Bericht

der Geschäftsprüfungskommission des Ständerates vom 19. November 1998 «Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens»

Stellungnahme des Bundesrates

vom 23. Juni 1999

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren,

Am 17. November 1998 haben Sie uns Ihren Bericht «Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens» zugestellt. Der Bericht enthält eine vom Ständerat am 17. November 1998 übermittelte Motion und von Ihrer Kommission formulierte Empfehlungen. Sie laden uns ein, zu ihrem Bericht sowie zum beiliegenden Expertenbericht vom 30. Juli 1998 Stellung zu nehmen.

Der Bundesrat äussert sich zur Motion, zu den Empfehlungen der Geschäftsprüfungskommission des Ständerates (GPK-S) und zum Expertenbericht wie folgt:

Genehmigen Sie, sehr geehrter Herr Präsident, sehr geehrte Damen und Herren, den Ausdruck unserer ausgezeichneten Hochachtung.

23. Juni 1999

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Ruth Dreifuss
Der Bundeskanzler: François Couchepin

10470

Stellungnahme

1 Einleitende Bemerkungen

Vorab möchte der Bundesrat den Mitgliedern der GPK-S seinen Dank für die Prüfung der wichtigen Frage der Online-Verbindungen im Polizeibereich aussprechen. Die rasante Entwicklung im Bereich der Informatik- und Telekommunikationstechnologie hat zu einer massiven Zunahme der Ausrüstung mit EDV-Anwendungen und Online-Verbindungen geführt. Das EJPD hat diese Entwicklung mitgemacht; wobei das Einrichten von Online-Verbindungen immer nur mit dem Ziel geschah, die Aufgaben im Polizeibereich effizienter zu erfüllen unter gleichzeitiger Wahrung des Persönlichkeitsschutzes der Betroffenen. Es ist klar, dass diese Entwicklung nicht unkontrolliert verlaufen darf. Im Rahmen des HERMES[1]-Verfahrens ist festgelegt, dass die einzelnen Phasen bei der Einrichtung von neuen Online-Verbindungen ein Genehmigungsverfahren vor dem Projektausschuss zu durchlaufen haben. Zusätzlich zum Bewilligungsverfahren nach HERMES muss im EJPD die Freigabe der einzelnen Projektphasen vom stellvertretenden Generalsekretär des EJPD, dem der Bereich Informatik des Departementes untersteht, genehmigt werden.

2 Motion der GPK-S

Gestützt auf den vorliegenden Bericht hat der Ständerat die folgende Motion seiner Geschäftsprüfungskommission an den Bundesrat übermittelt:

> Erhöhter Schutz für Personendaten bei Online-Verbindungen
>
> Der Bundesrat unterbreitet eine Revision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz. Die Revision verfolgt folgende Ziele:
>
> a. Bei der Errichtung von Online-Verbindungen ist auch für Pilotprojekte eine gesetzliche Grundlage vorzusehen.
>
> b. Bei Gesuchen und der Errichtung von Online-Anschlüssen an Informationssysteme des Bundes schafft dieser Mindeststandards für die Zusammenarbeit zwischen Bund und Kantonen. Er legt Zugriff, Nutzung, Schutz und Kontrolle seiner Datenbanken fest.

Am 8. März 1999 hat der Bundesrat seine Stellungnahme zur Motion der GPK-S dem Ständerat unterbreitet und beantragt, sie in ein Postulat umzuwandeln. An seiner Sitzung vom 16. März 1999 hat der Ständerat die Motion angenommen. Den Ausführungen des Departementschefs EJPD, wonach sich dieser der Motion dann nicht widersetze, wenn die verlangte Rechtsgrundlage für Pilotprojekte von Online-Verbindungen auf Stufe Bundesratsverordnung geschaffen werden könne, wurde

[1] Instrument und Standard für das Führen und Abwickeln von Informatikprojekten (vgl. Handbuch «Hermes», BFI, Ausgabe 1995

dabei Rechnung getragen. Im Folgenden ist die Antwort des Bundesrates auf die Motion der GPK-S integral wiedergegeben:

«Nach geltendem Recht bedarf es einer ausdrücklichen gesetzlichen Grundlage um ein Abrufverfahren einzurichten, das den Online-Zugang zu einer Datenbank erlaubt, die durch ein Bundesorgan im Sinne von Artikel 3 Buchstabe h DSG[2] *geführt wird und Personendaten enthält (Art. 17 Abs. 1 und Art. 19 Abs. 3 DSG). Wenn ein Abrufverfahren besonders schützenswerte Daten oder Persönlichkeitsprofile zugänglich macht, ist eine ausdrückliche Grundlage in einem formellen Gesetz erforderlich (Art. 19 Abs. 3 DSG). Der Bundesrat interpretiert diese Vorschriften in dem Sinne, dass sie auf jedes Datenbank-Projekt anwendbar sind, auch während der Pilotphase. Aus diesem Grund wäre es unnötig, eine Revision des DSG vorzunehmen, um zu präzisieren, dass die Vorschriften dieses Gesetzes auch für die Pilotphase von Informatikprojekten gelten.*

Nach Ansicht des Bundesrates geht es in Zukunft nicht so sehr darum, die Vorschriften des DSG bezüglich der gesetzlichen Grundlage zu verschärfen, sondern eher darum, diese zu optimieren. Die Notwendigkeit einer formellen gesetzlichen Grundlage für die Einführung eines Online-Zugangs zu besonders schützenswerten Daten verursacht nämlich gewisse Probleme in der Einführungsphase eines Projekts. Ohne eine Erprobung unter realistischen Bedingungen ist es oft schwierig, den Kreis der Bundesbehörden und kantonalen Instanzen, und in gewissen Fällen auch der Privatpersonen, zu umschreiben, der den Zugang mittels eines Abrufverfahrens zu einer im Aufbau befindlichen Datenbank benötigt. Die strikte Beachtung der Forderung nach einer formellen gesetzlichen Grundlage kann letztlich zu einer zu weiten Regelung führen, die Erwartungen bei den im Gesetz genannten Stellen weckt und folglich später eine Verweigerung eines Gesuchs um Online-Zugang erschwert.

In Anbetracht dieses Problems ist der Bundesrat bereit, eine Revision des DSG zu beantragen und eine spezifische Regelung vorzuschlagen für die Pilotphase eines Projektes, wenn ein wichtiges öffentliches Interesse die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen vor dem Erlass einer formellen gesetzlichen Grundlage erfordert. Eine Möglichkeit wäre die Schaffung einer Delegationsnorm im DSG, die es erlaubt, sich während dieser Phase auf eine Verordnung des Bundesrates zu stützen, oder auf eine Bewilligung durch den Datenschutzbeauftragten, die an Bedingungen geknüpft wäre. Das vorläufige Fehlen der gesetzlichen Grundlage müsste durch andere Garantien kompensiert werden, die eine Sicherstellung des Schutzes der Persönlichkeit der betroffenen Personen gewährleisten.

Da aus dem Text der Motion nicht klar hervorgeht, ob sich die Notwendigkeit einer gesetzlichen Grundlage auf eine formelle oder materielle gesetzliche Grundlage bezieht, beantragt der Bundesrat, die Motion in ein Postulat umzuwandeln.

Gegenwärtig ist der Geltungsbereich des DSG bezüglich der Organe, die Personendaten bearbeiten, begrenzt. Die Datenbearbeitung durch die Kantone wird grundsätzlich nicht durch das DSG, sondern durch das kantonale Recht geregelt (Art. 2 Abs. 1 DSG). Es spielt diesbezüglich keine Rolle, ob die bearbeiteten Daten direkt von den Kantonen erhoben worden sind, oder ob sie ihnen durch den Online-Zugang zu einer vom Bund geführten Datenbank übermittelt worden sind. Diese Autonomie der Kantone im Bereich des Datenschutzes ergibt sich aus der Organisationsautonomie der Kantone, die ein grundlegendes Prinzip des schweizerischen

2 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR **235.1**)

Föderalismus darstellt. Bezüglich des Datenschutzes ist jedoch die kantonale Autonomie schon mehrmals durch den Bundesgesetzgeber eingeschränkt worden (vgl. Art. 16 Abs. 2, Art. 37 Abs. 1 DSG; Art. 16 Abs. 3 BWIS[3]; Art. 16 Abs. 1, Art. 17 Abs. 1 BStatG [4]).

Diese Erweiterungen des Geltungsbereichs der eidgenössischen Datenschutzbestimmungen zeigen die Bestrebung des Bundesgesetzgebers auf, zu verhindern, dass die kantonale Autonomie den Standard des Schutzes der den Kantonen vom Bund übermittelten Daten herabsetzt. Denn der Bund ist verpflichtet, darauf zu achten, dass die von ihm bearbeiteten Personendaten nicht an Dritte weitergegeben werden, die nicht die gleichen Schutzstandards einhalten. Der Grad des Schutzes eines Informatiksystems und der Schutz der darin enthaltenen Daten wird durch das schwächste Glied der Kette bestimmt. Zur Zeit ist der Stand des Datenschutzes je nach Kanton unterschiedlich; so haben nur 17 Kantone und Halbkantone ein Datenschutzgesetz erlassen und nicht alle haben bisher ein Kontrollorgan geschaffen, wie Artikel 37 Absatz 2 DSG es vorschreibt. Der breite Online-Zugang von kantonalen und kommunalen Behörden zu gewissen Datenbanken des Bundes könnte sich in Zukunft als problematisch erweisen, wenn eine Harmonisierung des Schutzstandards zwischen dem Bund und den Kantonen unterbleibt. In dieser Hinsicht wäre es sinnvoll, auf Bundesebene den Standard für den Zugang, die Benutzung, den Schutz und die Kontrolle von Datenbanken des Bundes festzulegen. Es empfiehlt sich jedoch zu prüfen, ob dieser Standard der Form von direkt anwendbaren Bundesnormen bedarf oder ob er mittels Normen, die nur dann anwendbar sind, wenn eine entsprechende kantonale Regelung fehlt, erreicht werden kann. Aus diesen Gründen beantragt der Bundesrat, auch in diesem Punkt die Motion in ein Postulat umzuwandeln.

Der Bundesrat beantragt, die Motion in ein Postulat umzuwandeln.»

3 Empfehlungen der GPK-S

Zu den 12 Empfehlungen der GPK-S nimmt der Bundesrat wie folgt Stellung:

3.1 Prüfung der Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung

Die zunehmende Ausrüstung mit EDV-Mitteln führt dazu, dass immer mehr Online-Verbindungen eingerichtet werden, die zahlreichen Bundes- und Kantonsbehörden den direkten Zugriff auf verschiedene Datenbanken ermöglichen. Der Bundesrat prüft diese Verbindungen auf ihre Zweckmässigkeit (Notwendigkeit), Verhältnismässigkeit und Zweckbindung, bevor sie in formellen gesetzlichen Bestimmungen geregelt werden.

Beim Bearbeiten von Personendaten gelten die folgenden Grundsätze des DSG (Art. 4 Abs. 2 und 3): Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Zudem dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen er-

3 Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR **120**)
4 Bundesstatistikgesetz vom 9. Oktober 1992 (BStatG, SR **431.01**)

sichtlich oder gesetzlich vorgesehen ist. Beim Erlass von Spezialbestimmungen im Bereich des Datenschutzes hat der Bundesrat bisher immer auf die strikte Einhaltung der genannten Grundsätze geachtet. Bereits heute begründet der Bundesrat in seinen Botschaften die Zweckmässigkeit von vorgeschlagenen Massnahmen und gibt dem Parlament damit die Möglichkeit, diese zu beurteilen. In diesem Sinne stellt die vorliegende Empfehlung eine Aufforderung zur Überprüfung von Online-Verbindungen im Sinne der Grundsätze des DSG dar.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu.

3.2 Kontrolle durch die zuständige Instanz

Der Bundesrat sorgt für eine angemessenere Kontrolle der Online-Verbindungen durch den Eidgenössischen Datenschutzbeauftragten. Die Kontrolle stellt sicher, dass nur notwendige Verbindungen eingerichtet werden, d. h. wenn ein Bedürfnis nachgewiesen wurde, der Zweck bekannt ist, die Kosten geplant sind und die Risiken eines Missbrauchs oder einer Persönlichkeitsverletzung in einer Risikobeurteilung geprüft wurden.

Artikel 31 DSG sieht unter anderem vor, dass der Eidgenössische Datenschutzbeauftragte (EDSB) zu Vorlagen über Erlasse und Massnahmen des Bundes, die für den Datenschutz erheblich sind, Stellung nimmt. Da das Einrichten von Online-Verbindungen zweifellos datenschutzrelevant ist, wird der EDSB in jedem Fall beigezogen. In der Praxis wird der EDSB jeweils im Rahmen der Ämterkonsultation begrüsst. Wenn das betroffene Departement die Stellungnahme des EDSB nicht vollumfänglich übernehmen kann, berichtet es dem Bundesrat über die abweichende Stellungnahme des EDSB.

Die Vorlagen an den Bundesrat enthalten demnach immer Angaben zur Notwendigkeit und zum Zweck von einzurichtenden Online-Verbindungen. Das bedeutet, dass sich der EDSB, wie bereits dargelegt, dazu immer äussern kann. Die Planung der Kosten der Verbindung und die Beurteilung der Risiken eines Missbrauchs oder einer Persönlichkeitsverletzung hingegen erfolgen im Rahmen der Informatikprojektbearbeitung und sind Teil der für die Genehmigung der einzelnen Projektphasen notwendigen Unterlagen.

Der Bundesrat ist der Meinung, dass kein Anlass besteht, das geltende Verfahren anzupassen. Alle in der Empfehlung enthaltenen Elemente – Bedarfsnachweis, Zweck, Kosten, Risiken – werden im Rahmen des geltenden Verfahrens bei der Einrichtung von Onlineverbindungen geprüft. Der EDSB hat Zugang zu all diesen Informationen. Der EDSB legt sein Kontroll-Programm selber fest und entscheidet je nach Prüfungsgegenstand über die Zweckmässigkeit von systematischen oder stichprobenweisen Kontrollen. Er trägt dabei den Grundsätzen der Verhältnismässigkeit Rechnung.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu und wird dafür besorgt sein, dass der EDSB über alle notwendigen Informationen verfügt, um ihm eine angemessenere Kontrolle der Online-Verbindungen zu ermöglichen.

3.3 Transparenz über Online-Verbindungen in den bundesrätlichen Botschaften

Der Bundesrat sorgt dafür, dass in seinen Botschaften alle erforderlichen Angaben zu den geplanten Zugriffen enthalten sind, und zwar sowohl hinsichtlich ihrer Notwendigkeit, Zweckbindung, Verhältnismässigkeit und ihres Umfangs sowie in Bezug auf die Behörden, denen sie gewährt werden sollen.

Diese Forderung ist nicht neu. Das auf den 1. Oktober 1997 in Kraft gesetzte RVOG[5] sieht in seinem Artikel 3 Absatz 3 denn auch vor, dass das Handeln von Bundesrat und Bundesverwaltung den Grundsätzen der Zweckmässigkeit und der Wirtschaftlichkeit zu folgen habe. Im Übrigen hat der Bundesrat dieses Jahr aus Gründen der Zweckmässigkeit und Wirtschaftlichkeit seines Handelns entschieden, dass bei jedem Gesetzes- und jedem Verordnungsprojekt der Informatikverträglichkeit besondere Beachtung zu schenken sei. Dies bedeutet, dass neben den bestehenden oder geplanten Anwendungen, die Datenkommunikation und damit auch die Online-Verbindungen zu berücksichtigen sind. Der Bundesrat hat sich bereits bisher bemüht, der vorliegenden Empfehlung nachzuleben und hat in seinen Botschaften jeweils alle erforderlichen Angaben über die geplanten Zugriffe gemacht – sowohl hinsichtlich ihrer Notwendigkeit, ihrer Zweckbindung und ihrer Verhältnismässigkeit, als auch in Bezug auf den Umfang des Zugriffs und auf die Behörden, denen der Zugriff gewährt werden soll. Artikel 19 Absatz 3 DSG schreibt ausserdem vor, dass besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur durch ein Abrufverfahren zugänglich gemacht werden dürfen, wenn ein formelles Gesetz dies ausdrücklich vorsieht. Der Bundesrat wird in Zukunft der Transparenz bei Botschaften zu geplanten Online-Verbindungen verstärkt Beachtung schenken.

Im Gegensatz zur qualitativen Information des Parlamentes über geplante Online-Verbindungen ist die Vermittlung von quantitativen Informationen ungleich schwieriger, wenn nicht vorgängig im Rahmen eines Pilotbetriebes die tatsächlichen Bedürfnisse der potentiellen Nutzenden ermittelt werden können.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu.

3.4 Zusammenarbeit und Koordination zwischen Bund und Kantonen

Der Bundesrat sorgt für eine bessere Koordination und Zusammenarbeit zwischen Bund und Kantonen. Auf diese Weise sollen kantonale Entscheidungsverfahren eingeführt werden, die, wenn nicht identisch, so doch vereinheitlicht oder vergleichbar sind und gleichwohl den Föderalismus und die geltenden kantonalen Regelungen berücksichtigen.

Dem Bundesrat ist das in der Empfehlung angesprochene Problem bekannt. Wir bewegen uns hier allerdings in einem Spannungsfeld: Soll der Bund verbindliche und vielleicht übermässige Regelungen erlassen, oder soll er aus föderalistischer Rücksichtnahme die Wahl des am besten geeigneten Verfahrens den Kantonen und ihrem politischen Gespür überlassen? Da Online-Verbindungen für Personendaten gemäss

5 Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG, SR **172.010**)

DSG (Art. 19 Abs. 3) nur zulässig sind, wenn sie auf Gesetzes- und Verordnungsstufe ausdrücklich vorgesehen sind, hat der Bundesgesetzgeber diese Anforderungen erfüllt indem er jedes Mal, wenn sich die Notwendigkeit einer solchen Verbindung auf Grund der Prüfung der Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung zeigt, Bestimmungen erlassen, welche den kantonalen Behörden den Zugriff auf Informationssysteme des Bundes erlauben. Sobald dies einmal geschehen ist, haben sich die mit der Einrichtung der Online-Verbindung beauftragten Bundesbehörden bis anhin nicht mehr darum gekümmert, auf welche Art und Weise, mit welchem Verfahren und nach welchen Kriterien die kantonalen Behörden ihrerseits Zugriffsgesuche geprüft und entschieden haben.

Den Kantonen ein einheitliches Entscheidverfahren aufzuzwingen wäre schwierig. Der Bundesrat erachtet es jedoch als notwendig, dass die kantonalen politischen Behörden entscheiden, die Datenbearbeitungsregeln festlegen, z.B. das Bearbeitungsreglement für eine Applikation, und dem Umfang der durch den Bund auszuführenden Kontrollen zustimmen. Diese Frage sollte der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) unterbreitet werden. Das EJPD wird die vorliegende Empfehlung der KKJPD zur Traktandierung an einer ihrer nächsten Versammlungen zukommen lassen.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung im Sinne der vorstehenden Erklärungen zu.

3.5 Grundsätze für alle Online-Bewilligungsverfahren

Der Bundesrat legt Grundsätze für alle Bewilligungsverfahren bei der Einrichtung von Online-Verbindungen im Polizeibereich fest. Insbesondere regelt er die Aufgaben, Kompetenzen und Verantwortungen im Verfahren.

Der Bundesrat erachtet es als notwendig, Grundsätze für die Behandlung von Gesuchen festzulegen, wenn im Polizeibereich Online-Verbindungen eingerichtet werden. Er ist hingegen der Meinung, dass der Erlass solcher Grundsätze Sache des Departementes sei und nicht in eine Ergänzung der VDSG[6] gehöre.

Diese Empfehlung ist in engem Zusammenhang mit der vorhergehenden zu behandeln.

Stellungnahme des Bundesrates:

Der Bundesrat beauftragt das EJPD, einen Entwurf im Sinne der Empfehlung auszuarbeiten und diesen der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) vorzulegen.

3.6 Überprüfung der Delegationsnormen

Der Bundesrat überprüft die Delegation von Bewilligungsentscheiden auf die untersten operativen Verwaltungseinheiten in allen betroffenen Bereichen. Er sorgt dafür, dass die Online-Anschlussbewilligung von einer der Wichtigkeit und Trag-

6 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR **235.11**)

weite des Bewilligungsentscheides sowie der Sensibilität der Daten adäquaten, unabhängigen Bewilligungsinstanz vorgenommen werden.

Die Bewilligung von Online-Anschlüssen geschieht in mehreren Verfahrens- und Entscheidungsschritten:

a. Der Grundsatzentscheid, bestimmten Behörden den Anschluss zu erteilen (z. B. kantonalen Polizeibehörden, welche mit der Bekämpfung des illegalen Drogenhandels beauftragt sind), wird durch den Bundesgesetzgeber auf Stufe Bundesgesetz gefällt, wenn der Anschluss den Zugriff auf besonders schützenswerte Personendaten oder auf Persönlichkeitsprofile ermöglicht. Anderenfalls erfolgt der Grundsatzentscheid auf Stufe Bundesratsverordnung.

b. Der Entscheid über den Anschluss und den Online-Zugriff eines bestimmten Kantons auf ein Informationssystem des Bundes ist Gegenstand einer zwischen den politischen Behörden des Kantons und des Bundes zu treffenden Vereinbarung (vgl. Empfehlung 3.4).

c. Der dritte Entscheidungsschritt betrifft die einer bestimmten Person zu erteilende Berechtigung, via Online-Verbindung auf ein Informationssystem des Bundes zuzugreifen, wenn diese Person einer im Gesetz oder in der Verordnung erwähnten Behörde angehört.

Die vorliegende Empfehlung betrifft die dritte Entscheidstufe, nämlich die Erteilung der Zugriffsberechtigung an die Systembenützenden. Der Bundesrat widersetzt sich der Forderung grundsätzlich nicht, dass eine adäquate und unabhängige Bewilligungsinstanz die Gesuche um Zugriffsberechtigung der Benützenden prüft. Er befürchtet allerdings, dass die Empfehlung der GPK-S auf eine Bewilligungsinstanz hinzielt, welche sich hierarchisch zu weit weg von der Benützendenebene befindet. Eine amtsexterne Person wird in der Regel weder das für die konkrete Anwendung verantwortliche Amt noch die Mitarbeitenden kennen. Um überhaupt beurteilen zu können, ob einer konkreten kantonalen Angestellten die Zugriffsberechtigung auf eine Anwendung zu erteilen sei oder nicht, wird sich eine amtsexterne Person umfassend dokumentieren lassen und ein umfangreiches Dossier prüfen müssen. Die Ernennung einer Bewilligungsinstanz auf Stufe Departement würde einerseits eine erhebliche Arbeitsmehrbelastung auslösen und andererseits keine Gewähr dafür bieten, dass mit mehr Sachkenntnis entschieden wird. Zudem wäre das Verfahren vor dieser Bewilligungsinstanz für die Prüfung von rasch zu behandelnden normalen Mutationen (wie Aufgabenänderungen, Kündigungen, längere Abwesenheiten usw.) zu schwerfällig.

Der Bundesrat ist vielmehr der Auffassung, dass die Lösung bei den für das Informationssystem zuständigen Ämtern zu suchen sei. Auch wenn der Entscheid über die Zugriffsberechtigung grundsätzlich Aufgabe des Eigentümers der Datensammlung ist, könnte die Zugriffsberechtigung von bestimmten Benützenden durch die Datenschutzberater des Amtes der durch eine andere, nicht mit der in Frage stehenden Anwendung befassten Person geprüft werden. Gemäss der mit dem Kanton zu vereinbarenden Regelung (vgl. Empfehlung 3.4) müsste diese Person zudem beauftragt werden, die Übereinstimmung der eingerichteten mit den bewilligten Anschlüssen regelmässig zu kontrollieren.

Stellungnahme des Bundesrates:

Der Bundesrat beauftragt die Departemente, für ihre Informationssysteme eine Zuständigkeitsordnung für die Bewilligung von Online-Anschlüssen zu erlassen.

3.7 Kontrolle der Einhaltung der Sicherheits-Grundsätze

Der Bundesrat schafft Kontrollmöglichkeiten (Sicherheitsinspektionen) für die Systembetreiber des Bundes. Diese sollen eine Kontrolle darüber gewährleisten, ob die Anschluss- und Sicherheits-Grundsätze durch Benutzerinnen und Benutzer aus Kantonen und Gemeinden eingehalten werden.

Zahlreiche Bestimmungen sehen bereits vor, dass für kantonale Organe, die beim Vollzug von Bundesrecht Personendaten bearbeiten, das Bundesgesetz über den Datenschutz gilt. Dies ist insbesondere dann der Fall, wenn keine kantonalen Datenschutzvorschriften bestehen (Art. 37 Abs. 1 DSG) und wenn die Daten durch kantonale Sicherheitsorgane beim Vollzug des BWIS (Art. 16 Abs. 3 BWIS) bearbeitet werden. Auch das Zentralstellengesetz[7] schreibt vor, dass die Kantone nur dann durch ein Abrufverfahren auf das Datenverarbeitungssystem der Zentralstellen direkt zugreifen können, wenn die notwendigen Schutz- und Sicherheitsmassnahmen getroffen sind (Art. 12 Abs. 1 Zentralstellengesetz). Die letztgenannte Bestimmung erteilt den Zentralstellen zumindest indirekt die Befugnis, die Schutz- und Sicherheitsmassnahmen derjenigen Kantone, welche auf die Zentralstellendaten zugreifen, zu überprüfen. Für andere Datenbearbeitungen sollte die Kontrolle über die Einhaltung der vom verantwortlichen Systembetreiber angeordneten Schutz- und Sicherheitsmassnahmen durch die kantonalen und kommunalen Benützenden nach Auffassung des Bundesrates vorerst in den jeweiligen Verordnungen über die Behandlung von Personendaten der einzelnen Anwendungen geregelt werden. Da diese Kontrollen einen beträchtlichen Arbeitsaufwand auslösen würden, muss an dieser Stelle auch darauf hingewiesen werden, dass es sich höchstens um punktuelle und nicht um systematische Kontrollen handeln könnte.

Vorgängig sollte in der KKJPD eine Grundsatzdiskussion über diese Kontrollen geführt werden. Gemäss Artikel 37 Absatz 2 DSG müssen die Kantone ein Kontrollorgan bestimmen, welches für die Einhaltung des Datenschutzes sorgt. Die Kontrolle der Informatiksicherheitsmassnahmen könnte zum Beispiel durch diese vom Kanton bestimmten Kontrollorgane im Auftrag und nach Anweisung der für das Informationssystem verantwortlichen Bundesbehörde erfolgen. Die kantonalen Kontrollorgane könnten sich, wenn nötig, durch die Beauftragten des Bundes für Informatiksicherheit begleiten lassen. Ihre Kontrollberichte wären nicht nur der kantonalen Behörde zuzustellen, sondern auch der für das System verantwortlichen Bundesbehörde. Mit einer entsprechenden Revision von Artikel 37 DSG könnten solche Kontrollverfahren auf Gesetzesstufe präziser und klarer verankert werden.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung im Grundsatz zu und beauftragt das EJPD, die notwendigen Lösungsvorschläge auszuarbeiten.

7 Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes (SR **172.213.71**)

3.8 Standards für Gesuche

Der Bundesrat legt Standards fest für die Einreichung von Gesuchen um die Bewilligung von Online-Verbindungen im Polizeibereich.

Vorerst muss betont werden, dass sich der Geltungsbereich einer solchen Empfehlung nicht auf den Polizeibereich beschränken dürfte, sondern in jedem Bereich der Verwaltung anzuwenden wäre. Tatsächlich haben bereits heute alle Systemverantwortlichen mit Online-Verbindungen ihr eigenes Verfahren definiert zur Prüfung von Zugangsgesuchen neuer Benützenden. Der Bundesrat ist bereit zu prüfen, ob in diesem Gebiet eine gewisse Harmonisierung der Verfahren möglich wäre.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu und beauftragt das EJPD, Standards für das Gesuchsverfahren um Bewilligung von Online-Verbindungen auszuarbeiten.

3.9 Überprüfung der Nutzungsintensität von Online-Verbindungen

Der Bundesrat sorgt für die regelmässige Überprüfung der Nutzungsintensität von Online-Verbindungen im Polizeibereich.

Eine Überprüfung der Nutzungsintensität von Online-Verbindungen im Polizeibereich wäre im Rahmen von regulären Kontrollen technisch durchaus machbar. Bei allen EDV-Anwendungen im Polizeibereich wird die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen gemäss den Vorschriften von Artikel 10 VDSG protokolliert. Dies bedeutet, dass das System jeden Zugriff auf eine Datenbank protokolliert und dabei die Person, das Datum, die Uhrzeit und den Wortlaut der Anfrage registriert. Aus Datenschutzgründen sind diese Journalisierungsprotokolle im Moment noch ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften obliegt, und dürfen auch nur für diesen Zweck verwendet werden (Artikel 10 Absatz 2 der VDSG). Eine Revision dieser Verordnungsbestimmung würde die Verwendung der Journalisierungsprotokolle für die von der GPK-S verlangten Zwecke möglich machen. Dies würde jedoch auch eine Kontrolle der Anzahl Recherchen durch die einzelnen Benutzenden implizieren. Der Bundesrat wird den Rat des EDSB einholen, um ein Verfahren zur Überprüfung der Nutzungsintensität von Online-Verbindungen zu bestimmen, das nicht gleichzeitg eine übermässige Überwachung der Tätigkeiten der Benutzenden zur Folge hat.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung im Sinne seiner Erklärungen zu.

3.10 Sicherheitsprüfung der Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD

Der Bundesrat führt für Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD eine Sicherheitsprüfung ein. Im Gegensatz zu den Angestellten der Bundes-

polizei unterstehen diese heute keiner Sicherheitsprüfung, obwohl sie auf besonders schützenswerte Personendaten, auf Polizei- oder Staatsschutzdaten oder auf Informationen über die Sicherheitsmassnahmen oder Informatikentwicklungen der Bundesapplikationen Zugriff haben.

Das BWIS sieht in Artikel 19 Absatz 1 Buchstabe e vor, dass Sicherheitsprüfungen für diejenigen Bedienstete des Bundes vorgesehen werden können, die regelmässig Zugang zu besonders schützenswerten Personendaten haben, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte. Gestützt auf diese Bestimmung wäre es möglich, die Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD einer Sicherheitsprüfung zu unterziehen. Gemäss Artikel 19 Absatz 2 BWIS können die Kantone für ihre Bedienstete, die unmittelbar bei Aufgaben des Bundes zur Wahrung der inneren Sicherheit mitwirken, ebenfalls eine Sicherheitsprüfung durchführen.

Am 20. Januar 1999 hat der Bundesrat gestützt auf die Artikel 19, 21 und 30 BWIS die Verordnung über die Personensicherheitsprüfung[8] beschlossen. Die Liste der Funktionen, welche einer Sicherheitsprüfung unterzogen werden müssen, hat der Bundesrat hingegen noch nicht erlassen. Im Entwurf dieser Liste, die Mitte 1999 verabschiedet werden sollte, sind auch die Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD ausdrücklich genannt. Sobald die Liste vom Bundesrat genehmigt ist, werden die in Ihrer Empfehlung verlangten Sicherheitsprüfungen vorgenommen werden.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu.

3.11 Standort des Rechenzentrums EJPD

Der Bundesrat sorgt für eine angemessenere Unterbringung des Rechenzentrums EJPD.

Die GPK-S und der Expertenbericht machen auf die Sicherheitsproblematik aufmerksam, die sich aus dem Standort des Rechenzentrums EJPD ergeben. Das Problem ist dem EJPD bekannt. Es hat denn auch bereits 1995 durch Sicherheitsexperten aufzeigen lassen, wo allfällige Sicherheitsrisiken des Standorts Zollikofen liegen. Der Bericht der Sicherheitsexperten zeigt klar auf, dass die wünschbare physische Sicherheit am Standort in Zollikofen praktisch nicht realisiert werden kann. Dieses Ergebnis der Sicherheitsüberprüfung des Standortes Zollikofen wurde den Organen für die Gebäudesicherheit sowie dem Verfasser des Expertenberichtes GPK-S mitgeteilt.

Im Rahmen des Projektes NOVE-IT[9] hat der Bundesrat dem Vorschlag zugestimmt, die Computer des Rechenzentrums EJPD in den Computerräumen des VBS zu installieren, wobei die Anlagen der beiden Departemente vollständig getrennt bleiben. Die Anlagen des EJPD werden mit eigenem Personal und unter ausschliesslicher Verantwortung des EJPD betrieben. Der Umzugstermin steht noch nicht fest; der Transfer wird in Etappen und unter Berücksichtigung des EDV-Erneuerungsprogramms des EJPD erfolgen. Das Rechenzentrum des EJPD wird erst dann an ei-

8 Verordnung vom 20. Januar 1999 über die Personensicherheitsprüfungen (Personensicherheitsprüfungsverordnung, PSPV, AS **1999** ...)
9 Reorganisation der Informatik in der Bundesverwaltung

nem geeigneteren Standort untergebracht werden, wenn das EDV-Erneuerungsprogramm des EJPD den Umzug ohne Gefährdung des Betriebes bestehender Systeme zulässt und keine übermässigen Kosten verursacht.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu.

3.12 Entscheid betreffend die Zusammenlegung von KOMBV-KTV und EJPD-WAN

Der Bundesrat entscheidet so rasch wie möglich, ob eine Zusammenlegung von KOMBV-KTV und EJPD-WAN zu erfolgen hat.

Das Benutzernetz KOMBV-KTV[10] ist das TCP/IP-Netzwerk[11], welches alle kantonalen Netzwerke untereinander verbindet und Zugänge auf Applikationen in den Kantonen sowie der allgemeinen Bundesverwaltung ermöglicht (any-to-any Beziehung). Offene Verkehrsbeziehungen innerhalb der Kantone (auch zu den Hochschulen) von jedem zu jedem sowie zum Teil offene Verkehrsbeziehungen zu externen Netzen sind möglich.

Das EJPD-WAN[12] (ATM- Backbone) stellt die sternförmige Verkehrsbeziehung des RZ EJPD mit 26 Partnern dar. Eine Verkehrsbeziehung besteht ausschliesslich zwischen den entsprechenden Behörden und dem Rechenzentrum EJPD, nicht aber zwischen den Partnern untereinander oder zu externen Netzen wie Internet. Das EJPD-WAN kann somit als eine Mehrzahl individueller, geschlossener TCP/IP-basierender Benutzernetze betrachtet werden. Den Justiz- und Polizeibehörden in den Kantonen wird der selektive Zugriff auf Datenbankanwendungen des EJPD ermöglicht.

Die seit 1996 vom BFI im Aufbau stehende Kommunikationsinfrastruktur KOMBV3 (ATM-Netz der Swisscom) wird vom EJPD-WAN als Weitverkehrs-Trägernetz verwendet. Abhängig von Wirtschaftlichkeit und Verfügbarkeit wird eine stufenweise Migration auf KOMBV3 umgesetzt (physische Zusammenlegung). Dabei werden (basierend auf dem Trägernetz KOMBV3) die polizei- und staatsschutzrelevanten Informationen aus betriebs- und sicherheitstechnischen Gründen innerhalb des EJPD-WAN über geschlossene, logisch getrennte IP-Subnetze verbreitet. Dieses Konzept der logisch getrennten Netze, wie es das EJPD anwendet, wird auch von grossen Organisationen verwendet, die von den Aufgaben her mit dem EJPD vergleichbar sind. Das BKA (Bundeskriminalamt) betreibt für die Polizeidaten ein länderübergreifendes logisch getrenntes Netz. Grossbritannien betreibt das PNN (Police National Network) und das FBI in den USA verfügt über CJIS WAN (Criminal Justice Information System Wide Area Network) sowie NLETS (National Law Enforcement Telecommunications System).

Das EJPD hat ein Gutachten im Zusammenhang mit der Zusammenlegung der Netze WAN-EJPD und KOMBV-KTV erstellen lassen. Der Bundesrat wird die Ergebnisse dieser Studie, wonach die Bildung von logisch getrennten Subnetzen aus Sicht der Informatiksicherheit von Vorteil sei, noch zu prüfen haben. Erst nach dieser Prüfung

10 Kommunikation der Bundesverwaltung – Kantonverbund
11 TCP/IP, transmission control protocol/Internet protocol)
12 WAN, Wide-Area-Network

wird er sich definitiv zur Zweckmässigkeit einer Zusammenlegung der Netze KOMBV-KTV und EJPD-WAN äussern.

Stellungnahme des Bundesrates:

Der Bundesrat stimmt der Empfehlung zu.

4 Expertenbericht vom 30. Juli 1998

Der Bundesrat verzichtet darauf, sich zu jeder Empfehlung des Expertenberichtes zu äussern, da der grösste Teil derselben zutreffend und begründet ist. Die wichtigsten Empfehlungen sind ausserdem von der GPK-S übernommen worden. Einige Punkte verdienen jedoch, speziell hervorgehoben zu werden.

4.1 Grundsätze für Online-Verbindungen

Die im Expertenbericht genannten Grundsätze für Online-Verbindungen stellen eine gute Zusammenfassung der verschiedenen Anforderungen dar, die vor dem Einrichten solcher Verbindungen zu berücksichtigen sind. Die im Expertenbericht gemachten Zusammenstellungen können als nützliche Check-Listen dienen.

4.2 Anschluss des Rechenzentrums an die von ihm betriebenen Anwendungen

Der Experte weist darauf hin, dass zwischen dem Rechenzentrum EJPD (RZ EJPD) und einer einzelnen Anwendung zur Gewährleistung von Betrieb, Unterhalt und Wartung 26 Anschlüsse eingerichtet worden sind. Er ist der Auffassung, dass für diese Anschlüsse die gesetzliche Grundlage fehle und dass ihre Anzahl übertrieben sei. Der Experte empfiehlt dem EJPD deshalb, eine genügende gesetzliche Grundlage für die Anschlüsse der Mitarbeiterinnen und Mitarbeiter des RZ EJPD an diese Anwendung zu schaffen.

In diesem Einzelfall ist die Anzahl der mit dem Betrieb der Anwendung begründeten Anschlüsse tatsächlich hoch und war Gegenstand einer internen Kontrolle. Der Bundesrat stellt fest, dass diejenigen Anschlüsse, welche von Systembetreibenden zur Gewährleistung von Betrieb und Unterhalt einer Anwendung benützt werden, nicht in allen Verordnungen über die Bearbeitung von Personendaten analog behandelt wurden. Obwohl tatsächlich Online-Anschlüsse dieser Art praktisch für jede Anwendung existieren, sind sie in einigen Erlassen ausdrücklich vorgesehen (z. B. in den Verordnungen DOSIS, ISOK und FAMP), während der Bundesrat in anderen Fällen davon ausgegangen ist, dass die für die einzelne Anwendung geltende Rechtsgrundlage diese Art Anschlüsse implizit auch umfasse. Tatsächlich sind solche Anschlüsse dem Betrieb von Informationssystemen inhärent und werden nur im Auftrag des für die Anwendung verantwortlichen Organs zum Untersuchen von Anwendungsfehlern verwendet.

Der Bundesrat wird den EDSB beiziehen, um das Problem der Anschlüsse, welche dem Rechenzentrum zu Unterhaltszwecken gewährt werden, auf zweckmässige Art und Weise zu lösen.