eLogin&NOVA

Teilnahme- und Nutzungsbedingungen

(Stand 23.05.2022)

Deutsche Rentenversicherung Bund

Inhaltsverzeichnis

1 Einleitung

Im Folgenden werden die Begriffe „Administrator“ und „Benutzer“ im generischen Maskulin verwendet.

Die Datenstelle der Rentenversicherung (DSRV) ist eine von der Deutschen Rentenversicherung Bund administrativ verwaltete, aber von allen Trägern der Rentenversicherung unterhaltene Einrichtung. Diese gemeinsame Unterhaltung ist gesetzlich in § 145 Abs. 1 SGB VI verankert. Der Datenstelle sind durch Gesetze eigene Aufgaben zugewiesen (z.B. das Führen der Stammsatzdatei - § 150 SGB VI). In beinahe allen automatisierten Datenaustauschverfahren zwischen dritten Stellen und den Trägern der Rentenversicherung ist die DSRV als Datenannahme- und Datenverteilstelle beteiligt.

Die DSRV verfügt für verschiedene gesetzlich zugewiesene Aufgaben über eigene Datei-Systeme (Datenbaken oder IT-Verfahren). Die verarbeiteten Daten sind in beinahe allen Fällen Sozialdaten. Sozialdaten sind als Sozialgeheimnis zu schützen und unterliegen neben den Bestimmungen der Datenschutzgrundverordnung dem besonders geregelten Sozialdatenschutz (§ 35 SGB I, §§ 67ff SGB X). Die Deutsche Rentenversicherung muss durch technische oder organisatorische Maßnahmen die Vertraulichkeit, die Integrität und die Verfügbarkeit der verarbeiteten Sozialdaten gewährleisten und die technischen Systeme deshalb besonders absichern. Dazu muss sie Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet werden, verwehren (Zugangskontrolle), und muss gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle).

Das geschieht bei den Informations- und Kommunikationsdiensten der Deutschen Rentenversicherung mit der zentralen Benutzerverwaltung NOVA (NOVA: **N**utzer – **O**rganisation – **V**erfahren – **A**dministration oder auch NoVa: **N**utzer**o**rientierte **V**erwaltungs**a**nwendung) und der Anmelde- und Authentifizierungskomponente eLogin, mit der bei jeder Nutzung über Kennung und Passwort-Abfrage oder über Signaturkartenanmeldung eine Benutzerauthentifizierung durchgeführt wird.

In eLogin&NOVA werden personenbezogene Daten der Benutzer verarbeitet. Dies geschieht zur Umsetzung der Zugangs- und Zugriffskontrolle und damit zu Zwecken der Datenschutzkontrolle und für die Sicherstellung eines ordnungsgemäßen Betriebes der IT-Anwendungen der DSRV (Zweckbestimmung und strenge Zweckbindung § 67c Abs. 4 SGB X).

Die nutzende Stelle übermittelt die Benutzerdaten durch Eingabe in die NOVA. Die DSRV verarbeitet die Benutzerdaten in Erfüllung der Teilnahme- und Nutzungsbedingungen.

Die Einhaltung dieser Teilnahme- und Nutzungsbedingungen ist Voraussetzung für die Zulassung zu eLogin&NOVA und der angebundenen Verfahren der Deutschen Rentenversicherung und liegt im Verantwortungsbereich der nutzenden Stelle.

Diese Teilnahme- und Nutzungsbedingungen dienen der Realisierung und der Aufrechterhaltung eines hohen Schutzbedarfs im Hinblick auf Authentizität, Integrität und Vertraulichkeit der Daten.

2 Geltungsbereich

Der Geltungsbereich dieser Teilnahme- und Nutzungsbedingungen erstreckt sich auf sämtliche Daten, Systeme und Netzwerkkomponenten, die im Zusammenhang mit eLogin&NOVA stehen.

Diese Teilnahme- und Nutzungsbedingungen sind bindend für die nutzenden Stellen und alle Benutzer, die in die NOVA eingetragen sind und Dienste und Verfahren der DSRV bedienen, benutzen oder anderweitig damit zu tun haben.

Die DSRV ist jederzeit berechtigt, den Inhalt dieser Teilnahme- und Nutzungsbedingungen ohne vorherige Ankündigung zu ändern.

3 Bedingungen zur Teilnahme

1. Die nutzende Stelle bestätigt, diese Teilnahme- und Nutzungsbedingungen für eLogin&NOVA erhalten zu haben und verpflichtet sich zur Einhaltung dieser (in der jeweils gültigen Fassung).
2. Die nutzende Stelle bestätigt
    a. die Umsetzung der in diesen Teilnahme- und Nutzungsbedingungen beschriebenen Maßnahmen und
    b. die Verpflichtung der eigenen Mitarbeiter zur Einhaltung der in den Handlungsanweisungen bei Sicherheitsvorfällen (Anhang A) beschriebenen Maßnahmen.

Hinweis: Einzelne IT-Anwendungen und Dienste der DSRV haben eigene Teilnahme- und Nutzungsbedingungen. Wenn diese IT-Anwendungen und Dienste eLogin&NOVA für die Authentifizierung sowie Zugangs- und Zugriffssteuerung verwenden, wird auf die hier vorliegenden Teilnahme- und Nutzungsbedingungen verwiesen.

4 Datenerhebung

Im Rahmen der Nutzung von eLogin&NOVA verarbeitet die DSRV die folgenden Daten der Organisationen und der Benutzer:

1. Pflichtfelder bei Organisationen:
    a. Name der Organisation
    b. Organisationseinheit
    c. Betriebsnummer (BBNR) oder Gemeindeschlüssel (AGS)
    d. Adresse: Postleitzahl, Ort, Land
2. optionale Felder bei Organisationen:
    a. Namenszusatz
    b. Kontoführende Anstalt (KTAN)
    c. Kennungskürzel (für Benutzer der Organisation)
    d. E-Mail-Adresse
    e. Adresse: Straße, Hausnummer, Postfach
3. Pflichtfelder bei Benutzern (müssen vom jeweiligen Administrator gepflegt werden):
    a. Benutzername/ID (wird teilweise automatisch vergeben; kann im Nachhinein nicht mehr verändert werden)

b. persönliche Angaben: Anrede, Nachname, Vorname, Geburtsdatum (zur Authentifizierung bei telefonischen Kontakten eines Benutzers mit der Hotline oder der Benutzerverwaltung)
c. dienstliche Kontaktinformationen: E-Mail-Adresse, Telefonnummer
d. dienstliche Adresse: Postleitzahl, Ort, Land (hier kann die Adresse der Organisation angegeben werden)
e. Zugang über Benutzername/Kennwort: Es werden Startkennwörter sowie das jeweils aktuelle Kennwort (zum Abgleich bei Anmeldeversuchen) und die letzten drei Kennwörter (Sicherheitsmechanismus Kennworthistorie) gespeichert.
f. Zugang über Signaturkarte: es wird der DN (distinguished name) der Signaturkarte verarbeitet
g. Es wird beim Benutzer hinterlegt, welche Kombinationen aus Verfahren/Rollen/Struktureinheiten, Zugangsart (Benutzername/Kennwort, Signaturkarte, RACF) und target (Intranet, Internet, Extranet) ihm zugeordnet bzw. für ihn freigegeben sind.

4. optionale Felder bei Benutzern (Pflege erfolgt durch den Benutzer selbst, freiwillige Angaben):
   a. persönliche Angaben: Titel, Namenszusatz
   b. Kontaktinformationen: zusätzliche E-Mail-Adresse, Faxnummer
   c. Organisationsdaten: Arztnummer, Versichertenältester/Versichertenberater (GMSC), Personalnummer, E-Mail-Adresse
   d. Adresse: Straße, Hausnummer, Postfach (hier kann die Adresse der Organisation angegeben werden)

Die NOVA-Administratoren der nutzenden Stellen pflegen die Daten der Benutzer ihrer Institution selbst.

Die Daten der nutzenden Stelle und der Benutzer werden solange verarbeitet, wie die IT-Anwendungen oder Dienste der DSRV genutzt werden. Scheidet ein Benutzer aus, wird die Kennung stillgelegt. Beendet eine nutzende Stelle die Nutzung von IT-Anwendungen oder Diensten der DSRV werden alle Daten der Institution und sämtlicher Benutzer stillgelegt. Nach der Stilllegung von Benutzerstammsätzen oder ganzen Organisationen bleiben Daten danach noch 30 Jahre aus Revisionsgründen gespeichert und können bei Prüfungen oder zu Revisionszwecken von besonders zugelassenen Berechtigten eingesehen werden. Die Löschung erfolgt nach Ablauf der 30-jährigen Revisionsfrist.

5 Bereitstellung von eLogin&NOVA

1. Die DSRV gewährleistet im Rahmen der üblichen Sorgfaltspflichten die ordnungsgemäße Bereitstellung von eLogin&NOVA.
2. Mit Administration und Betrieb von eLogin&NOVA ist die DSRV betraut. Zu ihren Aufgaben gehören insbesondere die Unterstützung und Beratung der nutzenden Stelle bei der Realisierung der für einen Anschluss erforderlichen technischen Voraussetzungen, die Erteilung der Freigabe zur Nutzung einzelner Verfahren, die Verwaltung der Benutzerkennungen und die Unterstützung der nutzenden Stelle bei der Feststellung und Beseitigung von Störungen.
3. Ansprechpartner für die nutzenden Stellen ist bei Fragen oder Problemen die hier genannte Hotline für eLogin&NOVA:

Telefon-Nr.:	0931 6002 73500
Fax-Nr.:	0931 6002 3900
E-Mail-Adresse:	drvlogin@deutsche-rentenversicherung.de

4. Die Deutsche Rentenversicherung behält sich vor, bei datenschutz- und sicherheitsrelevanten Ereignissen den Betrieb einzelner IT-Anwendungen oder Dienste einzuschränken oder zu unterbinden.
5. Betriebs- und Wartungszeiten:
   a. Betriebszeiten eLogin: 24/7
   b. Betriebszeiten NOVA: Mo-Fr, 6-22 Uhr (bayerische Feiertage sind davon ausgenommen)
   c. Wartungszeiten eLogin&NOVA: werden Administratoren der nutzenden Stellen rechtzeitig vorher per E-Mail angekündigt

6 Mitwirkung der nutzenden Stelle

1. Die nutzende Stelle hat in ihrem Verantwortungsbereich die notwendigen technischen und organisatorischen Voraussetzungen einschließlich der Bereitstellung eines entsprechenden Netzanschlusses zu schaffen (Internetzugang, üblicher Internet-Browser mit entsprechenden Zertifikaten zur verschlüsselten Kommunikation der nutzenden Stelle mit der DSRV).
2. Sofern die nutzende Stelle personenbezogene Daten verarbeitet, muss sie geeignete und dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen (zum Beispiel Firewall, Virenscanner etc.) treffen, die die Gewährleistung der Einhaltung datenschutzrechtlicher Vorschriften erfordern.
   Dies sind Maßnahmen zur Datensicherung mit dem Ziel,
   a. den Verlust der Vertraulichkeit,
   b. den Verlust der Transparenz,
   c. den Verlust der Revisionsfähigkeit,
   d. den Verlust der Integrität und
   e. den Verlust der Authentizität zu verhindern sowie
   f. die Verfügbarkeit der Verfahren und der Daten sicherzustellen.
3. Im Fall einer Störung im Zusammenhang mit der Nutzung der Verfahren hat die nutzende Stelle unverzüglich die bei der DSRV eingerichtete und in Kapitel 6 benannte Hotline zu informieren. Die näheren Einzelheiten über die Art und den Umfang der Fehlermeldung einschließlich der Service- und Reaktionszeiten teilt die DSRV der nutzenden Stelle mit.

4. Die nutzende Stelle hat der DSRV schriftlich oder elektronisch mindestens zwei Administratoren zu benennen (Vertreterregelung). Diese erhalten Handbücher zur Administration ihrer Benutzer.
5. Die NOVA-Administratoren der nutzenden Stellen tragen die Verantwortung für
    a. die Umsetzung von Sicherheitsstandards bei Konfiguration, Betrieb und Nutzung der betroffenen Anwendungen,
    b. die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen (Notfallverantwortlicher) bei Eintreten eines der in Anhang B definierten Sicherheitsvorfälle,
    c. die Entgegennahme von Meldungen über Sicherheitsvorfälle,
    d. die Untersuchung und Bewertung von Sicherheitsvorfällen,
    e. die Nachbearbeitung von Sicherheitsvorfällen und
    f. die Überprüfung der Einhaltung der Sicherheitsvorkehrungen.
6. Änderungen beziehungsweise Abmeldungen der in den Verfahren registrierten Administratoren (oder deren Vertreter) müssen der DSRV unverzüglich und schriftlich oder elektronisch mitgeteilt werden.
7. Die nutzende Stelle übermittelt die Benutzerdaten durch Eingabe in die NOVA an die DSRV. Diese verarbeitet die Benutzerdaten in Erfüllung der Teilnahme- und Nutzungsbedingungen. Die Benutzerdaten werden nur für die Zugangs- und Zugriffskontrolle verarbeitet und unterliegen einer strengen Zweckbindung (§ 67c Abs. 4 SGB X).
8. Die nutzende Stelle verpflichtet sich dazu,
    a. der in Anhang A beschriebenen Handlungsanweisung bei Sicherheitsvorfällen nachzukommen.
    b. sich an die in Anhang B beschriebenen Richtlinien zum ordnungsgemäßen Umgang mit den Anmeldeinformationen zu halten.

7 Haftung

1. Nach Artikel 82 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen die an der Verarbeitung beteiligte Verantwortliche.
2. Soweit die Verantwortliche zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihr der Rückgriff gegenüber den übrigen an der Verarbeitung Beteiligten vorbehalten, soweit diese für den entstandenen Schaden mitverantwortlich sind.
3. Die an der Datenverarbeitung beteiligten Stellen unterstützen sich gegenseitig bei der Sachverhaltsaufklärung im Zusammenhang mit den unter den Ziffern 1 und 2 bezeichneten Ansprüchen, soweit gesetzlich zulässig.
4. Die Datenstelle der Rentenversicherung haftet nicht für Schäden durch fahrlässige Pflichtverletzung, soweit nicht Verletzungen des Lebens, des Körpers oder der Gesundheit anderer betroffen sind. Datenschutzverletzungen sind hiervon ausgenommen.

8 Geheimhaltung und Datenschutz

1. Die Benutzerdaten sind zunächst Beschäftigtendaten der nutzenden Stellen, die für die Durchführung des Dienst- oder Beschäftigungsverhältnisses nach den jeweils geltenden Datenschutzbestimmungen verarbeitet werden dürfen.
   Zur Durchführung des Beschäftigungsverhältnisses gehört auch die Gestaltung der Auf-

bau- und Arbeitsablauforganisation (zum Beispiel: dienstliche E-Mail-Adresse, dienstliche Telefonnummer, Einordnung in eine Abteilung). Den Beschäftigten müssen in der modernen Arbeitswelt auch Verarbeitungsmittel im erforderlichen Umfang zur Verfügung gestellt werden. Für die Steuerung des Zugangs zu den Verarbeitungsmitteln dürfen im notwendigen Umfang auch Beschäftigtendaten verarbeitet werden (zum Beispiel: Benutzer-Kennungen). Die nutzende Stelle verpflichtet sich, die im SGB I und SGB X enthaltenen Vorschriften über den Schutz der Sozialdaten zu beachten und einzuhalten. Sie hat insoweit das Sozialgeheimnis (§ 35 Abs. 1 SGB I) in ihrem Betrieb in der gleichen Weise zu wahren wie die Rentenversicherung.

2. Die DSRV betreibt die IT Anwendungen eLogin/NOVA als Verarbeitungsmittel sowohl für sich als auch für die nutzenden Stellen. Für die Datenverarbeitung mit eLogin/NOVA ist die DSRV verantwortlich. Die IT-Anwendungen eLogin/NOVA dienen der Steuerung des ordnungsgemäßen Betriebes von weiteren IT-Anwendungen und Diensten der DSRV mit denen Sozialdaten verarbeitet werden. Insbesondere werden der Zugang zu den IT-Verfahren und Diensten und der Zugriff auf Sozialdaten bedarfsgerecht gesteuert (Zweckbestimmung und Zweckbindung, § 67c Abs. 4 SGB X). Die Verarbeitung der Organisations- und Benutzerdaten erfolgt im Rahmen der Aufgabenerfüllung der DSRV, die sich aus den Bestimmungen des Sozialgesetzbuches ergibt.
Die Organisations- und Benutzerdaten sind in der Verfügungsgewalt der DSRV und deshalb ebenfalls Sozialdaten (§ 67 Abs. 2 SGB X), welche dem Schutzbereich des Sozialgeheimnisses und der Bestimmungen des Sozialdatenschutzes (§ 35 SGB I, §§ 67ff SGB X) unterliegen.
Durch die Eingaben von Organisations- und Benutzerdaten in eLogin/NOVA übermittelt die nutzende Stelle Beschäftigtendaten an die DSRV. Die DSRV erhebt diese Daten und verarbeitet sie zu den oben genannten Zweckbestimmungen.

3. Betroffene Personen, deren Daten durch einen Verantwortlichen verarbeitet werden, müssen spätestens im Moment der Datenerhebung über gesetzlich festgelegte Aspekte der Datenverarbeitung informiert werden. Die DSRV stellt hierfür ein Merkblatt zur Verfügung. Dieses können alle Benutzer jederzeit in eLogin im Benutzerbereich einsehen. Das Merkblatt informiert auch, wie Benutzer Auskunft über die eigenen verarbeiteten Daten erhalten können.
Welche Daten über die nutzende Stelle verarbeitet werden, können die NOVA-Administratoren der nutzenden Stelle ebenfalls in eLogin jederzeit einsehen. Zusätzlich werden Papierunterlagen verarbeitet – die Bestätigung der Kenntnisnahme dieser Teilnahme- und Nutzungsbedingungen, ggf. weiterer Schriftwechsel.

4. Die nutzenden Stellen dürfen die von der DSRV zur Verfügung gestellten IT-Anwendungen nur für die Zulassung berechtigter Personen und deren dienstlicher Nutzung von IT-Anwendungen der DSRV verwenden. Die nutzenden Stellen entscheiden eigenverantwortlich, welchen Beschäftigten für wie lange die Zugangs- und Zugriffsrechte eingeräumt werden.

Der Verantwortliche muss technische und organisatorische Sicherheitsmaßnahmen umsetzen. Die Datenübertragung zwischen IT-Systemen der nutzenden Stellen und der DSRV erfolgt verschlüsselt. Die IT-Anwendungen eLogin/NOVA sind selbst Bestandteil der Sicherheitsmaßnahmen der DSRV für die Steuerung des Zugangs und des Zugriffs auf Sozialdaten der Rentenversicherung.
Für den Datenschutz und die IT-Sicherheit in ihren Organisationen sowie die bestimmungsmäßige Verwendung der IT-Anwendungen eLogin/NOVA tragen die nutzenden Stellen die Verantwortung.

9 Schlussbestimmungen

Es gilt ausschließlich das Recht der Bundesrepublik Deutschland.

Sollte eine Bestimmung dieser allgemeinen Teilnahme- und Nutzungsbedingungen unwirksam sein oder werden, so wird die Wirksamkeit der Teilnahme- und Nutzungsbedingungen im Übrigen hierdurch nicht berührt. An die Stelle der unwirksamen Bedingung tritt diejenige Bedingung als maßgeblich, die dem Sinn und Zweck der unwirksamen Bedingung am nächsten kommt. Entsprechendes gilt bei Unvollständigkeit der Teilnahme- und Nutzungsbedingungen.

10 Anhang A: Handlungsanweisung bei Sicherheitsvorfällen

10.1 Sicherheitsvorfälle

Als Sicherheitsvorfall wird jedes Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden bezüglich Vertraulichkeit, Integrität und Authentizität der Daten hervorrufen können. Die Verfügbarkeit hat dabei keine Bedeutung. Auf Kap. B1.8 des IT-Grundschutzkataloges des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird verwiesen.

Sicherheitsvorfälle werden zum Beispiel erkennbar durch:

- gesperrte Benutzerkennungen ohne erkennbaren Grund
- Fehlermeldungen des Systems, die auf einen Missbrauch hindeuten
- Auftreten von Computer-Viren
- vorsätzlicher Missbrauch der Anwendung
- Abruf von Daten, die nicht für den Geschäftsablauf notwendig sind (Abruf zusätzlicher Versicherungskonten)

10.2 Eskalationsstufen/Behandlung von Sicherheitsvorfällen

Die Eskalationsstufen beschreiben ein hierarchisches Modell zur Behandlung von Sicherheitsvorfällen, bei dem jede höhere Stufe die Maßnahmen der darunter liegenden beinhaltet.

10.3 Konsequenzen bei Verstößen

Verstöße gegen diese Teilnahme- und Nutzungsbedingungen werden der zuständigen Aufsichtsbehörde gemeldet.

10.4 Reaktion auf Störungen oder Alarmierungen

Bei einem Missbrauchs- bzw. Schadensverdacht sind die in dieser Handlungsanweisung festgelegten Schritte einzuhalten.

Grundsätzlich ist die in Kapitel 5 genannte Hotline der Deutschen Rentenversicherung Bund zu informieren.
Bei vorsätzlichem oder fahrlässigem Verstoß gegen die in diesen Teilnahme- und Nutzungsbedingungen niedergelegten Grundsätze sind die gleichen Maßnahmen zu treffen, wie bei Missachtung von Organisationsanweisungen. Nach Prüfung durch die IT-Sicherheit und den Datenschutzbeauftragten der Deutschen Rentenversicherung Bund sind in Abhängigkeit der Schwere des Verstoßes die Aufsichtsbehörden der nutzenden Stellen zu informieren.

Es muss untersucht werden, wie und wo die Verletzung der in diesen Teilnahme- und Nutzungsbedingungen niedergelegten Grundsätze entstanden ist.

Anschließend müssen angemessene schadensbehebende oder -mindernde Maßnahmen und, sofern erforderlich, zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen von der Schwere des Verstoßes und des Schadens ab.

Es muss geregelt sein, wer auf Seiten der nutzenden Stelle für Kontakte mit der Deutschen Rentenversicherung Bund und anderen Behörden (zum Beispiel der zuständigen Aufsichtsbehörde) verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es muss dafür Sorge getragen werden, dass evtl. mitbetroffene Stellen schnellstens informiert werden. Die Verantwortlichkeiten und Maßnahmen bei Sicherheitsvorfällen sind in dieser Handlungsanweisung beschrieben.

10.5 Evaluierung der Eskalationsstrategie

Nach einem eingetretenen Sicherheitsvorfall ist die Durchführung der Maßnahmen von der nutzenden Stelle zu auditieren und einer abschließenden Bewertung zu unterziehen. Die Ergebnisse dieser Bewertung sind der in Kapital 5 genannten Hotline der Deutschen Rentenversicherung Bund mitzuteilen, um eine transparente Optimierung der Sicherheitsmechanismen in Absprache mit der nutzenden Stelle zu ermöglichen.

11 Anhang B: Richtlinien zum ordnungsgemäßen Umgang mit den Anmeldeinformationen

11.1 Umgang mit Benutzerkennung und Passwort

11.1.1 Einrichten und Ändern von Benutzerkennungen

- Benutzerkennungen werden maschinell gebildet.
- Benutzer dürfen nur durch den jeweiligen Administrator angelegt werden.
- Wenn ein Mitarbeiter aus der nutzenden Stelle ausscheidet oder über eLogin keinen Zugang mehr zu den Verfahren erhalten soll, muss die ihm zugewiesene Benutzerkennung unverzüglich stillgelegt werden.
  Aus Revisionsgründen und im Rahmen der Datensicherheit werden die Zugriffe bei der Deutschen Rentenversicherung protokolliert und für ein Jahr gespeichert.
- Um einen Missbrauch zu verhindern, ist die vorübergehende Sperrung der Benutzerkennung bei längerer Abwesenheit der berechtigten Person vorzunehmen.
- Die Vergabe/Änderung/Sperrung einer Benutzerkennung wird maschinell dokumentiert.

11.1.2 Richtlinien zum Umgang mit Kennwörtern

Beim Umgang mit Kennwörtern ist Folgendes zu beachten:

- Das Kennwort darf nicht leicht zu erraten sein.
- Das Kennwort muss geheim gehalten werden und darf nur dem Benutzer persönlich bekannt sein. Es ist verboten die Kennwörter aufzuschreiben oder zu hinterlegen.
- Ein Kennwortwechsel ist durchzuführen, wenn das Kennwort oder die Benutzerkennung unautorisierten Personen bekannt geworden ist.
- Jeder Benutzer muss sich nach der Aufgabenerfüllung am Verfahren abmelden.
- Jedes Kennwort muss bei der ersten Anmeldung geändert werden (Startkennwort).
- Benutzer werden nach drei falschen Kennworteingaben gesperrt. Die Anmeldung wird abgebrochen.
- Um einen Missbrauch durch Unbefugte auszuschließen, ist der Zugang zum PC beim Verlassen des Arbeitsplatzes zu sperren (zum Beispiel durch das Ziehen der Mitarbeiterchipkarte oder Aktivieren des Bildschirmschoners mit Kennwortschutz).
- Kennwörter sind unbeobachtet einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt werden.
- Fremde Kennwörter dürfen nicht ausgeforscht, ausprobiert oder benutzt werden.
- Kennwörter müssen so komplex wie technisch möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.

Kennwörter, die leicht zu erraten sind (Trivial-Kennwörter), dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:

- Begriffe wie zum Beispiel „Test", „Gast" oder „System",
- Begriffe aus dem Aufgabengebiet,
- Automarken, PKW-Kennzeichen, einfache Ziffern- und Buchstabenkombinationen,
- Zahlen und Daten aus dem Lebensbereich des Benutzers,
- Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen,
- Zeichenwiederholungen oder Zeichen, die durch nebeneinander liegende Tasten eingegeben werden.

Auf Antrag eines Berechtigten hebt der zuständige Administrator der nutzenden Stelle die Sperre der Benutzerkennung auf, nachdem er sich von der Identität des Berechtigten überzeugt hat.

11.2 Umgang mit Signaturkarten

Beim Umgang mit Signaturkarten ist Folgendes zu beachten:

- Akzeptiert werden nur Signaturkarten mit qualifizierter elektronischer Signatur (QES).
- Die Beschaffung der Signaturkarten sowie der Kartenleser erfolgt in Zuständigkeit der nutzenden Stellen.
- Die Freischaltung der Karte sowie die Vergabe der PIN erfolgen nur durch den einzelnen Benutzer.
- Die Signaturkarte ist von jedem einzelnen Benutzer sicher zu verwahren.
- Eine Weitergabe an Dritte ist nicht zulässig.

Für den Umgang mit der PIN gelten die Richtlinien und Vorgaben des entsprechenden Vertrauensdiensteanbieters.

Der neue Personalausweis mit eID wird an dieser Stelle nicht akzeptiert, da keine Vermischung von Berufs- und Arbeitsleben stattfinden soll.

11.3 Vergabe von Zugriffsrechten

Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils zuständigen Administrator vorzunehmen.