal der sozialen Sicherheit (www.socialsecurity.be)) zu melden. Baldmöglichst nach Erhalt dieser Meldung und in einem zeitlich angemessenen Rahmen werden alle möglichen Anstrengungen unternommen, um den Benutzernamen und das Kennwort des Benutzers zu ändern. Jeder Benutzer, der nicht von einem Unternehmen als Hauptzugangsverwalter angegeben wurde, ist u. a. dazu angehalten, diesen Verlust oder die nicht genehmigte Benutzung unverzüglich dem Haupt− oder Zugangsverwalter (lokalen Verwalter), von dem er seinen Benutzernamen und das Kennwort erhalten hat, mitzuteilen. Dieser muss baldmöglichst nach Erhalt dieser Meldung und in einem zeitlich angemessenen Rahmen alle möglichen Anstrengungen unternehmen, um den Benutzernamen zu deaktivieren und/oder das

Kennwort des Benutzers zu ändern.

Jeder Benutzer ist weiterhin für alle (direkten oder indirekten) Schäden haftbar, die durch die (insbesondere nicht genehmigte) Benutzung seines Benutzernamens und/oder seines Kennworts vor der Deaktivierung seines Benutzernamens und Kennworts entstanden sind.

Im Fall der Sperrung des Benutzernamens und/oder Kennworts muss der Benutzer, der von einem Unternehmen als Zugangsverwalter (lokaler Verwalter) angegeben wurde, einen neuen Benutzernamen und ein neues Kennwort bei Eranova, dem Kontaktzentrum der öffentlichen Einrichtungen der sozialen Sicherheit, beantragen; danach erhält er einen neuen Benutzernamen und ein neues Kennwort.

Artikel 5bis − Verwendung des digitalen Schlüssels
Der Zugriff des Benutzers auf bestimmte auf elektronischem Weg angebotene Dienste erfordert die Verwendung eines digitalen Schlüssels (wie das eID-Kartenlesegerät, ein auf TOTP (Time-based One-time password) basierender Sicherheitscode per mobier App oder SMS, ein Bürgertoken und Benutzername plus Passwort, (mobile) Schlüssel, die im Rahmen der durch den K. E. vom 22. Oktober 2017 zur Festlegung der Bedingungen, des Verfahrens und der Folgen der Anerkennung von Diensten zur elektronischen Identifizierung für Regierungsanwendungen anerkannt sind).

Diese digitalen Schlüssel und die damit verbundenen Daten sind strikt personengebunden und nicht übertragbar.

Jeder Endbenutzer ist für die korrekte Aufbewahrung, Sicherheit, Geheimhaltung und Verwaltung seiner digitalen Schlüssel und der damit verbundenen Daten verantwortlich.

Der Endbenutzer ist für die Wahl eines sicheren Kennworts oder sonstigen geheimen Codes verantwortlich.

Falls der Endbenutzer sich des Verlustes seines Benutzernamens, Kennworts, Bürgertokens oder sonstigen digitalen Schlüssels bewusst ist, oder einer unerlaubten Nutzung derselben durch Dritte, oder er einen solchen Verlust oder eine unerlaubte Nutzung vermutet, muss er unmittelbar sämtliche erforderlichen Maßnahmen ergreifen, um die digitalen Schlüssel zu deaktivieren.

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

Die digitalen Schlüssel werden im Rahmen von CSAM angewendet (siehe https://www.csam.be). Deren Erstellung und Benutzung unterliegen daher den Vorschriften der Benutzervereinbarung von CSAM. Einige digitale Schlüssel stehen nicht für jede Anwendung zur Verfügung.

Artikel 6 − Benutzung des Informationssystems
In Bezug auf die Benutzung des Informationssystems und der über dieses System angebotenen Dienste ist jeder Benutzer dazu verpflichtet:

1. vollständige, zutreffende, wahrheitsgemäße und nicht-irreführende Informationen zu erteilen;
2. die kraft Gesetz, Verordnung, Dekret, Anweisung oder Erlass der föderalen, regionalen,

lokalen oder internationalen Behörde vorgeschriebenen Bestimmungen zu respektieren;

3. die erteilten Informationen nicht zu manipulieren, auf welche Weise oder mit welcher Technik auch immer;
4. über das Informationssystem keine Daten, Meldungen oder Dokumente auf irgendwelche Weise zu versenden, bzw. Daten oder Dokumente über das Informationssystem hochzuladen,
    a) bei denen die Rechte (darunter Persönlichkeitsrechte oder geistige Eigentumsrechte) von Dritten oder der Anbieter des Informationssystems verletzt werden;
    b) deren Inhalt illegal, schädigend, verleumderisch, gewalttätig, obszön oder entwürdigend 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 Dienste beeinträchtigen oder stören könnten.

Artikel 7 − Benutzung des Zertifikats

Für den Zugriff des Benutzers auf bestimmte Dienste sind entweder die Benutzung eines elektronischen Personalausweises oder zusätzlich zur Benutzung eines Benutzernamens und eines Kennworts auch die Benutzung eines Privatschlüssels und eines qualifizierten Zertifikats 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 über einen anderen Zertifikatstyp, der in der Liste akzeptierter Zertifikate auf dem Internetportal der sozialen Sicherheit genannt wird, erforderlich.

Dasselbe Zertifikat kann zur Authentifizierung sowie für eine elektronische Signatur im Sinne von Artikel 1322, Absatz 2 des Zivilgesetzbuches verwendet werden. Wenn der Zugriff auf die angebotenen Dienste jedoch über einen elektronischen Personalausweis erfolgt, wird die Authentifizierung durch das Identitätszertifikat der Karte vorgenommen und die elektronische Signatur über das Signaturzertifikat der Karte angebracht.

Sobald die Daten zum Aufstellen einer Signatur zusammengestellt worden sind, ist der Zertifikatsinhaber alleinig für den Schutz dieser Daten verantwortlich. Wenn Zweifel über den Erhalt der Vertraulichkeit der Daten zum Erstellen einer Signatur bestehen 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 Aufstellen einer Signatur nicht mehr benutzen, um diese Daten zu unterzeichnen oder durch einen anderen Zertifizierungsdiensteanbieter 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 unerlaubte Benutzung, einschließlich jeder Benutzung durch Dritte. Der Benutzer muss den Privatschlüssel und das Zertifikat auf einem

sicheren Datenträger aufbewahren, vorzugsweise auf einer Prozessorchipkarte, mit der der Privatschlüssel nicht exportiert werden kann.

Das Informationssystem kann Zertifikate und Zertifikatstypen, die von den Zertifizierungsbehörden in der Liste auf dem Internetportal der sozialen Sicherheit (www.socialsecurity.be) ausgestellt wurden, validieren. Zertifikate, die von anderen Zertifizierungsbehörden ausgestellt wurden, können nur beantragt werden, nachdem die erforderlichen technischen Anpassungen zur Validierung dieser Zertifikate im Informationssystem umgesetzt worden sind. Der Benutzer, der festen Willens ist, ein qualifiziertes Zertifikat im Sinne von Artikel 2, 4° des Gesetzes vom 9. Juli 2001 über die Festlegung bestimmter Regeln im Zusammenhang mit dem juristischen Rahmen für elektronische Signaturen und Zertifikatsdienste zu verwenden, das jedoch von einer anderen Zertifizierungsbehörde als derjenigen, die auf dem Internetportal der sozialen Sicherheit angegeben ist, ausgestellt wurde, kann dieses unter Benutzung seines Benutzernamens und Kennworts über das dazu vorgesehene Formular auf dem Internetportal der sozialen Sicherheit mitteilen. Innerhalb eines angemessenen Rahmens und unter bestmöglicher Mitarbeit der betroffenen Zertifizierungsbehörde werden die erforderlichen Bemühungen unternommen, damit das Informationssystem auch Zertifikate der genannten Zertifizierungsbehörde validieren kann. Sobald dies der Fall ist, können auch Zertifikate der genannten Zertifizierungsbehörde verwendet werden.

Artikel 8 − Benutzung der elektronischen Signatur und Nachweis (Benutzer mit einem Zertifikat)

Die über das Informationssystem von dem Benutzer, der entweder über ein qualifiziertes Zertifikat im Sinne von Artikel 2, 4° des Gesetzes vom 9. Juli 2001 über die Festlegung bestimmter Regeln im Zusammenhang mit dem juristischen Rahmen für elektronische Signaturen und Zertifikatsdienste oder einen anderen Zertifikatstyp, der in der Liste akzeptierter Zertifikate auf dem Internetportal der sozialen Sicherheit genannt wird, oder über einen elektronischen Personalausweis verfügt, gesendeten Berichte werden mit einer elektronischen Signatur versehen, wie in Artikel 1322, Absatz 2 des Zivilgesetzbuches genannt.

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

Der Benutzer erkennt ausdrücklich an, dass alle Informationen über Meldungen, die durch die Anbieter des Informationssystems auf dauerhafte und nicht zu ändernde Weise gespeichert werden, eine rechtliche Beweiskraft wie eine Privaturkunde 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 ausgestellten Zertifikats unter Einhaltung des dazu vorgesehenen Verfahrens geleistet wurde, außer im Falle eines Missbrauchs, Verlustes oder Diebstahls.

Artikel 9 − Kontrollpflicht des Benutzers

Der Benutzer ist verantwortlich für die Kontrolle des Inhalts der durch ihn über das Informationssystem versandten Nachrichten und für die betreffende Betreuung anlässlich von Nachrichten, die durch die Anbieter des Informationssystems an den Benutzer versandt werden und die sich auf den/die durch den Benutzer versandte(n) Nachricht(en) beziehen.

Der/die materielle(n) Fehler in einer vom Benutzer versandten Nachricht, in einer Empfangsmeldung, die sich darauf bezieht oder in jeder anderen Meldung oder jedem anderen Dokument, die bzw. das sich auf den Benutzer bezieht und die 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 etc.), von denen die Anbieter des Informationssystems (oder seine Lizenzerteiler) der/die Inhaber sind.

Der Benutzer erhält ein nichtexklusives 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 zu erzeugen.

Artikel 10bis – Freie Lizenzen

Wenn für das Informationssystem und die Dienste eine freie Software verwendet oder zur Verfügung gestellt wird, gilt die zu dieser Software gehörende Lizenz für den Benutzer.

Neben den Regeln, die in der Lizenz der besagten freien Software enthalten sind, gelten die folgenden unabhängigen und ergänzenden Bestimmungen bezüglich der Haftbarkeit der Verwalter, der Administratoren, der Mitarbeiter und des Personals des Informationssystems (nachfolgend „das Informationssystem“ genannt) und die von ihnen gebotene Garantie auch für den Benutzer.

Wenn das Informationssystem eine freie Software anpasst, wird dabei versucht, möglichst dafür zu sorgen, dass diese Software von dem Benutzer angewendet werden kann, ohne sich jedoch dabei im Hinblick auf Ergebnisse zu verpflichten.

Der Benutzer seinerseits verpflichtet sich dazu, die ihm zur Verfügung gestellte Software möglichst adäquat und korrekt zu benutzen und ggf. alle nützlichen Informationen, die zu der Lösung von Problemen in Zusammenhang mit der Softwarebenutzung beitragen können, dem Informationssystem zur Verfügung zu stellen.

Da die besagte Software frei benutzt werden kann, wird das Informationssystem auf keinen Fall, außer auf schriftliche Mitteilung hin, für direkte oder indirekte, sekundäre oder nebensächliche, materielle oder immaterielle, vom Benutzer oder von Dritten verursachten

und sich aus der Benutzung der Software oder gerade aus der Unmöglichkeit der Benutzung der Software ergebenden Schäden haftbar gemacht werden.

Artikel 11 − Übergangsmaßnahmen

Zurzeit kann das Signaturzertifikat des elektronischen Personalausweises lediglich über das System der Datenübertragung mit (S)FTP, anhand von MQSeries oder anderen zugelassenen Kanälen benutzt werden; es ermöglicht jedoch nicht den Zugriff auf die Dienste, die auf dem Internetportal der sozialen Sicherheit und auf dem Internetportal des föderalen Dienstes angeboten werden, außer in Bezug auf die Anwendung „Elektronisches Antragsformular für die Zugriffsberechtigung“.

ANLAGE 1 − Anwendungen über das Internetportal der sozialen Sicherheit

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App oder SMS) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Anwendungen, die für jeden autorisierten Benutzer zugänglich sind, gemäß Artikel 3.1.a			
Dimona (ungesichert)	Für diese Anwendungen ist kein digitaler Schlüssel erforderlich		
Arbeitsmeldung			
Elektronisches Antragsformular für die Zugriffsberechtigung			
Öffentliche Abfrage des Arbeitgeberrepertoriums			
Werkgever IDentificatie/ion Employeur, Identifikation des Arbeitgebers (WIDE) – ungesichert			
Einbehaltungspflicht			
Gütlich vereinbarte Tilgungspläne			
Anwendungen, die für Kuratoren zugänglich sind, gemäß Artikel 3.1.b			
eCUR	Ja	Ja	Ja
Werkgever IDentificatie/ion Employeur, Identifikation des Arbeitgebers (WIDE)			
Anwendungen, die für Zugangsverwalter (lokale Verwalter) und für von den Zugangsverwaltern angegebene Benutzer zugänglich sind, gemäß Artikel 3.1.c und 3.1.d			
Abfrage der e-Box	Ja	Ja	Ja
Dimona (gesichert)			
DmfA − Multifunktionelle Meldung			
DmfA für provinziale und lokale Verwaltungen			
MSR − Meldung soziale Risiken (eintragen und ändern)			
Gesicherte Abfrage des Arbeitgeberrepertoriums			
Abrufen Urlaubsbestand			
Limosa − Meldepflicht			
Zugangsverwaltung für Unternehmen und Organisationen			

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Anwendungen, die für Zugangsverwalter (lokale Verwalter) und für von den Zugangsverwaltern angegebene Benutzer zugänglich sind, gemäß Artikel 3.1.c und 3.1.d			
Ecaro	Ja	Ja	Ja
Trillium			
Werkgever IDentificatie/ion Employeur, Identifikation des Arbeitgebers (WIDE)			
Capelo − Ergänzungen zur Laufbahnakte			
Capelo – Historische Daten			
Student@Work			
DestHa − Verwaltung von Versandregeln des befugten Arbeitnehmers			
Abfrage Rechnungen Arbeitgeber			
Checkinatwork			
Horeca@work			
Publiato			
Arbeitsmeldung − FRONTEND			
Einbehaltungspflicht			
FollowIt			
Verwaltung und Verlauf der Vollmachten der sozialen Sicherheit (Mahis)			
DB2P	Nein	Nein	Ja
Öffentliche Mandatsträger			
Arbeiten im Ausland			
Ändern einer LSS-Meldung (DmfA)			
Ändern einer DmfAPPL-Meldung			
Registrieren (gesichert)			
Im Ausland arbeiten – Selbstständige(r)			
Green@work			
Rina			
BelgianIDpro			
Befreiung Sozialbeiträge Selbständige			
ContactData			
CareerPro Documents			
Vorübergehende Arbeitslosigkeit und Validierungsbuch			
Dossier Laufbahnunterbrechung und Zeitkredit			
Vereinsarbeit	Nein	Nein	Ja
Working in the Arts - Amateurkunstvergütung	Nein	Nein	Ja
Check In and Out at Work	Nein	Nein	Ja
Chaman: Verwaltung technischer Kanäle	Nein	Nein	Ja

ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Abruf von Informationen über Unternehmen	Für diese Anwendungen ist kein digitaler Schlüssel erforderlich		
Anwendungen, die für Zugangsverwalter (lokale Verwalter) und für von den Zugangsverwaltern angegebene Benutzer zugänglich sind, gemäß Artikel 3.2.b und 3.2.d			
Abruf von Informationen über mein Unternehmen	Ja	Ja	Ja
Umfrage zur Strecke Wohnung-Arbeitsplatz			
Vigilis (e-Schalter)			
e-Notification			
Die Eindeutige Startermeldung (DEUS)			
Anwendungen, die für Zugangsverwalter (lokale Verwalter) und für von den Zugangsverwaltern angegebene Benutzer zugänglich sind, gemäß Artikel 3.2.c und 3.2.d			
Tax-on-Web (TOW)	Ja	Ja	Ja
Abfrage der Tax-on-Web-Meldung			
Anwendungen, die für Zugangsverwalter (lokale Verwalter) und die von den Zugangsverwaltern angegebenen Benutzer zugänglich sind, gemäß Artikel 3.2.e			
Belcotax-on-Web	Nein	Nein	Ja
PLZA − Paperless Zoll und Akzisen			

ANLAGE 3 − Anwendungen über das Internetportal eHealth

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Anwendungen, die für jeden autorisierten Benutzer zugänglich sind, gemäß Artikel 3.3.a			
Authentische Quelle Implantierbare Medizinische Hilfsmittel	Für diese Anwendungen ist kein digitaler Schlüssel erforderlich		
Pharma formulary			
Healthdata.be Data Reporting			
„Centraal reservatiesysteem COV19“ (mit Reservierungscode)			
Anwendungen, die für jeden autorisierten Benutzer, abhängig von seiner Eigenschaft, zugänglich sind, s. Artikel 3.3.b			
BHOD – Bereitschaftshonorare	Ja	Ja	Ja
CEBAM Digital Library for Health / DCLH / EBMPRACTICENET			
E-Schalter „Zorg & Gezondheid“	Nein	Nein	Ja
WebWachtMailer			
eHealth Web Application for File Exchange for Batch applications (WebFX)			
eTCT – Feedback an die Krankenhäuser über die von ihnen erbrachte Pflegeleistung und deren Kosten			
UPPAD			
BINC (Begeleiding in Cijfers) – Online-Registrierungssystem für private Einrichtungen der besonderen Jugendbetreuung			
Plattform „Welzijn & Gezondheid“			
Interface for communication on experiments between sponsors, ethics committees and the competent authority (ICE-SEC)			
Anwendungen, die für jeden autorisierten Benutzer zugänglich sind, gemäß Artikel 3.3.c			
Elektronischer Datenaustausch für die Flämische Pflege- & Gesundheitsagentur (VESTA)	Nein	Nein	Ja
Krebsregistrierung			
Technische Zelle über das Web (eTCT)			
Elektronische Geburtsmeldung (eBirth)			
Abfrage der Versicherbarkeit einer Person			
Übermittlung von Rechnungen Drittzahler			
eBox Update Info			
Project on Cancer of the Rectum, die Online-Antrag zur Registrierung von Rektumkrebs (PROCARE DATA ENTRY)			
Medic-e intern – Elektronische Eingabe und Abfrage der Evaluation von Personen mit Behinderung			

Tool for Administrative Reimbursement Drugs Information Sharing (TARDIS)	Nein	Nein	Ja
ODEA			

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Anwendungen, die für jeden autorisierten Benutzer zugänglich sind, gemäß Artikel 3.3.c			
Abfrage der Patientenverfügung für Euthanasie – eutha-consult	Nein	Nein	Ja
ORTHOpedic Prosthesis Identification Data – Electronic Registry − ORTHOpride®			
Project on cancer of the rectum − Central Image Repository (PROCARE RX)			
Qermid©Pacemakers-Quality Electronic Registration of Medical Implant Devices			
SMUREG			
Medizinisch-administrative Ströme – Heimpflege (MEDADM-INF)			
ZNA − Pflegeportal – SARAi			
Registrierung therapeutischer Projekte (TherPro –PatientRegistration)			
BHOD – Bereitschaftshonorare			
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 Belgian Virtual Tumourbank			
Katalog der Belgian Virtual Tumourbank			
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 − IT-System Branchenübergreifendes Gateway			
Abfrage des GMA-Anspruchs			
DOMINO			

	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Anwendungen, die für jeden autorisierten Benutzer zugänglich sind, gemäß Artikel 3.3.c			
Zentrales Rückverfolgungsregister	Nein	Nein	Ja
eTarif			
eHealthOCC			
Statistik Wohlbefinden Jugendliche			
GKB2.0 – Gemeinsamer Kundenbestand			
PARIS (Prescription & Autorisation Requesting Information System)			
BelRAI			
eHealth API Portal			
eHealthCreaBis			
BelRAI Vlaanderen			
Corona-Impfung – App zur Meldung von Patienten mit seltenen/komplexen Erkrankungen			
Corona Test Prescription & Consultation			
MyINAMI			
Heracles			
MediPrima			

Anlage 4 − Benutzung der authentischen Quelle für Arzneimittel von Softwareentwicklern

1. Einleitung

Die eHealth-Plattform stellt über ihr Internetportal die authentische Quelle für Arzneimittel zur Verfügung.

Die authentische Quelle für Arzneimittel enthält Daten, die von der Föderalagentur für Arzneimittel und Gesundheitsprodukte (FAAGP) sowie dem Landesinstitut für Kranken- und Invalidenversicherung (LIKIV) stammen.

2. Verfügbarmachung für Softwareentwickler

Softwareentwickler, die anerkannte oder registrierte Softwarepakete für Pflegeerbringer entwickeln, können die authentische Quelle für Arzneimittel in ihrer Gesamtheit über das Internetportal der eHealth-Plattform herunterladen.

Die Modalitäten für die Verfügbarmachung eventueller Updates werden auf dem Internetportal der eHealth-Plattform veröffentlicht.

3. Benutzung der authentischen Quelle für Arzneimittel

Die Softwareentwickler dürfen die authentische Quelle für Arzneimittel ausschließlich für deren Integration in ihre anerkannten oder registrierten Softwarepakete für Pflegeerbringer verwenden.

Mit Ausnahme der eventuellen Kosten für die technische Integration der authentischen Quelle für Arzneimittel in die Softwarepakete ist es den Softwareentwicklern verboten, sich die Verfügbarmachung des Inhalts der authentischen Quelle für Arzneimittel für die Benutzer der Softwarepakete vergüten zu lassen.

Der Inhalt der authentischen Quelle für Arzneimittel darf von den Softwareentwicklern oder von Dritten auf keinerlei Weise zum Zweck der Veröffentlichung oder für kommerzielle Zwecke verwendet werden.

Die Rechte auf geistiges Eigentum oder die Urheberrechte für die Daten, die in der authentischen Quelle für Arzneimittel enthalten sind, gehören exklusiv den Parteien, die die Daten an die authentische Quelle für Arzneimittel gegeben haben, wie u. a. die FAAGP und das Landesinstitut für Kranken− und Invalidenversicherung (LIKIV).

Es ist den Softwareentwicklern verboten, die Daten, die in der authentischen Quelle für Arzneimittel aufgenommen wurden, durch eine gesamte oder teilweise Änderung des Inhalts zu löschen oder zu ändern.

Die Softwareentwickler dürfen die authentische Quelle für Arzneimittel mit anderen Daten anreichern, doch ausschließlich im Rahmen ihrer eigenen Verantwortlichkeit und mit der ausdrücklichen Mitteilung darüber an die Benutzer.

4. Verantwortlichkeiten

Die FAAGP, das Landesinstitut für Kranken− und Invalidenversicherung (LIKIV), die eHealth-Plattform und alle anderen Parteien, die bei der Zusammenstellung und der Verfügbarmachung der authentischen Quelle für Arzneimittel betroffen sind, setzen alles daran, um die Arbeit für eine korrekte Zusammenstellung und Verfügbarmachung der authentischen Quelle für Arzneimittel,

jedoch ohne eine Verpflichtung in Bezug auf die Ergebnisse in diesem Bereich, anzugehen.

Die FAAGP, das Landesinstitut für Kranken− und Invalidenversicherung (LIKIV), die eHealth-Plattform und alle anderen Parteien, die bei der Zusammenstellung und Verfügbarmachung der authentischen Quelle für Arzneimittel betroffen sind, sind von der Haftung für die konkrete Benutzung der in der authentischen Quelle für Arzneimittel verfügbaren Informationen vollständig freigestellt. Sie können auf keinen Fall für jegliche Form von direkten oder indirekten, sekundären oder nebensächlichen, materiellen oder immateriellen, vom Benutzer oder von Dritten verursachten und und sich aus der Benutzung der Software oder gerade aus der Unmöglichkeit der Benutzung der Software ergebenen Schäden haftbar gemacht werden.

5. Nichteinhalten der Benutzungsbedingungen und Schadensersatz

Für jedes Nichteinhalten der Benutzungsbedingungen hat der betroffene Softwareentwickler der FAAGP, dem Landesinstitut für Kranken− und Invalidenversicherung (LIKIV) und der eHealth-Plattform unter gemeinsamem Titel einen Schadensersatz in Höhe von € 50.000,− zu zahlen.

Falls die eHealth-Plattform, die FAAGP oder das Landesinstitut für Kranken− und Invalidenversicherung (LIKIV) feststellt, dass ein Softwareentwickler eine oder mehrere der vorliegenden Benutzungsbedingungen nicht einhält, werden sie den betroffenen Softwareentwickler darüber informieren. Der Softwareentwickler ist anschließend dazu angehalten, die Benutzung der authentischen Quelle für Arzneimittel unverzüglich und unwiderruflich einzustellen, und zwar mit einer Strafe einer zusätzlichen Schadensersatzzahlung in Höhe von 5.000 € an die zuvor genannten Parteien für jeden Tag, an dem sich zeigt, dass der Softwareentwickler seinen Verpflichtungen nicht nachkommt.