Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD

(Online-Weisung EJPD)

vom 30. September 2004

Das Eidgenössische Justiz- und Polizeidepartement,

gestützt auf Artikel 38 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[1] (RVOG),

verordnet:

1. Abschnitt: Allgemeines

Art. 1 Zweck

[1] Diese Weisung harmonisiert das Verfahren bei der Einrichtung von Online-Verbindungen im Eidgenössischen Justiz- und Polizeidepartement (EJPD).

[2] Sie regelt:

a. das Verfahren und die Voraussetzungen für die Einrichtung einer Online-Verbindung zwischen dem EJPD und den Organen des Bundes und der Kantone, mit welcher Angestellte dieser Organe (Benutzende) Zugang durch ein Abrufverfahren zu einer Informatikanwendung des EJPD erhalten;

b. das Verfahren und die Voraussetzungen für die Erteilung von individuellen Zugriffsbewilligungen oder von Gruppenzugriffsbewilligungen an diese Benutzenden, wenn ihnen Personendaten durch diese Online-Verbindung zugänglich gemacht werden.

Art. 2 Voraussetzungen

Voraussetzungen für die Einrichtung einer Online-Verbindung zwischen einer Informatikanwendung des EJPD und den Benutzenden sind:

a. eine hinreichende gesetzliche Grundlage nach Artikel 19 Absatz 3 des Bundesgesetzes vom 19. Juni 1992[2] über den Datenschutz (DSG), welche die Zugriffsberechtigungen und ihre wesentlichen Rahmenbedingungen festlegt (Art. 3);

b. die Zweckbindung (Art. 4);

c. die Sicherheit der Online-Verbindung (Art. 5);

1 SR **172.010**
2 SR **235.1**

d. ein Gesuch der zuständigen kantonalen Behörde, wenn die Einrichtung einer Online-Verbindung einen kantonalen Dienst betrifft (Art. 16).

2. Abschnitt: Grundsätze für die Einrichtung einer Online-Verbindung

Art. 3 Rechtsgrundlage

Eine Online-Verbindung bedarf einer ausdrücklichen Rechtsgrundlage. Sind besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen, bedarf es eines formellen Gesetzes.

Art. 4 Zweckbindung

1 Eine Online-Verbindung darf nur zu den in der Rechtsgrundlage definierten Zwecken eingerichtet werden.

2 Umschreibt die Rechtsgrundlage den Zweck nur in allgemeiner Weise, muss das Gesuch um Einrichtung einer Online-Verbindung den Zweck präziser umschreiben.

Art. 5 Sicherheit

1 Eine Online-Verbindung darf erst dann installiert werden, wenn die korrekte Bearbeitung der Daten und die Datensicherheit gewährleistet werden können, d. h. wenn die technischen und organisatorischen Massnahmen nach Abschnitt 3 erfüllt sind.

2 Der Zugang zu allen Informationen und Fachanwendungen des EJPD wird von einer zentralen Sicherheitsinfrastruktur (SSO Portal EJPD[3]) gesteuert. Das SSO Portal EJPD gewährleistet eine standardisierte Benutzerverwaltung und eine starke Benutzerauthentisierung.

3. Abschnitt: Technische und organisatorische Massnahmen

Art. 6 Risikobeurteilung

Vor der Inbetriebnahme einer Informatikanwendung mit einer Online-Verbindung nimmt das für die Anwendung verantwortliche Bundesamt eine Risikobeurteilung nach den entsprechenden Weisungen des Informatikrates Bund (IRB) sowie des Informatikstrategieorgans des Bundes (ISB) vor und setzt die daraus abgeleiteten Massnahmen um.

3 Single-Sign-On Portal EJPD

Art. 7 Sicherheitskonzept der Informatikanwendung

1 Das für die Informatikanwendung verantwortliche Bundesamt erstellt auf der Grundlage der Risikobeurteilung ein Konzept über die Informatiksicherheit, welches hinreichende technische und organisatorische Schutz- und Sicherheitsmassnahmen nach Artikel 20 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG[4]) beschreibt.

2 Das Sicherheitskonzept der Informatikanwendung legt namentlich fest:

a. die Anwendungsverantwortlichen;
b. die Datenschutzverantwortlichen;
c. die Informatiksicherheitsverantwortlichen;
d. das Aufsichtsorgan;
e. die Protokollierungsregeln;
f. das Verfahren der Benutzeridentifikation und -authentisierung;
g. die Datenchiffrierung;
h. das Zugriffserteilungsverfahren;
i. die Regeln und das Verfahren für die Unterbrechung inaktiver Verbindungen und für die Sperrung nicht beanspruchter Zugriffsrechte;
k. das Verfahren der Kontrolle nach Artikel 9 Absatz 1 VDSG.

3 Das Sicherheitskonzept der Informatikanwendung ist periodisch durch das hierfür verantwortliche Bundesamt zu aktualisieren.

4 Der Schlussbericht des Informatiksicherheitsbeauftragten des Departements (ISBD) und des Informatikstrategieorgans Bund (ISB) kann das Sicherheitskonzept der Informatikanwendung ersetzen, wenn die in Absatz 2 genannten Punkte im Bearbeitungsreglement aufgeführt werden.

Art. 8 Bearbeitungsreglement

Die für die Informatikanwendungen verantwortlichen Bundesämter erlassen nach Artikel 21 VDSG ein Bearbeitungsreglement ihrer Informatikanwendungen.

4. Abschnitt: Grundsätze für die Erteilung von individuellen Zugriffsbewilligungen

Art. 9 Eignung

Der Online-Zugriff muss geeignet sein, den konkreten Benutzungszweck zu erreichen.

4 SR **235.11**

Art. 10 Notwendigkeit

[1] Ein Online-Zugriff muss zur Erfüllung der gesetzlich übertragenen Aufgaben erforderlich sein.

[2] Die Notwendigkeit ist anzunehmen, wenn die Aufgabe ohne den Online-Zugriff nicht ohne unverhältnismässigen Mehraufwand erfüllt werden kann.

Art. 11 Verhältnismässigkeit

[1] Der Online-Zugriff muss verhältnismässig sein.

[2] Er ist verhältnismässig, wenn der Eingriff in die Persönlichkeit der betroffenen Personen in einem angemessenen Verhältnis zum zu erwartenden Nutzen der Datenbearbeitung steht.

[3] Die Zugriffberechtigung ist auf die Daten und Bearbeitungsfunktionen zu beschränken, welche für die Aufgabenerfüllung des Benutzenden notwendig sind.

Art. 12 Beurteilungskriterien

Bei der Beurteilung der Grundsätze nach den Artikeln 9–11 sind namentlich folgende Kriterien massgeblich:

a. voraussichtliche Nutzungsfrequenz des einzelnen Zugriffs;

b. bisherige Nutzungsfrequenz des betreffenden Organs;

c. Anzahl der bereits zugriffsberechtigten Mitarbeitenden des betreffenden Organs;

d. gesamter Zugriffsumfang des betreffenden Organs;

e. Notwendigkeit des unabhängigen und raschen Handelns (z.B. ausserhalb der ordentlichen Geschäftszeiten);

f. beantragte Zugriffsprivilegien (Suchkriterien, Umfang der einsehbaren Daten);

g. beantragte Funktionen (Abfragen, Schreiben, Mutieren, Löschen).

5. Abschnitt: Organisation

Art. 13 Zentrale Authentisierungsstelle

[1] Die zentrale Authentisierungsstelle (Authentisierungsstelle EJPD) ist zuständig für die Authentisierung von Benutzenden, die einen Online-Zugriff auf Informatikanwendungen des EJPD beantragen. Sie führt das SSO Portal EJPD.

[2] Sie nimmt die Gesuche um Zugriffserteilung entgegen, authentisiert die Benutzenden und leitet die Begehren an das für die Informatikanwendung verantwortliche Bundesamt weiter.

[3] Sie koordiniert das Verfahren für die Erteilung von individuellen Zugriffsbewilligungen.

Art. 14 Zuständigkeiten des für die Informatikanwendung verantwortlichen Amtes

1 Die Datenschutzberaterin oder der Datenschutzberater des für die Informatikanwendung verantwortlichen Bundesamtes (DSBO) überwacht die Planung und die Errichtung von Online-Verbindungen und sorgt für die Einhaltung der Regeln zur Erteilung der individuellen Zugriffsbewilligungen.

2 Sie oder er prüft das erste individuelle Gesuch um Zugriffsbewilligung aus jedem Organ des Bundes oder der Kantone und kontrolliert, ob die Voraussetzungen nach dem 4. Abschnitt erfüllt sind. Sie oder er überwacht stichprobenweise nach den Ziffern 9–12 die Erteilung der nächsten individuellen Zugriffsbewilligungen.

3 Sie oder er prüft die Richtigkeit und Vollständigkeit des Bearbeitungsreglements.

4 Die oder der Informatiksicherheitsbeauftragte der Verwaltungseinheit (ISBO) ist zuständig für die Prüfung der Informatiksicherheitsaspekte. Sie oder er prüft namentlich die Konformität der Sicherheitsmassnahmen zu den Voraussetzungen der Artikel 6 und 7.

Art. 15 Leistungserbringer der Informatikanwendung

Der Leistungserbringer jeder Informatikanwendung ist zuständig für die technische Umsetzung der Online-Verbindungen, wenn die individuellen Zugriffsbewilligungen erteilt sind.

6. Abschnitt: Verfahren für die Einrichtung einer Online-Verbindung

Art. 16 Gesuch der zuständigen kantonalen Behörde

Die zuständige kantonale Behörde richtet das Gesuch um die Einrichtung einer Online-Verbindung an das für die Informatikanwendung verantwortliche Bundesamt. Das Gesuch enthält:

a. den Namen der Organe, für welche sie die Einrichtung einer Online-Verbindung beantragt;

b. den Namen der Informatikanwendung, für welche diese Organe eine Online-Verbindung brauchen;

c. den Zweck, für welchen die Verbindung eingerichtet werden soll, sofern die Rechtsgrundlage den Zweck nur in allgemeiner Weise umschreibt.

Art. 17 Prüfung des Gesuchs zur Einrichtung einer Online-Verbindung

1 Die oder der DSBO prüft das Gesuch, namentlich:

a. das Bestehen einer hinreichenden Rechtsgrundlage;

b. die Zweckbindung;

c. die Gesuche für Gruppenzugriffsbewilligungen.

2 Sie oder er stellt das Bearbeitungsreglement der Informatikanwendung der gesuchstellenden kantonalen Behörde zu, wenn das Gesuch angenommen wird.

7. Abschnitt:
Verfahren für die Bewilligung von individuellen Online-Zugiffen

Art. 18 Anschlussgesuch

1 Das Gesuch um die Erteilung einer individuellen Zugriffsbewilligung ist mit einem Formular des EJPD einzureichen, das über das Internet oder Intranet abgerufen werden kann.

2 Das Gesuch ist elektronisch an die Authentisierungsstelle EJPD zu senden.

Art. 19 Prüfung der individuellen Bewilligungsgesuche zum Online-Zugriff

1 Das für die Informatikanwendung verantwortliche Bundesamt prüft die individuellen Bewilligungsgesuche zum Online-Zugriff nach den Grundsätzen des 4. Abschnitts.

2 Beim ersten individuellen Gesuch eines Organs des Bundes oder der Kantone prüft die oder der DSBO sämtliche Bewilligungsvoraussetzungen. Bei der Prüfung von weiteren, individuellen Zugriffsbewilligungen für die Benutzenden desselben Organs werden die Bewilligungsvoraussetzungen stichprobenweise kontrolliert.

3 Das für die Informatikanwendung verantwortliche Bundesamt bezeichnet die Personen, welche die weiteren Gesuche bearbeiten. Es kann kantonale Organe mit der Prüfung der weiteren Begehren beauftragen.

Art. 20 Gruppenzugriffsbewilligungen

1 Eine Gruppenzugriffsbewilligung erlaubt allen Benutzenden einer bestimmten Benutzergruppe die Verwendung der gleichen Identifikationsparameter (Gruppen-Logins) bei der Anmeldung beim SSO Portal EJPD und bei den Informatikanwendungen des EJPD.

2 Eine Gruppenzugriffsbewilligung kann einer bestimmten Benutzergruppe erteilt werden, wenn die Voraussetzungen nach dem 4. Abschnitt erfüllt sind. Zusätzlich müssen fogende Bedingungen erfüllt sein:

a. die Arbeitsstation wird laufend benutzt;

b. die Verbindung mit einer Anwendung muss sehr schnell erstellt werden, weil der Zugriff dringend ist;

c. die Arbeitsstation kann durch sämtliche Mitglieder der im Zugriffsbegehren erwähnten Benutzergruppe benutzt werden;

d. die Inhaberinnen und Inhaber von Gruppenbewilligungen können im betreffenden Informationssystem Daten nur abfragen;

e. die Schichtpläne der Benutzergruppe werden während eines Jahres aufbewahrt;

f. die Liste der Mitglieder der Benutzergruppe wird dem oder der Anwendungsverantwortlichen weitergegeben; und

g. die Mutationen in der Benutzergruppe werden zweimal jährlich dem oder der Anwendungsverantwortlichen gemeldet.

Art. 21 Aufsicht

Die oder der DSBO überprüft periodisch, ob die gewährten Zugriffe den Anforderungen nach dem 4. Abschnitt entsprechen.

8. Abschnitt: Schlussbestimmungen

Art. 22 Ausführungsbestimmungen

Diese Weisung ist als Anhang integraler Bestandteil der Bearbeitungsreglemente aller Informatikanwendung des EJPD mit Online-Verbindungen.

Art. 23 Übergangsbestimmungen

[1] Die beim Inkrafttreten der vorliegenden Weisung bestehenden individuellen Zugriffsberechtigungen bleiben bis zur Einführung der starken Authentisierung der Benutzenden bestehen. Zu diesem Zeitpunkt werden die individuellen Zugriffsbewilligungen gemäss Artikel 19 überprüft.

[2] Wenn eine bestehende Informatikanwendung durch eine neue ersetzt wird, so bleiben die Bewilligungen zur Einrichtung einer Online-Verbindung (Art. 17) gültig.

[3] Bis zur Einführung der digitalen Signatur im EJPD ist zwingend ein unterschriebener Abdruck des Anschlussbegehrens (Art. 18 Abs. 1) per Post oder per Fax an die Authentisierungsstelle EJPD zu schicken.

[4] Das EJPD stellt die Bearbeitungsreglemente der Informatikanwendungen, die am 31. August 2004 online zugänglich sind, den für die angeschlossenen Organen der Kantone zuständige kantonale Behörde bis zum 31. Dezember 2004 zu.

Art. 24 Inkrafttreten

Diese Weisung tritt am 1. Oktober 2004 in Kraft.

30. September 2004 Eidgenössisches Justiz- und Polizeidepartement:

Christoph Blocher