Beilage 1

Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens

Expertenbericht über die Praxis der Bundesverwaltung

zuhanden der Sektion „Behörden“
der Geschäftsprüfungskommission des Ständerates

mit Nachtrag 1
Auswertungen und Zusammenfassung
des verwaltungsinternen Vernehmlassungsverfahrens

Dokument	C:\Eigene Dateien\ONLINE\Expertenbericht.doc
Version:	4.0 Schlussdokument
Datum:	30/07/1998
Ersetzt Dokument vom:	30/06/1998
Autor:	© lic.iur. Lukas Fässler, Rechtsanwalt, Hirschmattstrasse 36, 6002 Luzern
Letzte Änderung von:	30.7.1998
Autorisiert:	Sektion Behörden der GPK-S; PVK; betroffene Bundesämter sowie GS EJPD und GS FD; lic.iur. Lukas Fässler, Luzern
Freigabe am:	1.8.1998

Inhaltsverzeichnis

1 EXPERTENAUFTRAG

11 Untersuchungsfelder

Die Parlamentarische Verwaltungskontrollstelle (PVK) führt im Auftrag der Geschäftsprüfungskommission des Ständerates (GPK-S) eine Evaluation über die **„Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens“** durch. Der vorliegende Expertenbericht befasst sich gemäss Auftrag[1] mit den Fragestellungen gemäss Block 2 . Dabei stehen folgende Untersuchungsfelder und Einzelfragen im Vordergrund:

- Ist-Situation
  a) Darstellung des IST-Zustandes bezüglich bestehender Anschlüsse an die ausgewählten Polizei-Informationssysteme.

- Entwicklungsperspektiven
  a) Zukünftige Entwicklungsperspektiven und Planungsgrundlagen bezüglich Online-Anschlüsse an Polizei-Informationssysteme.

- Verfahren
  a) Untersuchung der genauen Bedingungen, Verfahren und Zuständigkeiten, unter denen die Online-Verbindungen geplant oder eingerichtet werden.
  b) Nach welchen Verfahren und wie erfolgt in der Praxis die Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens, wenn die Anschlüsse bereits (im Voraus) bei der Ausarbeitung eines neuen polizeilichen Informationssystems vorgesehen sind?
  c) Nach welchen Verfahren und wie erfolgt in der Praxis die Bereitstellung von Online-Verbindungen im Bereich des Polizeiwesens, wenn solche nachträglich eingerichtet werden?

- Rechtsgrundlagen
  a) Welche Rechtsgrundlagen werden erarbeitet, um die Online-Anschlüsse, die einen Zugriff auf die Informatiksysteme der Polizei ermöglichen, rechtlich abzustützen?
  b) Wie wird die Frage der Ausarbeitung der erforderlichen Rechtsgrundlagen geprüft?

- Pilotprojekte
  a) Wie und unter welchen Bedingungen wird bei den immer häufigeren „Pilotprojekten“ verfahren?
  b) Welche besonderen Rechtsgrundlagen werden für diese Pilotprojekte ausgearbeitet?

- Vernehmlassung/Rechtliches Gehör
  a) Welche Organe werden im Rahmen der Bereitstellung von Online-Anschlüssen angehört?

- Kontrolle
  a) Welche Kontrollmassnahmen werden getroffen?

[1] *Expertenvertrag vom 21.10.1997 mit Pflichtenheft gleichen Datums, Ziffer 22 ff*

- Kosten
  a) Wie werden bei einem System, auf das die Kantone Zugriff haben, die Kosten zwischen Bund und Kantonen verteilt?
  b) Wer übernimmt konkret die Kosten einer Online-Verbindung zwischen Bund und Kantonen?

- Datenschutz und Datensicherheit
  a) Welche Sicherheitsmassnahmen sind in der Praxis vorgesehen bzw. werden getroffen?
  b) Welche Garantien werden von den Kantonen zur Sicherstellung der Rechtmässigkeit und des Datenschutzes verlangt?

- Archivierung
  a) Wie wird bei der Archivierung der Daten dieser Informatiksysteme verfahren?

12 Fragestellungen

In den obgenannten Untersuchungsfeldern sind folgende Detailfragen zu klären. Der dargestellte Raster bildet Ausgangslage und Leitlinie für die Einzelgespräche mit den bezeichneten Kontaktpersonen.

Untersuchungsfeld	Fragestellungen
Ist-Situation	• Verifizierung der chronologischen Auflistung (Online-Raster) mit Klärung allfälliger Fragen (Begriffe, Abkürzungen etc.). • Gibt es Veränderungen der Ist-Situation per Befragungstag gegenüber den Angaben in der chronologischen Auflistung.
Entwicklungsperspektiven	• Was ist in den nächsten 2 Jahren (1998 und 1999) hinsichtlich neuer Online-Anschlüsse geplant. • Welche Stellen (Neubenutzer) sind involviert. • Welche Stellen (Dateneigentümer) sind verantwortlich. • Wer führt das entsprechende Projekt. • In welchem Planungsstadium befinden sich die einzelnen Ausbauschritte. • Gibt es dazu Unterlagen (Vorstudie, Konzept, Detailkonzept, Vorgehenplan, Projektorganisation, Projekthandbuch).

Verfahren **a)** Für bereits **<u>im voraus</u>** vorgesehene Online-Verbindungen	• Wie ist das Verfahren für einen Drittanschluss. • Wer ist zuständig für was. • Wo sind das Verfahren, Aufgaben, Kompetenzen und Verantwortung geregelt. • Gibt es eine Bewilligungsbehörde. • Wie ist das Projektmanagement geregelt. • Wie ist das Projekt-Controlling geregelt. • Wie ist die Datenschutz- und Datensicherheitsprüfung geregelt.
b) für **<u>nachträglich</u>** sich ergebende Online-Verbindungsbedürfnisse	• Gibt es konkrete Beispiele nachträglicher (auch zeitlich beschränkter) Online-Anschlüsse im Untersuchungsbereich. • Wie ist das Verfahren für einen Drittanschluss. • Wer ist zuständig für was. • Wo sind das Verfahren, Aufgaben, Kompetenzen und Verantwortung geregelt. • Gibt es eine Bewilligungsbehörde. • Wie ist das Projektmanagement geregelt. • Wie ist das Projekt-Controlling geregelt. • Wie ist die Datenschutz- und Datensicherheitsprüfung geregelt. • Wie ist bei zeitlich beschränkten Online-Anschlüssen das Verfahren für den Verbindungs-Abbau geregelt. • Welche Dokumentationen gibt es zu nachträglichem Online-Verbindungsaufbau in den konkreten Fällen.
Rechtsgrundlagen	• Auf welche konkreten Rechtsgrundlagen können sich die Online-Anschlüsse abstützen: a) bei im voraus geplanten Online-Anschlüssen b) bei nachträglich sich ergebenden Online-Verbindungsbedürfnissen. • Wer nimmt bei der jeweiligen gesetzlichen Delegation der Verantwortung für Online-Anschlüsse auf die zuständige Verwaltungseinheit die Ueberprüfung der geltenden Grundsätze vor. • In welchem Verfahren findet diese Ueberprüfung statt. • Wie werden die Ergebnisse der Ueberprüfung dokumentiert.

Pilotprojekte	• Welche konkreten Online-Verbindungen sind im Untersuchungsbereich mittels Pilotprojekten zustandegekommen. • Welche Abweichungen zu den Verfahrens- und Vorgehensgrundlagen im ordentlichen Projektmanagement ergeben sich. • Wie werden diese Abweichungen konkret behandelt. • Gibt es zusätzliche Kontrollinstanzen und Kontrollmassnahmen innerhalb eines Pilotprojektes. • Auf welche konkreten Rechtsgrundlagen stützt man im konkreten Pilotprojekt den Aufbau und die Einrichtung von Online-Anschlussverbindungen.
Vernehmlassung Rechtliches Gehör	• Welche Organe innerhalb des Amtes, des Departementes und der ganzen Verwaltung werden zu einem konkreten Online-Projekt angehört. • Gibt es dazu gesetzliche oder weisungsbasierende Grundlagen. • Sind solche Stellungnahmen dokumentiert. • Wer sorgt für die Beachtung und Umsetzung der vorgetragenen Beachtungspunkte der antwortenden Stellen. • Wie wird bei Meinungsdifferenzen vorgegangen.
Kontrolle	• Welche Kontrollmassnahmen werden bezüglich Einhaltung der gesetzlichen Anforderungen sowie der vereinbarten oder auferlegten Beachtungspunkte im Projektmanagement getroffen. • Welche Kontrollmassnahmen werden bezüglich Einhaltung der gesetzlichen Anforderungen sowie der vereinbarten oder auferlegten Beachtungspunkte im laufenden Betrieb (produktive Nutzung in der Betriebs- und Unterhaltsphase) getroffen.
Kosten	• Wie werden Investitions- und Betriebskosten für Online-Verbindungen innerhalb und ausserhalb der Bundesverwaltung budgetiert und ausgewiesen. • Werden die Kosten von Online-Verbindungen innerhalb der Bundesverwaltung auf die Benützer aufgeteilt. • Werden die Kosten für die Dienstleistungserbringung durch das Service-Zentrum oder den Datenherr bundesverwaltungsintern weiterverrechnet. • Werden die Kosten für die Bereitstellung (Investitionskosten) und den Betrieb (Betriebskosten) von Online-Verbindungen zu Stellen ausserhalb der Bundesverwaltung budgetiert und verrechnet. • Auf welche Rechtsgrundlagen stützen sich die Kostenfragen (Verrechnung, Leistungserbringung intern,

	extern).
Datenschutz Datensicherheit	• Wie und durch wen werden Datenschutz- und Datensicherheitskonzepte in der projektmässigen Bereitstellung von Online-Verbindungen erarbeitet. • Gibt es konkrete Konzepte zu den laufenden Verbindungen. • Wie und durch wen werden Datenschutz- und Datensicherheitskonzepte in der pilotmässigen Bereitstellung von Online-Verbindungen erarbeitet. • Werden diese Konzepte Dritten zur Vernehmlassung, Begutachtung, allenfalls Genehmigung unterbreitet. • Können konkrete Beispiele solcher Begutachtungen und Genehmigungen im Untersuchungsbereich gezeigt werden. • Wie werden diese Fragen im konkreten bei Online-Anschlüssen mit Dritten (Kantone) bearbeitet. • Können dazu konkrete Beispiele gezeigt werden. • Welche Garantien werden von den Kantonen zur Sicherstellung der Rechtmässigkeit und des Datenschutzes verlangt. • Werden mit den Kantonen entsprechende Datenbank-Nutzungsverträge geschlossen, in welchen die Verantwortlichkeit, der Zugriffsschutz, die Berechtigungen sowie die Haftungsfragen geregelt werden. Können solche Verträge konkret gezeigt werden.
Archivierung	• Wie werden die Daten der entsprechenden Informationssysteme konkret archiviert. • Welche Bestimmungen sind dafür zu beachten. • In wessen Verantwortung liegt die Initialisierung, Durchführung und Uebergabe der Daten zur Archivierung.

Nicht alle hier aufgelisteten Fragen sind anlässlich der persönlichen Befragungen der Verantwortlichen der untersuchten Systeme behandelt worden. Einerseits waren sie aufgrund der konkreten IST-Situation nicht relevant (kein Pilotprojekt laufend, keine bundesexternen Anschlüsse vorhanden), anderseits konnten sie durch entsprechende Nachdokumentation seitens der zuständigen Organe beantwortet werden.

Der vorliegende Fragenraster wurde den Verantwortlichen der zuständigen Bundesstellen vorab als Vorbereitungsunterlage für das persönliche Gespräch mit dem Experten zugestellt.

13 Vorgehen

Die Erarbeitung des vorliegenden Expertenberichts wurde mit der PVK gemeinsam geplant und auf die Gesamtprojektplanung abgestimmt. Zunächst wurden von den ausgewählten Organen die Unterlagen über die Entwicklung der zu untersuchenden Informatiksysteme eingeholt (Initialisierung, Voranalyse, Konzept, Realisierung, Einführung, Betrieb und Unterhalt sowie neuere Entwicklungen). Zudem wurden die Erlasse, die zur rechtlichen Abstützung dieser Systeme und

derer Zugriffe geschaffen wurden, einverlangt. Gleichzeitig erstellten die betroffenen Organe zuhanden der PVK und des Experten anhand eines Rasters eine aktuelle Auflistung der Online-Verbindungen. Darin werden die Verbindungspartner, Anschlussdaten, Benutzerzahlen, Rechtsgrund, benutztes Kommunikationsnetz, Kommunikationsprotokoll, technische Rechte sowie Sicherheitsmassnahmen aufgelistet. Dieser chronologische Raster stellt eine erstmalige Gesamtsicht auf die untersuchten Polizei-Informationssysteme aus dem Blickwinkel Online-Verbindungen dar. Nach der Analyse der eingeforderten Dokumente wurden mit den Vertretern der verschiedenen Organe gemäss nachfolgender Uebersicht Befragungen durchgeführt.

Wann	Wer	Untersuchungsbereich	Befragte
2.2.1998	**Bundesamt für Polizeiwesen**	RIPOL & DOSIS	• Lic.iur. Adrian Lobsiger Direktionsadjunkt • Lic.iur. Arnold Bolliger Abteilungschef der Abteilung Besondere Dienste
3.2.1998	**Bundesamt für Ausländerfragen**	ZAR	• Dr. iur. Christoph Müller Direktionsadjunkt • Lic.oec. Bernard Hayoz StV Sektionschef Sektion Zentrales Ausländerregister/Statistik Benutzerprojektleiter BFA • Lic.iur. Claudio Hayoz Datenschutzberater BFA • Rudolf Müller EDV-Entwickler BFA
	Rechenzentrum EJPD	Bereich Ressourcen und Sicherheit	• Heinz Többen, Bereichsleiter Ressourcen & Sicherheit RZ EJPD
11.2.1998	**Bundespolizei**	ISIS ISIS-Plus	• Lic.iur. Christoph Herrli Chef Vorauswertung der Abteilung Information und Auswertung

Nach der Zustellung weiterer Dokumentationen und Unterlagen durch die benannten Ansprechpartner bei den zuständigen Bundesorganen analysierte der Experte die gesamten Unterlagen je Untersuchungsbereich, wertete die Befragungsergebnisse aus und verarbeitete diese in den vorliegenden Expertenbericht.

Erste Ergebnisse des Expertenberichtes wurden der Sektion Behörden der Geschäftsprüfungskommission des Ständerates am 6. Mai 1998 vorgestellt. Anschliessend verarbeitete der Experte weitere einverlangte Ergänzungsunterlagen in den Bericht. Am 1. und 2. Juli 1998 orientierte der Experte mündlich das Bundesamt für Polizeiwesen, die Bundespolizei, das Bundesamt für Ausländerfragen sowie das Rechenzentrum EJPD über die wesentlichen

Berichtsergebnisse. Im Anschluss an diese Erläuterung wurde das interne Vernehmlassungsverfahren eröffnet. Die Eingabefrist lief bis 23. Juli 1998. Die Ergebnisse des Vernehmlassungsverfahrens sind in einem separaten Dokument „Nachtrag 1 Auswertungen und Zusammenfassung des verwaltungsinternen Vernehmlassungs-verfahrens (Version 1.0)“ vom 30.7.1998 festgehalten.

2 RECHTSGRUNDLAGEN UND GRUNDSÄTZE FÜR ONLINE-VERBINDUNGEN

21 Einleitung

Das nachfolgende Kapitel bezweckt in einer kurzen Uebersicht die Darstellung der Grundlagen (Gesetze, Verordnungen, Strategien, Weisungen, Richtlinien, Normen und Standards) und Grundsätze für die Vorbereitung, Realisierung und den Betrieb von Informatiksystemen, welche gegenüber Dritten geöffnet sind oder werden sollen (bestehende oder geplante Online-Anschlüsse).

*Wir verstehen unter „**Online-Verbindung“** jede in der Regel in Echtzeit stattfindende Datenverarbeitung durch Systembenutzer über eine funktionsfähige Kommunikationsinfrastruktur auf einem Informatiksystem oder auf einer Fachanwendung des bereitgestellten Informatiksystems.* Die vorliegende Betrachtung betrifft ausschliesslich die Informationssysteme RIPOL, DOSIS, ISIS (-Plus) und ZAR des Bundes, welche innerhalb und/oder ausserhalb der Bundesverwaltung Dritten für Online-Bearbeitungen zur Verfügung gestellt werden.

22 Gesetzliche Grundlagen im Polizeiwesen

Alle untersuchten Informationssysteme (RIPOL, DOSIS, ISIS (-Plus) und ZAR) sind Organisationseinheiten des Bundes zuzuordnen, welche den Sicherheitsweisungen des Bundesamtes für Informatik (BfI) unterliegen. Deshalb gelten für diese Anwendungen die Grundlagen und Vorgaben an die Informatik-Sicherheit in der Bundesverwaltung. Als übergeordnete gesetzliche Grundlagen sind deshalb insbesondere, jedoch nicht abschliessend, folgende Erlasse massgebend:

a) Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).
b) Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11).
c) Verordnung über das Bundesamt für Informatik und über die Koordination der Informatik in der Bundesverwaltung vom 11.12.1989 (VINFBV; SR 172.010.58).
d) Verordnung über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung vom 10.6.1991(VINFS; SR 172.010.59).
e) Verordnung über die Klassifizierung und Behandlung von Informationen im zivilen Verwaltungsbereich vom 10. Dezember 1990 (SR 172.015).

Aus diesen gesetzlichen Grundlagen lassen sich folgende **Grundsätze für die Planung, Realisierung und den Betrieb von Online-Verbindungen im Polizeibereich** ableiten:

1. Bundesorgane und mithin auch die kantonalen Behörden (im Sinne von Art. 24 Abs. 1 und 4 DSG) dürfen Personendaten nur bei Vorhandensein einer entsprechenden Rechtsgrundlage bearbeiten (Art. 17 Abs. 1 DSG). Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, wenn ein formelles Gesetz es ausdrücklich vorsieht (Art. 17 Abs. 2 DSG).

2. Personendaten dürfen durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein formelles Gesetz es ausdrücklich vorsieht (Art. 19 Abs. 3 DSG).

Grundsatz 1:
Rechtsgrundlage für die (Online-)Bearbeitung von Personendaten.

Grundsatz 2:
Formelles Gesetz für die (Online-)Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen.

3. Soweit kantonale Behörden Bundesaufgaben in den Bereichen Bekämpfung des Terrorismus, des gewalttätigen Extremismus, des organisierten Verbrechens, des verbotenen Nachrichtendienstes sowie zur Gewährleistung der militärischen Sicherheit erfüllen, unterstehen sie dem Datenschutzrecht des Bundes (Art. 24 Abs. 1 und 4 DSG).

Grundsatz 3:
Ausdehnung der eidgenössischen Datenschutzgrundsätze auf Kantonsbehörden bei Erfüllung von Bundesaufgaben.

4. Bevor ein Bundesorgan eine Online-Verbindung einrichten darf, muss es prüfen, ob diese Verbindung überhaupt nötig ist und ob sie mit den Grundsätzen der Verhältnismässigkeit und Zweckmässigkeit vereinbar ist. Dieser Grundsatz leitet sich aus Art. 4 Abs. 2 und 3 DSG ab.

Grundsatz 4:
Realisierung einer Online-Verbindung nur, wenn diese notwendig, verhältnismässig und zweckmässig ist.

Grundsatz 5:
Überprüfung dieser Grundsätze (4) *vor* Bereitstellung einer Online-Verbindung.

5. Sowohl für im voraus feststehende wie auch nachträglich geplante Online-Verbindungen muss durch die Anwendungsverantwortlichen in Zusammenarbeit mit den zuständigen Organen eine Risikobeurteilung vorgenommen werden. Diese müssen sicherstellen, dass insbesondere auch der Bereich der Kommunikation ausreichend geschützt ist. Dazu sind entsprechende Sicherheitsmassnahmen zu treffen (Art. 1 Abs. 1 lit. d, Art. 3 und 4 VINFS; SR 172.010.59).

Grundsatz 6:
Risikobeurteilung vor einem Online-Anschluss vornehmen.

6. Die Bundesorgane haben alle angemessenen und geeigneten technischen und organisatorischen Datenschutz- und Datensicherheitsmassnahmen zu treffen (Art. 8, 9 und 20 Abs. 1 VDSG). Das verantwortliche Bundesorgan muss sowohl bei der Planung, der Realisierung sowie beim Betrieb von Informatiksystemen und –anwendungen sicherstellen, dass diese Systeme vor äusseren Einwirkungen und unbefugtem Zugriff geschützt sind (Art. 1 Abs. 1, 2 und 4 VINFS; SR 172.010.59).

Abbildung: Grundsatzschema zu Art. 3 und 4 der Vo über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung VINFS.

Grundsatz 7:
Angemessene und geeignete technische und/oder organisatorische Schutzmassnahmen gegen äussere Einwirkungen und unbefugten Zugriff ergreifen.

7. Die Sicherheitsmassnahmen sind regelmässig auf Aktualität zu prüfen (Art. 6 Abs. 3 VINFS; SR 172.010.59) und die Planungen von Systemen sind dem Datenschutzbeauftragten (Art. 11 Abs. 2 DSG) und dem Bundesamt für Informatik (BfI) rechtzeitig zu melden (Art. 7 Abs. 1 VINFS; SR 172.010.59). Alle neuen Informatikprojekte, wesentliche Aenderungen, Ergänzungen und Neukonzeptionen von bestehenden Anwendungen sind dem BfI mit einem Antrag gemäss HERMES zu melden (Technische Weisung Nr. 3; Art. 2).

Als wesentlich gilt, wenn
- bestehende Rechtsgrundlagen angepasst werden müssen,
- der personelle Aufwand 2 Mitarbeiterjahre übersteigt,
- der ausgabenwirksame Aufwand Fr. 200'000.— übersteigt.

Grundsatz 8:
Planung, Aenderungen, Ergänzungen und Neukonzeption von Informatiksystemen an EDSB und BfI melden.

Grundsatz 9:
Sicherheitsmassnahmen regelmässig auf Aktualität prüfen und an die geltenden technischen Weisungen des BfI anpassen.

8. Das Bundesamt für Informatik (Art. 3 Abs. 1 Buchstabe c VINFBV; SR 172.010.58) erlässt im Einvernehmen mit den anderen zuständigen Organen (Art. 5 Abs. 2 VINFS; SR 172.010.59) die notwendigen Weisungen und Richtlinien (Art. 3 Abs. 2 Buchstabe l VINFBV; SR 172.010.58) und überwacht deren Vollzug (Art. 8 VINFS; SR 172.010.59). Technische Weisungen und allgemeinverbindliche Beschlüsse der Informatikkonferenz Bund (IKB) sind für alle Verwaltungseinheiten der Bundesverwaltung (Art. 58 VwVG; mit Ausnahme der PTT-Betriebe und der Schweizerischen Bundesbahnen) verbindlich.

Im Zuge dieser Bestimmungen sind insbesondere nachfolgende Weisungen zu beachten:

Technische Weisungen

- TW 03 Meldung der Informatikprojekte an das BFI vom 22.8.1990.
- TW 08 Handbuch für LAN-Projektleiter vom 16.10.1996.
- TW 09 SNA /SNI Namenskonventionen – 92, vom 16.9.1992.
- TW 11 Domain Name System (DNS) vom 13.11.1996.
- TW 16 Projektführung und Systementwicklung in Informatikprojekten vom 19.4.1995 und Handbuch HERMES Ausgabe 1995.
- TW 17 Adressierung NSAP (Network Service Access Point) vom 18.10.1995.
- TW 18 World Wide Web (WWW) in der Bundesverwaltung vom 15.1.1997.

Weisungen Informatiksicherheit

- WS S01 Handhabung der Benutzeridentifikationen und der Passwörter vom 18.8.1993 und Merkblatt zur Verwendung von Passwörtern in der Bundesverwaltung vom Dezember 1993.
- WS S02 Grundschutz von Informatiksystemen und –anwendungen vom 19.4.1995.
- Handbuch Nr. 1 zur WS S02 Verfahren für die Checklistenbearbeitung und Gesamtmassnahmenkatalog vom 1.10.1996.
- WS S03 Umsetzung der Network Security Policy (NSP) vom 25.6.1997.

9. Die jeweilige zuständige Bundesstelle hat die Einzelheiten der Bearbeitung und damit auch der Online-Anbindung in einem **Bearbeitungsreglement** resp. in **Weisungen über die organisatorischen und technischen Massnahmen** zu regeln.

- für RIPOL: Art. 4 Abs. 1 RIPOL-Vo,
- für DOSIS: Art. 9 Abs. 4 DOSIS-Vo,
- für ZAR: Art. 7 Abs. 4 ZAR-Vo,
- für ISIS: Art. 5 Abs. 3 und 20 Abs. 2 ISIS-Vo.

Grundsatz 10:
Bearbeitungsreglemente erlassen und in Weisungen die organisatorischen und technischen Massnahmen regeln.

23 Zusammenfassung

Zusammenfassend lassen sich folgende für das Polizeiwesen des Bundes massgebliche Grundsätze für Online-Verbindungen festlegen:

Grundsätze für Online-Verbindungen

1. **Online-Bearbeitung von Personendaten nur mit gesetzlicher Grundlage.**
2. **Online-Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen nur mit formeller gesetzlicher Grundlage.**
3. **Ausdehnung der eidg. Datenschutzgrundsätze auf Kantons- und Kommunalbehörden bei Erfüllung von Bundesaufgaben.**
4. **Realisierung von Online-Verbindungen nur, wenn diese notwendig, verhältnismässig und zweckmässig sind.**
5. **Ueberprüfung von Notwendigkeit, Verhältnismässigkeit und Zweckmässigkeit vor Bereitstellung einer Online-Verbindung.**
6. **Risikobeurteilung vor Online-Anschluss.**
7. **Ergreifen angemessener und geeigneter technischer und/oder organisatorischer Schutzmassnahmen vor äusseren Einwirkungen und unbefugtem Zugriff vor Online-Anschluss.**
8. **Meldepflicht bezüglich Planung, Aenderung, Ergänzung und Neukonzeption von Informationssystemen an EDSB und Bfl.**
9. **Regelmässige Aktualisierung der technischen und organisatorischen Sicherheitsmassnahmen und Anpassung an die geltenden technischen Weisungen des Bfl.**
10. **Regelung der Einzelheiten der Online-Bearbeitung in Bearbeitungsreglementen und Weisungen.**

3 UNTERSUCHUNGSERGEBNISSE

31 RIPOL

311 Gesetzliche Grundlagen und Grundsätze

Folgende gesetzliche Grundlagen sind im Anwendungsbereich des automatisierten Personen- und Sachfahndungssystem (RIPOL) massgebend:

1. Schweizerisches Strafgesetzbuch (SR 311.0; insbesondere Art. 351bis StGB),
2. Verordnung über das automatisierte Fahndungssystem vom 19.6.1995 (RIPOL-Verordnung; SR 172.213.61),
3. Richtlinien des BAP betreffend Einführung von RIPOL 2 vom 25.6.1990,
4. Benutzer- und Wartungsreglement „automatisiertes Fahndungssystem des Bundesamtes für Polizeiwesen“ vom Mai 1987.

Daraus lassen sich folgende Grundsätze für die Bewilligung von Online-Anschlüssen durch die zuständige Bundesbehörde ableiten:

Das Bundesamt für Polizeiwesen (BAP) trägt die Verantwortung für das RIPOL. Es koordiniert seine Tätigkeiten mit den am RIPOL beteiligten Behörden von Bund und Kantonen. Das BAP erteilt dem jeweiligen Benutzer von Bund und Kantonen die notwendigen Bewilligungen für den Gebrauch des Systems und überwacht die Einhaltung dieser Verordnung und die gestützt darauf erlassenen Weisungen (Art. 4 Abs. 1 RIPOL-Vo). Die Berechtigung zur Bearbeitung von im RIPOL abgespeicherten Daten ist im separaten Anhang zur RIPOL-Verordnung bis auf die Ebene der Datenfeldnamen über Berechtigungsstufen (A = Ansicht; B = Abgleich ob verzeichnet oder nicht; C = Ansicht nur bei verzeichneten Ausländern; M = Mutation) geregelt (Art. 6 Abs. 1 RIPOL-Vo). Hinsichtlich Datensicherheit gilt, dass die Datenübermittlung an die schweizerischen Vertretungen mit konsularischen Aufgaben und an die ausländischen Interpol-Stellen chiffriert zu erfolgen hat (Art. 17 Abs. 1 RIPOL-Vo). Die gemäss Datenschutzgesetz angemessenen organisatorischen und technischen Massnahmen müssen von den beteiligten Behörden für ihren Bereich getroffen werden. Der Zugriff auf RIPOL wird mit individuellen Benutzerprofilen und Passwörtern gesichert. Die mit direkten Anschlüssen an das RIPOL ausgestatteten Behörden regeln die Zugangsberechtigung zu den Datenstationen und sichern die Arbeitsräume wirksam gegen den Zutritt unbefugter Personen (Art. 17 Abs. 2, 3 und 4 RIPOL-Vo). Das Rechenzentrum EJPD (RZ EJPD) sorgt dafür, dass die Daten und Programme des RIPOL nach allfälliger Zerstörung, Entwendung oder Verlust wiederhergestellt werden können (Art. 17 Abs. 5 RIPOL-Vo).

Gemäss Benutzer- und Wartungsreglement des BAP vom Mai 1987 obliegt der Projektgruppe RIPOL (Zusammensetzung vgl. Ziffer 6.1. des Reglementes) die Prüfung der Ausbauwünsche bzw. Projekterweiterungen. Das BAP (interne Zuständigkeit ist im Reglement nicht bezeichnet) beschliesst über Anschlussbegehren der Bundes-Projektbenutzer. Der Dienst für Informatik (DFI) des Eidg. Justiz- und Polizeidepartements ist für die Realisierung der budgetierten Anschlussbegehren zuständig (Ziffer 713 des Reglementes). Im Verhältnis zu den angeschlossenen Kantonen gilt, dass Projekterweiterungen und grössere Programmänderungen sowie Anpassungen seitens des BAP der Fachgruppe „Informatik“ der Schweizerischen Polizeitechnischen Kommission mitgeteilt werden. Anschlussbegehren und Erhöhungen der Abfragestationen sind durch das jeweilige Polizeikommando direkt an das BAP (Ziffer 712 Reglement: Dienst für Polizeiwesen; *wohl nach der Reorganisation nicht mehr zutreffende Organisationsbezeichnung*) schriftlich einzureichen. Der jeweilige Entscheid liegt beim BAP, das den Zeitpunkt der Realisierung festlegt (Ziffer 81 des Reglements).

312 IST-Situation Online-Verbindungen

Benutzerzahl
Gemäss chronologischer Auflistung über die Online-Verbindungen RIPOL vom 26.11.1997, deren Aktualität anlässlich der Befragung vom 2. Februar 1998 bestätigt wurde, sind seit 1984 bis heute insgesamt

13234 Benutzer

an RIPOL angeschlossen worden.

Benutzerkategorien
Alle angeschlossenen Benutzer legitimieren sich über Art. 351bis StGB zur Nutzung von RIPOL. Die Konkretisierung bezüglich inhaltlicher Nutzung des Informationssystems durch diese Benutzerkategorien erfolgte durch den Bundesrat in der RIPOL-Verordnung (Art. 3 RIPOL-Vo).

Netzinfrastruktur und Sicherheitsmassnahmen
Alle angeschlossenen Verbindungspartner kommunizieren über bundeseigene Netzinfrastrukturen (LIS/EJPD; WAN EJPD; KOMBV3 oder KOMBV4). Die Kommunikation findet über TCP/IP, über X.25 oder SNA statt (standardisierte Kommunikationsprotokolle). Als Sicherheitsmassnahmen werden zum Teil software-basierende End-to-End Chiffrierungen, Link-Chiffrierungen (auf dem EJPD-eigenen Basisnetz) oder Firewall-Abschottungen eingesetzt. Die Daten sollen dadurch in keinem Falle offen und ungeschützt über die Kommunikationsnetze gehen.

313 Anschlussverfahren

Im Zusammenhang mit der Frage nach den Aufgaben, Kompetenzen und Verantwortungen im Bereich der Online-Anbindung von bundesverwaltungsinternen oder bundesverwaltungsexternen Benutzern fällt vorerst die Delegationsnorm in Art. 351bis Abs. 4 Buchstabe b StGB auf. Sodann hat der Gesetzgeber zur Frage der Online-Anbindung konkrete Regelungen erlassen, indem er in einer abschliessenden Aufzählung jene Behörden (von Bund und Kantonen) bezeichnet, die RIPOL nutzen dürfen (Art. 351bis Abs. 2 und 3 StGB). Er umschreibt die Nutzungsberechtigung mit den beiden Begriffen:

- Über RIPOL Ausschreibungen ***verbreiten*** (Art. 351bis Abs. 2 StGB)
- Personendaten aus RIPOL ***bekanntgeben*** (Art. 351bis Abs. 3 StGB)

In Absatz 4 von Art. 351bis StGB beauftragt der Gesetzgeber den Bundesrat, *die Behörden zu bestimmen, welche Personendaten direkt ins RIPOL eingeben, solche direkt abfragen oder denen Personendaten im Einzelfall bekanntgegeben werden können.* Diese Aufgabe hat der Bundesrat in der RIPOL-Verordnung insofern erfüllt, als er die beteiligten Behörden (Art. 3 RIPOL-Vo) und die Verantwortung für das Informationssystem (Art. 4 RIPOL-Vo) geregelt hat. In Art. 3 RIPOL-Vo bezeichnet der Bundesrat die Behörden, welche

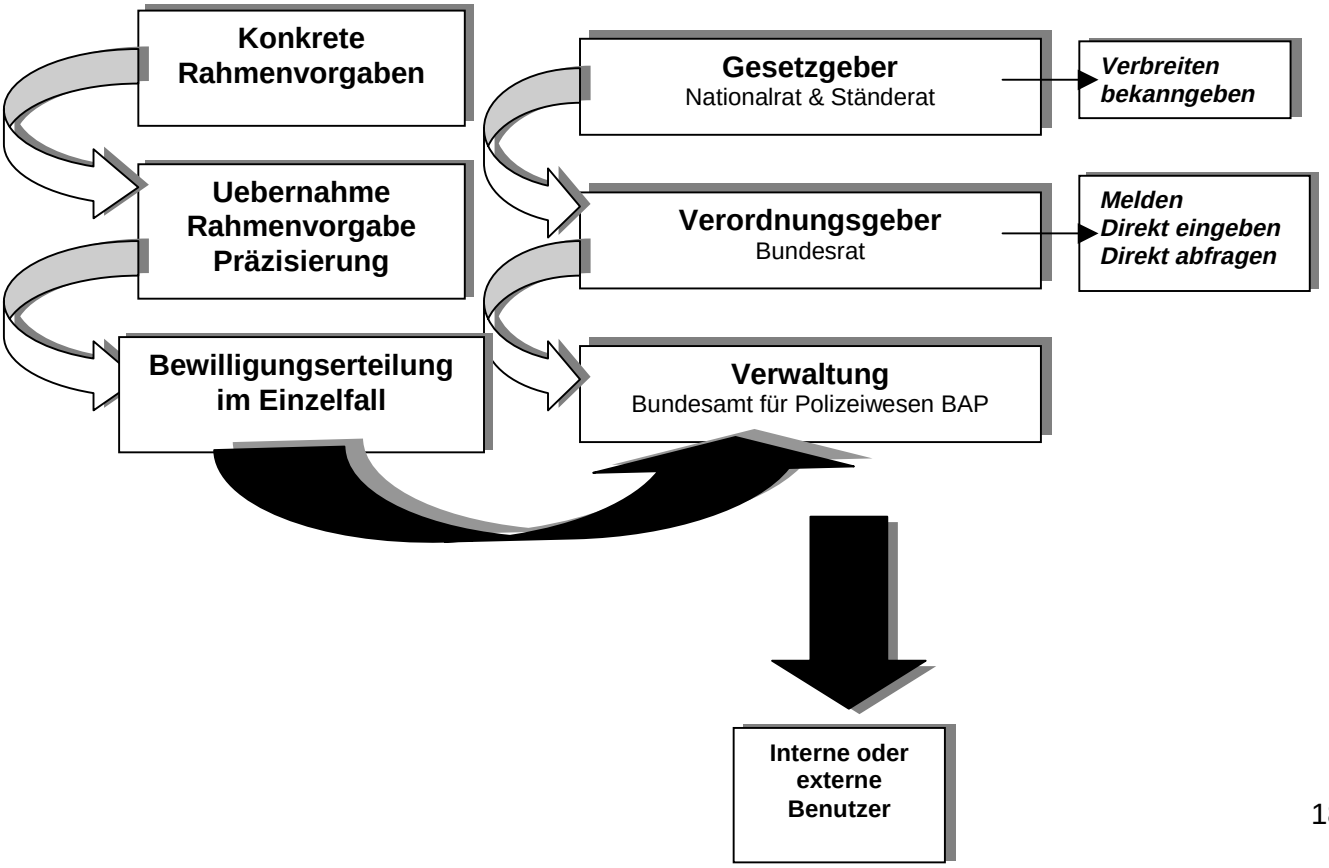
- dem BAP Ausschreibungen ***melden*** können (Art. 3 Abs. 1 RIPOL-Vo)
- Ausschreibungen ***direkt eingeben*** können (Art. 3 Abs. 2 RIPOL-Vo)

- Daten ***direkt (online) abfragen*** können (Art. 3 Abs. 3 RIPOL-Vo).

Vorerst kann festgehalten werden, dass der Gesetzgeber selber unter dem Titel „automatisiertes Fahndungssystem“ eine Anzahl Benutzerbehörden festgelegt hat (Art. 351bis Abs. 2 und 3 StGB). Er umschreibt deren Nutzungskompetenz mit „Ausschreibungen verbreiten“ und „Personendaten bekanntgeben“. Trotzdem ermächtigt er den Bundesrat zusätzlich, die Behörden zu bestimmen, welche Personendaten direkt ins RIPOL eingeben, solche direkt abfragen oder denen Personendaten im Einzelfall bekanntgegeben werden können. Damit wird nicht mehr klar ersichtlich, in welchem Verhältnis die Begriffe „verbreiten“ und „bekanntgeben“ (in Art. 351bis Abs. 2 und 3 StGB) zur Delegationsnorm („Der Bundesrat bestimmt...“; Art. 351bis Abs. 4 StGB) und dem dort verwendeten Begriff „direkt abfragen“ steht. Sind die Benutzerkategorien in Absatz 2 und 3 hinsichtlich Nutzung von RIPOL abschliessend definiert oder erhält der Bundesrat darüber hinausgehende Kompetenz, zusätzliche Behörden im Bereich von Online-Anbindungen zu definieren? Die vom Gesetzgeber gewählten Begriffe sind denn auch nicht geeignet, im Rahmen der heute technisch möglichen Kommunikationslösungen eine klare Abgrenzung zu schaffen. Zudem eröffnet die in Art. 351bis Abs. 3 Buchstabe h StGB umschriebene Generalklausel „weitere Justiz- und Verwaltungsstellen“ einen sehr weiten Anschlusspielraum.

In Art. 4 RIPOL-Vo überträgt der Bundesart seinerseits die Verantwortung für das RIPOL an das BAP. Das BAP erhält die Aufgabe, Kompetenz und Verantwortung, den Benutzern (beteiligte Behörden im Sinne von Art. 3 RIPOL-Vo) die notwendigen Bewilligungen für den Gebrauch des Systems zu erteilen, die Einhaltung der Verordnung zu überwachen und gestützt darauf Weisungen zu erlassen (Art. 4 RIPOL-Vo). In Art. 6 präzisiert der Bundesrat den Datenzugriff. Der Benutzer hat nur auf diejenigen Datenbanken Zugriff, die er zur Erfüllung seiner gesetzlichen Aufgaben benötigt (Art. 3 Abs. 3 RIPOL-Vo). Die Berechtigung zur Bearbeitung von im RIPOL abgespeicherten Daten wird im Anhang detailliert geregelt.

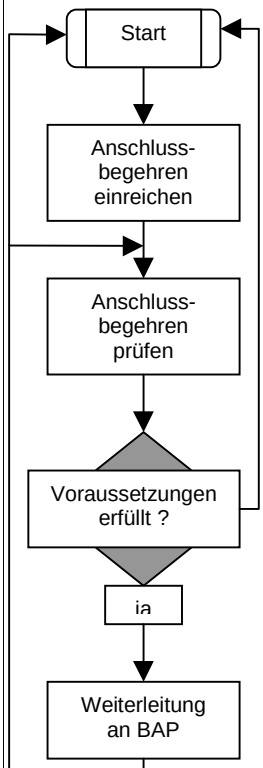
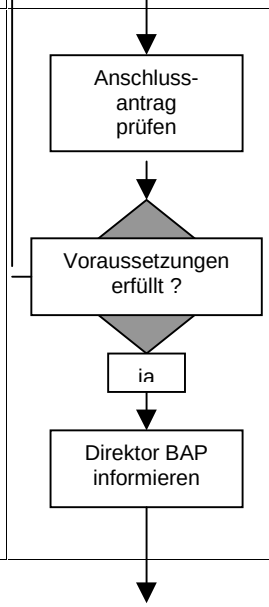
Delegationskaskade bezüglich Online-Bewilligungen



Anlässlich der Herbsttagung 1994 der Konferenz der kantonalen Polizeikommandanten der Schweiz wurde im Einvernehmen mit dem BAP das Vorgehen bei Anschlussgesuchen von Gemeindepolizeien festgelegt (Beilage 2 der Nachlieferung von Unterlagen durch das BAP zuhanden des Experten). Die in Briefform zusammengefassten Schritte können in der nachfolgenden Prozessbeschreibung übersichtlich dargestellt werden. Die dort aufgeführten Schritte haben mit Ausnahme der Anschlussgesuche von Schweizerischen Vertretungen im Ausland und der Interpolstellen für alle Bewilligungsverfahren Gültigkeit. Die Darstellung entspricht den Anforderungen an ein Qualitätsmanagement-System nach der internationalen Norm ISO 9000 und würde sich grundsätzlich für alle wichtigen Abläufe in der Bundesverwaltung eignen. Dabei wird davon ausgegangen, dass ein Geschäft im weitesten Sinne an eine Verwaltungsstelle herangetragen wird (Input), dort in Einzelschritten und unter Zuhilfenahme von Checklisten und Arbeitsanweisungen von zuständigen und verantwortlichen Mitarbeitern (Verantwortung) bearbeitet wird (Ablauf; Beschreibung und Hilfsmittel). Das Ergebnis (Output) muss dabei den definierten Qualitätsstandards (Erfolgskenngrössen des Prozesses) der zuständigen Behörde resp. des Gesetzgebers entsprechen.

Für das Online-Bewilligungsverfahren im Bereich RIPOL lässt sich die Geschäftsprozess-beschreibung wie folgt darstellen:

Bundesamt für Polizeiwesen	Bewilligungsverfahren für Online-Anbindung RIPOL	Prozess 0xx

Input	Ablauf	Beschreibung und Hilfsmittel	Verant-wortung	Output
Interne Anfrage, interne Bedarfsab-klärung, interner Rationalisie-rungsantrag etc.		Jede Polizeibehörde (nicht der Kantonspolizei unterstellte Gemeinde- bzw. Stadtpolizeien), die Anschluss an RIPOL wünscht, stellt ein schriftliches Gesuch mit kurzer Begründung an die zuständige Kantonspolizei (Beilage 4a der Nachlieferung von Unterlagen durch das BAP zuhanden des Experten). Diese prüft, ob die rechtlichen kantonalen Voraussetzungen für einen Online-Anschluss gegeben sind. Sie fällt eine Entscheidung und leitet das Gesuch an das Bundesamt für Polizeiwesen (BAP) weiter **Formular 4.5**	Gemeinde-polizei Kantonspolizei Kantonspolizei Kantonspolizei	Anschluss-begehren Gesuchsprüfung Antrag Kantonspolizei
Antrag Kantonspolizei		Das BAP prüft, ob die rechtlichen Voraussetzungen gegeben sind. Diese Prüfung erfolgt durch den Chef der Abteilung Besondere Dienste (BESODI) zusammen mit dem Datenschutz-beauftragten des Amtes in rechtlicher, qualitativer und quantitativer Hinsicht sowie seitens des RZ EJPD betreffend technischer Sicherheit. Bei einem negativen Entscheid antwortet das BAP (konkrete der Chef BESODI) direkt dem Gesuchsteller (mit Kopie zur Kenntnis an die zuständige Kantonspolizei). **Formular 4.1** Der Direktor BAP wird über den Bewilligungsentscheid in Kenntnis gesetzt **Formular 4.2**	BAP Chef BESODI DSB des BAP Chef BESODI Chef BESODI	Bewilligungs-entscheid für Online-Anschluss Negativent-scheid an den Gesuchsteller Kopie an KAPO Mitteilung an Direktor BAP

	Zustellung Bewilligungs-entscheid	Bei einem positiven Entscheid schickt das BAP das Begehren an die zuständige Kantonspolizei und bedient das RZ EJPD mit einer Entscheidskopie **Formular 4.3 und Formular 4.4**	Chef BESODI	Bewilligungs-entscheid Entscheidkopie an RZ EJPD
Anschluss-gesuch an RZ EJPD	Technisches Anschlussgesuch stellen	Das kantonale Polizeikommando stellt ein Anschlussgesuch beim RZ EJPD **Formular 3**	Polizei-kommando	
Technische und örtliche Kommunika-tionsinfrastruk-turen der neuen Benutzer	Technische Betriebsbereitschaft erstellen	Das RZ EJPD sorgt im direkten Kontakt mit den zuständigen kantonalen Stellen (Polizei, Informatik) für die technische Betriebsbereitschaft (Netzwerk, Knoten, Anschlüsse etc.). **Standards, Normen & Richtlinien RZ EJPD**	RZ EJPD Bereich Telematik, Planung & Engineering	Technischer Anschluss gemäss Standards
	Technische Betriebsbereitschaft melden	Das RZ EJPD meldet dem BAP die technische Betriebsbereitschaft des Anschlusses.	RZ EJPD	Meldung Betriebs-bereitschaft an BAP
Zugriffs-parameter	Benutzeranforde-rungen festlegen	Das BAP regelt die Anschlussmodalitäten. Die notwendigen Benutzerprofile und Zugriffsanforderungen werden direkt mit der zuständigen kantonalen oder kommunalen Stelle vereinbart.	Chef BESODI	Benutzerprofile Zugriffsanforde-rungen
	Benutzerverant-wortlichen bestimmen lassen	Grössere Verwaltungseinheiten (z.B: Kantonspolizeikorps) geben ihre Profile selber ein. In diesem Falle verlangt das BAP, dass von der nachsuchenden Verwaltungseinheit gegenüber dem verantwortlichen Kommandanten ein zuständiger Benutzerverantwortlicher bezeichnet wird.	Benutzer-verantwortlicher	
	Benutzerparametri-sierung eingeben	Die neue „REGI-Kennung“ muss mit dem RZ EJPD konkret abgestimmt werden. Anschliessend sind die Benutzerparametrisierungen im System einzugeben. **CL00001**	Chef BESODI oder Benutzerverant wortlicher	Benutzerpara-metrisierung
	Zur produktiven Nutzung freigeben	RIPOL wird dem neuen Benutzer zur produktiven Nutzung zur Verfügung gestellt	Chef BESODI oder Benutzerver-antwortlicher	
	Ende			
Version 1.0	**Was** Prozesserstellung	**Wann erstellt** 6.3.1998	**Von wem** FI	**Geprüft** 20.4.1998 Bo	**Freigabe** 30.4.1998 Wi

Abbildung: mögliche Prozessbeschreibung aufgrund der bekannten Ablaufaktivitäten für die produktive Inbetriebnahme eines Online-Anschlusses von RIPOL.

Checkliste CL00001
Benutzerparametrisierung

„l'OFP peut ensuite „saisir" le nouvel administrateur xx. Il s'agit ici d'attribuer à l'actuel administrateur de la police cantonal yy un nouveau numéro d'utilisateur en tant qu'administrateur zz. Pour ce fair il faut changer la REGI-Kennung dans le masque 1111 et enregistrer avec F2, muter le profil 802 dans le masque 2211 et enfin attribuer les masques 1111, 1112, 1113, 1121, 2211 et 2212 dans le „Sportoto" 9000.)

etc. .....

314 Betrieb und Unterhalt

RIPOL ist seit 1984 operativ im Einsatz. Sukzessive sind in den letzten 14 Jahren verschiedene bundesverwaltungsinterne und bundesverwaltungsexterne Benutzerstellen angeschlossen worden. Die Anforderungen an RIPOL sind laufend gestiegen und von den Benutzern eingebracht worden. Für den Weiterausbau und die Wartung des Projektes RIPOL hat das BAP ein Benutzer- und Wartungsreglement (Stand Mai 1987) erlassen, welches die Modalitäten festlegt. Für den Ausbau und Betrieb ist die Sektion automatisiertes Fahndungssystem des BAP zuständig. Einer Projektgruppe obliegt die Prüfung der Ausbauwünsche resp. Projekterweiterungen. Der Projektvorsitz liegt beim Chef Dienst für Polizeiwesen. Der Einbezug der kantonalen/kommunalen Anforderungen und Projekterweiterungen erfolgt durch das BAP über die Fachgruppe Informatik der Schweizerischen Polizeitechnischen Kommission sowie der jeweiligen Benutzerarbeitsgruppe. Das Reglement hat sich in den Grundsätzen bewährt.

Autonomiebestrebungen allenthalben lassen beim Bund und in den Kantonen parallele Anwendungen entstehen. Insbesondere die Kantone tendieren dazu, einheitliche, integrierte Systeme auf interkantonaler Ebene einzurichten, ohne sich dabei an die Datenschutzstandards des Bundes gebunden zu fühlen. Mangelnde Strategie, juristischer Formalismus, Erwartungen der Fahndungsorgane und Datenschutzanforderungen erschweren eine Koordination (vgl. nachfolgend Ziffer 324). Das kantonsweise von Privaten erstellte System ABI, welches von ehemaligen Mitarbeitern des RZ EJPD (!!) angeboten wird und offenbar mit deutlich lascherer Beachtung der Datenschutzgesetzgebung operiert, könnte bald die Bundeslösungen, insbesondere im Bereich RIPOL, DOSIS konkurrenzieren. Das System ABI, dessen Anwendung auf die Bereiche organisierte Kriminalitäts- (OK) und Betäubungsmittelbekämpfung bereits geplant wird, erfreut sich zunehmender Beliebtheit unter den kantonalen Polizeikorps. Es wird demnächst in 19 Kantonen operativ eingesetzt (vgl. „Online-Datenaustausch zwischen Bund und Kantonen, Bericht der Verwaltungskontrolle des Bundesrates (VKB) an den Bundesrat vom 22.12.1997 mit Nachträgen vom 9.2.1998, nachfolgend VKB-Bericht genannt, Seite 24-25; Schreiben BAP an PVK vom 5.12.1997, Seite 7).

315 Kostenbeteiligungen

Die Kommunikationsinfrastruktur (Netzbereitstellung) finanziert gemäss Art. 22 RIPOL-Vo der Bund. Er bezahlt die Erschliessung und den Betrieb der Datenleitungen zu einem zentralen Anschlusspunkt (Hauptverteiler; Knotenpunkt) am Kantonshauptort. Ebenso übernimmt der Bund die gesamten Projekt-, Ausbau- und Erweiterungskosten (Software-Entwicklung) sowie die Kosten des zentralen Rechenzentrumsbetriebs (Systembetrieb). Eine Leistungsverrechnung des Bundes für seine Dienstleistungen im Bereich Informatik und Telekommunikation findet nicht statt. Eine

solche wäre wohl derzeit auch bezüglich Akzeptanz und Durchsetzung einheitlicher Informationssysteme im Polizeibereich eher kontraproduktiv (Bericht VKB, a.a.O., Seite 30-31).

Die Kantone übernehmen die Installations- und Betriebskosten für die Feinverteilung innerhalb der Kantone sowie die Anschaffungs- und Betriebskosten der angeschlossenen kantonalen Arbeitsplätze.

316 Kantone und andere bundesverwaltungsexterne Anschlüsse

RIPOL ist hinsichtlich kantonaler und kommunaler Nutzung eine sehr grosse und weit verbreitete Applikation. Aus der chronologischen Auflistung ergibt sich, dass 95.4 % oder 12628 bundesverwaltungsexterne Benutzer der Kantone und der kommunalen Behörden angeschlossen sind. 24 Benutzeranschlüsse sind für schweizerische Vertretung im Ausland und 30 Anschlüsse für Interpolstellen eingerichtet. Mit diesen zusammen ergibt sich ein bundesverwaltungsinterner Benutzeranteil von lediglich 4.6% oder insgesamt 606 Benutzern.

RIPOL-Nutzungsanteile

Bundesverwaltungs-**EXTERN**	**95.4% =**	**12‘628 Benutzer**
Bundesverwaltungs-**INTERN**	**4.6% =**	**606 Benutzer**

Gemäss Ausführungen des Chefs der Abteilung Besondere Dienste (BESODI) anlässlich der Expertenbefragung am 2.2.1998 werden schweizerische Vertretungen im Ausland (Konsulate) ebenfalls an RIPOL angeschlossen. Die Legitimation ergibt sich aus Art. 3 Abs. 3 Buchstabe b der RIPOL-Vo, wonach die Schweizerischen Vertretungen im Ausland mit konsularischen Aufgaben nach Ausschreibungen von Personen sowie von ungeklärten Straftaten, einschliesslich der Sachfahndung direkt Online-Abfragen vornehmen können. Diese Anschlussmöglichkeit ist mit der Verordnungs-Revision im Herbst 1995 geschaffen worden. Datenübermittlungen an die schweizerischen Vertretungen mit konsularischen Aufgaben und an die ausländischen Interpol-Stellen haben chiffriert zu erfolgen (Art. 17 Abs. 1 RIPOL-Vo). Das Anschlussverfahren ist auf informeller Ebene gelöst worden, indem das Generalsekretariat EJPD mit dem Generalsekretariat EDA die entsprechenden Abmachungen getroffen haben soll. Die zuständigen Verwaltungsdirektionen sind danach mit dem Vollzug betraut worden. Im Bereich BAP ist gemäss Aussagen wiederum der Chef BESODI für die Anschlussbewilligung zuständig.

317 Entwicklungsperspektiven

Am 15. März 1995 ist das Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes (ZentG, SR 172.213.71) in Kraft getreten. Damit wurde die rechtliche Grundlage geschaffen, welche es dem Bund erlaubt, die Kantone und ausländische Polizeikräfte im Kampf gegen die international tätige Schwerstkriminalität zu unterstützen. Dem Bund hat das Gesetz eine zentrale Rolle beim Erkennen und Bekämpfen des organisierten Verbrechens zuerkannt. Das ZentG regelt auch den internationalen und interkantonalen polizeilichen Informationsaustausch. Gestützt auf Art. 11 Abs. 1, 12 Abs. 2, 13 Abs. 1 und 15 des ZentG haben die kriminalpolizeilichen Zentralstellen des Bundes das Recht, zur Erfüllung ihrer Aufgaben ein Datenverarbeitungssystem zur Bekämpfung des organisierten Verbrechens (ISOK) durch die Zentralstelle für die Bekämpfung des organisierten Verbrechens zu betreiben und zu benutzen. RIPOL als automatisiertes Personen- und Sachfahndungssystem ist von dieser Entwicklung nicht betroffen. RIPOL ist

deshalb weder von der Ausarbeitung der neuen Verordnungen über kriminalpolizeiliche Zentralstellen im Bundesamt für Polizeiwesen (ZentV) und über das Datenverarbeitungssystem zur Bekämpfung des organisierten Verbrechens (ISOK-Verordnung) noch von der Revision der Verordnung über das Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels vom 26. Juni 1996 (DOSIS-Verordnung) tangiert.

Aufgrund der mündlichen Erläuterungen anlässlich der Befragung des BAP am 2.2.1998 sind folgende Entwicklungen bei den Online-Anschlüssen des RIPOL geplant:

a) Anschlusserweiterungen bei den kantonalen Strassenverkehrsämtern für Abfragen in der Fahrzeugfahndung,
b) Anschluss weiterer Schweizerischer Vertretungen im Ausland (Los Angeles, London, Lagos) für ihre konsularischen Aufgaben (vgl. Protokoll Projektausschuss RIPOL vom 9.7.1997, Ziffer 3 Seite 2; Ausschreibung von Personen, ungeklärte Straftaten, Sachfahndung),
c) Anschlusserweiterung bei den ausländischen Interpol-Stellen für Abfragen nach abhandengekommenen Fahrzeugen und Gegenständen,
d) Anschlusserweiterung für das kantonale Lagezentrum Ostschweiz (konkordatsbasierender Kantonszusammenschluss für kriminalpolizeiliche Aufgaben).
e) Anschlusserweiterungen bei den Städte- und Gemeindepolizeien.

32 DOSIS

321 Gesetzliche Grundlagen und Grundsätze

Folgende gesetzlichen Grundlagen sind im Anwendungsbereich des Datenverarbeitungssystems zur Bekämpfung des illegalen Drogenhandels (DOSIS) massgebend:

1. Betäubungsmittelgesetz (BetmG; SR 812.121; insbesondere Art. 30 BetmG),
2. Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG; SR 172.213.71; insbesondere Art. 11 Abs. 1, 12 Abs. 2, 13 Abs. 1 und 15 ZentG),
3. Verordnung über das Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels (DOSIS-Vo; SR 812.121.7) mit Datenkatalog (Anhang 1 zur DOSIS-Vo),
4. Verordnung über kriminalpolizeiliche Zentralstellen im Bundesamt für Polizeiwesen (ZentV; SR 172.213.711),
5. Weisung des Eidgenössischen Justiz- und Polizeidepartementes über das Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels (Weisung-DOSIS-Departement; nach Aufnahme des DOSIS-Vollbetriebs aufgehoben und ersetzt durch DOSIS-Bearbeitungsreglement),
6. Weisungen über die Kontrolle des Datenverarbeitungssystems zur Bekämpfung des illegalen Drogenhandels (Weisung-DOSIS-Kontrolle; nach Aufnahme des DOSIS-Vollbetriebs aufgehoben und ersetzt durch DOSIS-Bearbeitungsreglement),
7. DOSIS-Bearbeitungsreglement des BAP vom 20.12.1996. Dieses Bearbeitungsreglement ist auf den 1. April 1998 durch dasjenige vom 20. März 1998 ersetzt worden).

Daraus lassen sich für die Bewilligung von Online-Anschlüssen durch die zuständige Bundesbehörde folgende Grundsätze ableiten:

Gesetzesstufe

Der Bund führt im Bundesamt für Polizeiwesen (BAP) unter anderen eine Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs nach Art. 9 ZentG und Art. 29 BetmG. Diese Zentralstelle unterstützt die Behörden des Bundes und der Kantone sowie anderer Staaten bei der Verhinderung und Bekämpfung des unerlaubten Betäubungsmittelverkehrs (Art. 9 Abs. 1 ZentG). Art. 11 Abs. 1 bis 3 ZentG enthält die wesentlichen Grundsätze über das Datenbearbeitungssystem DOSIS. Der Gesetzgeber hat darin dem Bundesrat die generelle Kompetenz eingeräumt, dass eine Zentralstelle zur Erfüllung ihrer Aufgaben ein Datenverarbeitungssystem betreiben kann und in diesem System besonders schützenswerte Daten und Persönlichkeitsprofile bearbeitet werden können, wenn und solange dies zur Erfüllung der Aufgaben der Zentralstelle notwendig ist. Zudem hat der Gesetzgeber festgelegt, dass ein solches Informationssystem von anderen Informationssystemen der Polizei und der Verwaltung getrennt geführt werden muss. In Art. 12 ZentG statuiert der Gesetzgeber das Recht von Dienststellen der Kantone, die im Rahmen ihrer Zuständigkeit mit der Zentralstelle zusammenarbeiten, durch ein Abrufverfahren auf das Datenverarbeitungssystem direkt zuzugreifen, sofern die notwendigen Schutz- und Sicherheitsmassnahmen getroffen sind. Dem Bundesrat wird die Kompetenz zuerkannt, dass er auch den Dienststellen der Kantone das Recht zur Dateneingabe einräumen kann. Der Bundesrat hat zudem die Einzelheiten der Datenverarbeitung durch die Zentralstellen und die Koordination der Systeme, das Zugriffsrecht und den Umfang des Zugriffs durch Stellen des Bundes und der kantonalen Behörden sowie die Aufbewahrungsdauer der Daten, Kontrollen und Schutzbestimmungen zu regeln (Art. 15 ZentG).

Verordnungsstufe

In der ZentV regelt der Bundesrat die Zusammenarbeit mit den Zentralstellen (Art. 6 ZentV), die spezielle Meldepflicht im Bereich des unerlaubten Betäubungsmittelverkehrs (Art. 12 ZentV), die Weitergabe von Personendaten an auskunftspflichtige Behörden (Art. 7 ZentV) sowie die Weitergabe von Personendaten an weitere Empfänger (Art. 8 ZentV). In der DOSIS-Verordnung regelt der Bundesrat speziell den Betrieb und die Benützung des Datenverarbeitungssystems DOSIS durch die Zentralstelle zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs. In diesem Sinne werden in einer separaten Verordnung die DOSIS-spezifischen Grundsätze festgelegt. Die DOSIS-Vo geht somit als lex specialis der allgemeiner gehaltenen ZentV vor.

DOSIS ist danach ein Informationssystem, welches ausschliesslich Daten enthalten darf, die den illegalen Drogenhandel betreffen. Drittpersonendaten werden darin nur so weit registriert, als diese für die Ermittlungen von Nutzen sind (Art. 3 DOSIS-Vo). Mit der Aenderung der DOSIS-Vo vom 19.11.1997 ist mit Wirkung ab 1.1.1998 aber die Führung von DOSIS-Stammdaten in einem gemeinsamen Index mit den ISOK-Stammdaten (Informationssystem zur Bekämpfung des organisierten Verbrechens) zulässig geworden (Art. 7 Abs. 7 DOSIS-Vo). Neu ist auch die Möglichkeit geschaffen worden, zur Vermeidung von Doppelerfassungen (vgl. dazu insbesondere die ergänzenden Bemerkungen des BAP in seiner Vernehmlassung vom 22.7.1998, Seite 2, Ziffer C./1.) bestimmte Daten (im Anhang zur DOSIS-Vo besonders markiert) in den zentralen Aktennachweis (ZAN) zu kopieren (Art. 11b Abs. 6 DOSIS-Vo). Das Vorgehen muss vom BAP im Bearbeitungsreglement im einzelnen geregelt werden. Die Uebertragung von Daten im DOSIS muss während des gesamten Uebertragungsvorganges in chiffrierter Form erfolgen (Art. 6 DOSIS-Vo).

Folgende Stellen dürfen durch ein Abrufverfahren an DOSIS angeschlossen (Art. 8 Abs. 1 DOSIS-Vo) werden:

- Die Zentralstelle (d.h. die Zentralstelle zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs),
- Die Betäubungsmitteldienste der kantonalen Polizeikorps,
- Der Kontrolldienst DOSIS/ISOK,

- Der Datenschutzbeauftragte des Bundesamtes für Polizeiwesen,
- Der Projektleiter und die Systemadministratoren,
- Dienststellen der Eidgenössischen Zollverwaltung nur für das Subsystem „Drogenlexikon und Modi Operandi“ (Art. 8 Abs. 3 DOSIS-Vo).

Auf Antrag hin können für konkrete Verfahren auch spezialisierte Strafverfolgungsbehörden der Kantone an DOSIS angeschlossen werden (Art. 8 Abs. 2 DOSIS-Vo). Von allen Benutzern darf aber gleichzeitig nur ein einziges der insgesamt 7 Subsysteme (PV=“Personen und Vorgänge“; JO=“Journal“; GT=“Geschäfts- und Terminkontrolle“; ER=“Allgemeine Erkenntnisse“; DL=“Drogenlexikon und Modi Operandi“; LA=“Lagebericht“; VI=“Visualisierung) abgefragt werden (Art. 8 Abs. 5 DOSIS-Vo). Ist ein weiterer Kanton durch das Ermittlungsverfahren betroffen, kann die Zentralstelle oder die zuständige kantonale Dienststelle der entsprechenden Behörde jenes Kantons das Zugriffsrecht ebenfalls einräumen (Art. 9 Abs. 3 DOSIS-Vo). Die Zentralstelle und die kantonalen Betäubungsmitteldienste geben die von ihnen erhobenen Vorgänge selbst ins DOSIS ein. Sie bestimmen dabei die Kategorien der Vorgänge, legen die Aufbewahrungsdauer fest und qualifizieren die Daten als gesichert oder ungesichert (Art. 10 Abs. 1 DOSIS-Vo). Der Kontrolldienst DOSIS/ISOK des BAP (Kontrolldienst) überprüft, ob die erfassten Daten den Bestimmungen dieser Verordnung entsprechen. Ist dies nicht der Fall, werden die Daten korrigiert oder gelöscht. Insbesondere überprüft der Kontrolldienst die provisorisch erfassten Daten, falls erforderlich in Zusammenarbeit mit der Stelle, welche die Daten erfasst hat. Der Kontrolldienst bestätigt die endgültige Fassung der Daten oder veranlasst deren Korrektur oder Löschung. Das BAP regelt die Einzelheiten der Datenkontrolle im Bearbeitungsreglement (Art. 10 Abs. 3 und 4 DOSIS-Vo). Art. 11, 11a und 11 b der DOSIS-Vo (in Kraft ab 1.1.1998) regeln ausführlich die Weitergabe von Daten an auskunftspflichtige Behörden (Art. 11), an weitere Empfänger (11a) und die Beschränkung der Datenweitergabe (Art. 11b). Darin wird die Zentralstelle ermächtigt, dass sie im DOSIS gespeicherte Personendaten an diverse Behörden „weitergeben“, „unaufgefordert weitergeben“ oder „bekanntgeben“ (vgl. dort) darf. Die Weitergabe sowie Empfänger, Gegenstand und Grund des Auskunftsersuchens sind im DOSIS zu registrieren (Art. 11b Abs. 5 DOSIS-Vo).

DOSIS-Grundsätze

1. **Von anderen Informationssystemen getrennt geführt.**
2. **Nur Daten über den illegalen Drogenhandel speichern.**
3. **Chiffrierung während gesamter Datenübertragung.**
4. **Numerus clausus von Benutzerstellen.**
5. **Gleichzeitig nur eines der 7 Subsysteme abfragen.**
6. **Datenweitergaben sind im DOSIS zu registrieren.**

322 IST-Situation Online-Verbindungen

Benutzerzahl

Gemäss chronologischer Auflistung über die Online-Verbindungen DOSIS vom 26.11.1997, deren Aktualität anlässlich der Befragung vom 2. Februar 1998 bestätigt wurde, sind seit dem 15.1.1993 bis heute insgesamt

409 Benutzer

an DOSIS angeschlossen worden.

Benutzerkategorien
Alle angeschlossenen Benutzer legitimieren sich über das Zentralstellengesetz und insbesondere gestützt auf die DOSIS-Vo (Art. 8 DOSIS-Vo) zur Nutzung von DOSIS. Die Zugriffsberechtigungen sind in der Zugriffsmatrix DOSIS-Vollbetrieb gemäss Anhang 2 zur DOSIS-Vo festgelegt.

Netzinfrastruktur und Sicherheitsmassnahmen
Alle angeschlossenen Verbindungspartner kommunizieren über bundeseigene Netzinfrastrukturen (LIS/EJPD; WAN EJPD). Die Kommunikation findet über TCP/IP statt (standardisierte Kommunikationsprotokolle). Als Sicherheitsmassnahmen werden zum Teil software-basierende End-to-End Chiffrierungen oder Firewall-Abschottungen gegenüber KOMBV1 – LIS eingesetzt.

323 Anschlussverfahren

Gesetzesstufe
Für den Online-Anschluss des BAP findet sich die gesetzliche Grundlage in Art. 11 Abs. 1 ZentG. Die Dienststellen der Kantone, die im Rahmen ihrer Zuständigkeit mit der Zentralstelle zusammenarbeiten, werden durch Art. 12 Abs. 1 ZentG zum Online-Anschluss legitimiert. In Art. 15 ZentG hat der Gesetzgeber die detaillierte Ausgestaltung des Online-Anschlussverfahrens an den Bundesrat delegiert.

Verordnungsstufe
In der ZentV sind keine Detailbestimmungen zum Online-Anschlussverfahren enthalten. Die damit zusammenhängenden Aufgaben, Kompetenzen und Verantwortlichkeiten sind hier nicht geregelt. Im wesentlichen wird in der ZentV nur festgelegt, an welche Behörden die Zentralstellen Personendaten weitergeben können (Art. 6, 7 und 8 ZentV). In der DOSIS-Vo regelt der Bundesrat dazu ebenfalls nur am Rande die Grundsätze eines Online-Anschlussverfahrens, indem er in Art. 8 Abs. 1 DOSIS-Vo die dafür direkt berechtigten Stellen bezeichnet (vgl. dazu die Ergänzungen des BAP in seiner Stellungnahme vom 22.7.1998, Seite 2, Ziffer C./2.). Auf Antrag hin können für konkrete Verfahren auch spezialisierte Strafverfolgungsbehörden der Kantone an DOSIS angeschlossen werden (Art. 8 Abs. 2 DOSIS-Vo). Die Zugriffsberechtigungen sind in der Zugriffsmatrix DOSIS-Vollbetrieb gemäss Anhang 2 zur DOSIS-Vo festgelegt. Zum Online-Anschlussverfahren selber, insbesondere zur Zuweisung oder Delegation einer Bewilligungskompetenz an das EJPD oder an das BAP sowie den damit zusammenhängenden Aufgaben, Kompetenzen und Verantwortlichkeiten enthält auch die DOSIS-Vo keine Angaben.

Ausführungsebene
Erst die (heute aufgehobene) Weisung des EJPD über das provisorische Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels aus dem Jahre 1994 (Weisung-DOSIS-Departement) bestimmt in Art. 4 Abs. 3, dass Anträge für Zugriffsbewilligungen vom Chef der Zentralstelle oder von seinem Stellvertreter genehmigt und die Zugriffe vom Rechenzentrum bzw. vom DOSIS-Administrator des BAP in DOSIS installiert werden. Nach Aufnahme des DOSIS-Vollbetriebs ist diese provisorische Weisung durch das Bearbeitungsreglement vom 20.12.1996 ersetzt worden. Ein neues Bearbeitungsreglement vom 20.3.1998, welches die diversen aufbau- und ablauforganisatorischen Veränderungen berücksichtigt, liegt vor und ist am 1.4.1998 in Kraft gesetzt worden. Das Bearbeitungsreglement des BAP vom 20. Dezember 1996 nimmt sich detailliert dem Anschlussverfahren und den damit zusammenhängenden Fragen an. Im Abschnitt 2 (Benutzer und Datenzugriff) wird in Art. 10 Abs. 2 erstmals explizit festgehalten, dass Anträge für Online-Anschlüsse vom antragstellenden Kommando (kantonales Polizeikommando) durch den DOSIS-Verantwortlichen der Zentralstellendienste zu genehmigen sind (Delegation der Direktion des BAP an DOSIS-Verantwortlichen). Diese Funktion wird zur Zeit vom Chef der Einheit Kriminalanalyse der

Zentralstellen wahrgenommen (vgl. auch Art. 1 Lit. f. Entwurf des Bearbeitungsreglements vom 20.3.1998). Die Anträge für Zugriffsberechtigungen sind an den DOSIS-Administrator zu stellen. Dieser verwaltet die Anträge und koordiniert die Realisierung. Er übermittelt dem Rechenzentrum die Anträge zur Installation im Hauptsystem und der Bereitstellung der TAXI- und DOSIS-Mail-Software. Er installiert auch die individuellen Zugriffsprofile jedes einzelnen Benutzers (Art. 10 Abs. 3 Bearbeitungsreglement). Die individuellen Zugriffsberechtigungen der am DOSIS-System arbeitenden Mitarbeiter erteilt, installiert und verwaltet das Rechenzentrum EJPD (Art. 10 Abs. 4 Bearbeitungsreglement).

324 Betrieb und Unterhalt

Das BAP ist im Januar 1993 an DOSIS angeschlossen worden. Derzeit sind 58 Benutzer des BAP im System registriert und zur Benutzung autorisiert. Die Kantonalen Polizeikorps sind ab September 1994 sukzessive an DOSIS angeschlossen worden. Im Jahre 1994 kamen LU (1.9.1994), SG (1.10.1994), TG (1.10.1994) und AG (1.11.1994) dazu. Im Jahre 1995 wurden die Kantone GE (1.3.1995), BE (1.4.1995), VD (1.4.1995) und TI (1.7.1995) mit DOSIS verbunden. Im Jahre 1996 sind keine Anschlüsse vorgenommen worden. 1997 sind weitere Kantone an DOSIS angekoppelt worden, so BS (23.4.1997), GR (23.4.1997), BL (6.5.1997), ZH (30.5.1997), OW, SO, UR, VS, ZG, Stapo ZH (je am 10.9.1997), FR und NE (je am 1.10.1997), SZ (13.10.1997), GL (27.10.1997), JU (29.10.1997), SH (5.11.1997), AI und AR (je am 11.12.1997) sowie NW (19.1.1998).

Im laufenden Betrieb und Unterhalt sind die Aufgaben und Verantwortlichkeiten in der DOSIS-Vo, der Weisung DOSIS-Kontrolle (Erlassbehörde Zentralstelle für Rauschgift im BAP) und im Bearbeitungsreglement des BAP (Erlassbehörde BAP) geregelt. Es kann auf diese Grundlagen verwiesen werden, da eine systematische Darstellung der dort geregelten Punkte für die Hauptfragen des vorliegenden Berichtes nicht notwendig ist.

Wie aus dem VKB-Bericht hervor geht, entstehen bekanntermassen in Teilbereichen der polizeilichen Fahndungsinstrumente parallele Anwendungen zwischen Bund und Kantonen. Die Datenbank DOSIS ist nach Auffassung vieler Kantone wegen der gesetzlich erst ab 1998 (Revision Teilvorlage C im Paket „Personenregister“) möglichen Verknüpfung mit ISOK und der strengen Datenschutzbestimmungen einer effektiven Polizeiarbeit eher hinderlich. Insbesondere erfülle DOSIS wegen der Begrenztheit auf einen einzigen Bereich der Kriminalität (illegaler Drogenhandel), der relativ kurzen Aufbewahrungsdauer der (ungesicherten oder nicht überprüften) Einträge (2 Jahre) und der Schwierigkeiten bei der Verwendung von Vorakten (im Gegensatz zu den gerichtspolizeilichen Akten) die Erwartungen der Polizeikorps an ein funktionales Fahndungsinstrument nicht. Ein kantonsweise von Privaten erstelltes System (ABI, angeboten von ehemaligen Mitarbeitern des RZ EJPD; demnächst in 19 Kantonen operativ) mit offenbar deutlich lascherer Beachtung der Datenschutzgesetzgebung könnte bald schon die Bundeslösung konkurrenzieren (VKB-Bericht Seite 24, Ziffer 32).

325 Kostenbeteiligungen

Aehnlich wie im Bereich RIPOL (Art. 22 RIPOL-Vo) regelt die DOSIS-Vo die Finanzierung des Informationssystems DOSIS (Art. 20 DOSIS-Vo). Der Bund finanziert den Datentransport bis zum zentralen Anschlusspunkt bei den Kantonen. Die Kantone übernehmen die Anschaffungs- und Unterhaltskosten ihrer Geräte sowie die Installations- und Betriebskosten für ihre Feinverteilungsnetze. Andere Aufwendungen, insbesondere eine Leistungsverrechnung des Bundes für seine Dienstleistungen im Bereich Informatik und Telekommunikation resp.

Rechenzentrumsbetrieb findet nicht statt. Es gelten bezüglich Akzeptanz und Durchsetzbarkeit dieselben Bemerkungen wie in Ziffer 315. (vgl. auch VKB-Bericht, a.a.O., Seite 30-31).

326 Kantone und andere bundesverwaltungsexterne Anschlüsse

Die insgesamt 409 angeschlossenen Benutzer des Informationssystems DOSIS verteilen sich zwischen Bund und Kantonsstellen wie folgt. 351 Benutzer (85.8%) gehören zu den Kantonalen Polizeikorps, 58 Benutzer sind Mitarbeitende des BAP (14.2%).

DOSIS-Nutzungsanteile

Bundesverwaltungs-**EXTERN** **85.8% = 351 Benutzer**

Bundesverwaltungs-**INTERN** **14.2% = 58 Benutzer**

Die Kantone NW, AI und AR sind zwar am System angeschlossen, eine operative Nutzung durch die entsprechenden Benutzer ist aber erst nach Abschluss der Ausbildung vorgesehen (Art. 12 Bearbeitungsreglement BAP). Diese dürfte in der Zwischenzeit erfolgt sein, sodass aktuell 3-5 zusätzliche externe Benutzer an DOSIS angeschlossen sein sollten.

327 Entwicklungsperspektiven

Gemäss Schreiben BAP vom 5.12.1997 an die parlamentarische Verwaltungskontrolle können ab Ende 1997 alle kantonalen Betäubungsmitteldienste auf DOSIS im Abrufverfahren (online) zugreifen (Seite 5). Auf den 1.1.1998 hat der Bundesrat auch die Aenderungen vom 19. November 1997 zur DOSIS-Vo in Kraft gesetzt. Aufgrund der formellgesetzlichen Grundlage in Art. 11 Abs. 1 ZentG muss der Betrieb von DOSIS aber nachwievor von ISOK und ZAN getrennt erfolgen. Das BAP macht geltend, dass dadurch für die Bekämpfung der organisierten Kriminalität zum Teil schwer lösbare Problem entstehen, weil nicht in einer gemeinsamen Datenbank alle relevanten Deliktsbereiche bearbeitet werden können. Aufgrund dieser Ausgangslage hat der Bundesrat in der Botschaft betreffend Schaffung und Anpassung gesetzlicher Grundlagen für Personenregister (Paket "Personenregister“ zur Aenderung des StGB, des SVG und des ZentG) die Revision von Art. 11 Abs. 1 ZentG eingeleitet. Sie soll es den Zentralstellendiensten des BAP erlauben, eine ihrer neuen Organisationsstruktur und Arbeitsweise angepasste einheitliche Datenbank betreiben zu dürfen. Die Vorlage besteht aus vier Teilen, die alle elektronische Personendatenbanken betreffen:

- Teilvorlage A: Personendossierverwaltung im BAP.
- Teilvorlage B: Automatisierung Strafregister.
- Teilvorlage C: Personendatenverarbeitung durch kriminalpolizeiliche Zentralstellen im BAP.
- Teilvorlage D: Automatisierte Register über Fahrzeuge, Fahrzeughalter und Administrativmassnahmen.

Die Vorlage bezweckt die rechtzeitige Schaffung oder Anpassung der formellgesetzlichen Rechtsgrundlagen (vgl. Art. 38 Abs. 3 DSG), die für einen rationellen und dem technischen Fortschritt entsprechenden Betrieb der Personendatenbanken in den vier Teilbereichen erforderlich sind.

Hinsichtlich DOSIS ist insbesondere die Teilvorlage C von Bedeutung. Sie sieht vor, dass die kriminalpolizeilichen Zentralstellen im BAP zu einem nationalen und internationalen Informations-, Analyse-, Koordinations- und Ermittlungszentrum ausgebaut werden. Die bisherigen Zentralstellenfunktionen werden dabei unter einer neuen und einheitlichen Organisationsstruktur zusammengefasst. Sie unterteilen sich in eine kriminalanalytische, eine operative und eine logistische Einheit (Botschaft Seite 6, Ziffer 114.2). Die mit der Teilvorlage C vorgeschlagene Aenderung von Artikel 11 Abs. 1 ZentG soll den Mitarbeitenden der kriminalpolizeilichen Zentralstellendienste im BAP den individuellen Zugriff auf DOSIS und ISOK ermöglichen. Diese Zwischenlösung soll die Zeit überbrücken, bis das Nachfolgeprodukt von DOSIS und ISOK entwickelt und als einheitliches und gemeinsames Informationssystem einsatzbereit sein wird (Botschaft Seite 8, Ziffer 114.5). Auch das neue gemeinsame Informationssystem der kriminalpolizeilichen Zentralstellen im BAP soll von anderen Datenbanken der Polizei und Verwaltung streng getrennt betrieben werden müssen (Botschaft Seite 17, Ziffer 23).

An DOSIS sind am 31.12.1997 praktisch alle Kantonalen Polizeistellen im Betäubungsmittelbereich angeschlossen, sodass die Bewilligungserteilung nicht mehr von grosser Bedeutung sein wird. Aus der Botschaft des Bundesrates (Paket Personenregister) ist jedoch ersichtlich, dass die Errichtung eines gemeinsamen Informationssystems auf dem Gebiet der Strafverfolgung auch im Uebereinkommen über die Errichtung eines Europäischen Polizeiamtes vorgesehen ist (EUROPOL-Uebereinkommen, Abl. Nr. C 316 vom 27. November 1995, S. 1), welches vom Rat aufgrund von Art. K.3 des Vertrags über die Europäische Union am 26. Juli 1995 angenommen und den Mitgliedstaaten zur Ratifizierung empfohlen wurde. Die Schaffung der neuen formellgesetzlichen Grundlage für ein zukünftiges gemeinsames Informationssystem sei daher auch im Hinblick auf die Zusammenarbeit mit ausländischen Polizeikräften sinnvoll. Daraus kann geschlossen werden, dass das einheitliche und gemeinsame Nachfolgesystem von DOSIS und ISOK mit internationalen Behördenstellen kommunizieren kann, wenn der Gesetzgeber ausdrücklich dafür die formellgesetzlichen Grundlagen schafft. Diese Tatsache ist aus der Sicht der Entwicklungsperspektiven und der Praxis für die Bewilligung von Online-Anschlüssen insofern relevant, als die Bewilligungspraxis sowie die Regelung der zuständigen Behörde und des Verfahrens für die Erteilung von solchen Anschlussbewilligungen zunehmende Bedeutung erhalten werden.

328 Zusammenfassung und Bewertung für RIPOL und DOSIS

1. Primäres Hauptmerkmal im Bereich der Bewilligung von Online-Anschlüssen für die Informationssysteme RIPOL und DOSIS ist eine fortlaufende Delegation der Zuständigkeit, Aufgaben, Kompetenzen und Verantwortung für Online-Bewilligungen bis auf die unterste operative Verwaltungseinheit.

   Während die Zugriffs- und Bearbeitungsrechte bis auf Feldebene geregelt werden (RIPOL-Vo Anhang) und Benutzer- und Wartungsreglement die Modalitäten für den Weiterausbau und die Wartung des Projektes RIPOL detailliert darstellen, fehlen für das Bewilligungsverfahren entsprechend detaillierte Verfahrensbestimmungen (Prozessbeschreibungen), Checklisten oder Arbeitsanweisungen. Einzig in Ziffer 713 des Benutzer- und Wartungsreglements RIPOL vom Mai 1987 wird festgestellt, dass das BAP über Anschlussbegehren der Bundesprojektbenutzer beschliesse. Ueber die viel zahlreicheren Anschlussbegehren der kantonalen und kommunalen Benutzer sagt das Benutzer- und Wartungsreglement nichts aus. Auch werden weder das konkrete Bewilligungsverfahren noch die dabei zwingend zu prüfenden Anschlussgrundsätze oder die Dokumentation und Ablage der entsprechenden Bewilligungsentscheide geregelt.

Im DOSIS werden ebenfalls besonders schützenswerte Daten und Persönlichkeitsprofile gespeichert. Dies hat den Gesetzgeber veranlasst, ausdrücklich eine Trennung dieses Informationssystems von anderen Informationssystemen der Polizei und der Verwaltung zu statuieren. Der Gesetzgeber stellt also sehr hohe Anforderungen an die Bearbeitung und den Umgang mit diesen sensiblen Daten. Diesen sehr hohen Anforderungen steht die Tatsache entgegen, dass hinsichtlich Online-Anschlüssen vom Bundesrat weder in der ZentV noch in der DOSIS-Vo explizit eine Regelung bezüglich Zuständigkeit, Aufgaben und Verantwortung sowie zu beachtender Grundsätze bei der Bewilligungserteilung erlassen wurde, obwohl der Gesetzgeber dies in Art. 15 ZentG vom Bundesrat verlangt hat. Erst auf der Verwaltungsstufe (Weisung DOSIS-Departement und Bearbeitungsreglement BAP) sind die entsprechenden Grundsätze festgelegt worden. Auf dieser Stufe kommt eine weitere Delegation an die unterste operative Verwaltungseinheit durch Delegation der Entscheidungskompetenz vom Direktor BAP an den Verantwortlichen für das jeweilige System hinzu. Angesichts der Entwicklungsaussichten mit möglichen Anschlüssen von ausländischen Polizeikräften (EUROPOL-Uebereinkommen) ist eine klare Regelung des Bewilligungsverfahrens, der Zuständigkeiten, Aufgaben und Verantwortung sowie der ausdrücklich zu beachtenden Grundsätze durch die Bewilligungsbehörde zwingend notwendig.

2. Die in übergeordneten Erlassen (Gesetz, Verordnung) aufgestellten Grundsätze für Online-Bewilligungen drohen durch eine immer weiter nach unten delegierte Verantwortung verloren zu gehen, indem durch die Delegation auf die operative Anwendungsebene andere Interpretationen und Interessen den ursprünglichen Gesetzgeberwillen aushöhlen können. Die ehemals statuierten Grundsätze können aufgrund der steten Weiterdelegation sowie der Festschreibung in verschiedenen Erlassen in der Einzelfallanwendung (Bewilligungserteilung) auf unterster Verwaltungsstufe damit letztlich auch unbeachtet bleiben.

3. Der politische Wille des Gesetzgebers für die Delegation von Online-Bewilligungen (Rahmenbedingungen) wird mit jeder Delegationsstufe nach unten unpräziser und unklarer, resp. durch Rahmenbedingungen und Einflussfaktoren der nächsten Delegationsstufe überlagert.

4. Eine Delegation von Bewilligungskompetenz für Online-Anschlüsse nach unten verläuft diametral entgegensetzt zur Sensibilität der Daten im Polizeiwesen. Je höher die Sensibilität (Schutzwert der Daten; besonders schützenswerte Daten; Persönlichkeitsprofile) der zu bearbeitenden Daten ist, desto weniger nach unten sollte die Kompetenz für Online-Bewilligungen delegiert werden.

5. Je weiter die Bewilligungskompetenz für Online-Anschlüsse nach unten delegiert wird, je schneller besteht Gefahr für einen Interessenkonflikt der zuständigen Bewilligungsbehörde. Sie setzt sich aufgrund ihres eigenen, legitimen Interesses an der umfassenden Nutzung ihres Informationssystems (vgl. dazu die Ergänzungen des BAP in seiner Stellungnahme vom 22.7.1998, Seite 3 und 4, Ziffer 4) schneller dem Vorwurf aus, die für eine Bewilligung vorgebrachten Gründe eines Antragstellers eher positiv zu bewerten. Dies insbesondere auch dann, wenn die entsprechende Verwaltungseinheit als Jahresziel des Departementes die Vorgabe erhält, alle Kantone an ein entsprechendes Informations-System anzuschliessen.

6. Auf der untersten operativen Stufe einer Verwaltungseinheit bestehen direkte Kontakte (Arbeitsgruppen, Interkantonale Polizeigremien; konkrete Einsätze etc.) zwischen

Antragstellern und Bewilligungsbehörde. Diese Tatsache ist nicht geeignet, die Unabhängigkeit der Bewilligungsbehörde zu untermauern. Insbesondere im Rahmen der Ueberprüfung der sensiblen Bewilligungsvoraussetzung, nur auf diejenigen Datenbanken Zugriff zu gewähren, die der antragstellende Benutzer zur Erfüllung seiner gesetzlichen Aufgaben benötigt (Art. 3 Abs. 3 RIPOL-Vo), kann zwischen gleichrangigen Verwaltungseinheiten mit ähnlich gelagerten Aufgaben weniger Veranlassung zur kritischen Hinterfragung der Notwendigkeit, Zweckmässigkeit und Verhältnismässigkeit eines Online-Anschlusses bestehen (vgl. dazu die Ergänzungen des BAP in seiner Stellungnahme vom 22.7.1998, Seite 3 und 4, Ziffer 4). Im Bereich der sehr sensiblen Datenbestände im Polizeiwesen kommt der Wahrung der Unabhängigkeit einer Bewilligungsbehörde besonders grosse Bedeutung zu.

7. In sogenannten Pilotprojekten wird zum Teil ohne entsprechende formelle gesetzliche Grundlage der Aufbau und die Realisierung eines Informationssystems mit sensiblen Daten an die Hand genommen (z.B: VOSTRA, EVA oder Bereich Geldwäscherei). Sukzessive werden solche Informationssysteme unter Anschluss immer weiterer Testbenutzer aufgebaut und ausgedehnt und die Anforderungen und Funktionalitäten des Informationssystems erweitert. Der definitive Schritt in einen operativen Betrieb ist vielfach unter solchen Voraussetzungen kaum mehr klar zu erkennen und abzugrenzen. Die formelle gesetzliche Grundlage wird erst im Nachhinein geschaffen.

8. Zusätzliche Schwierigkeiten bietet die Tatsache, dass der Bund zwar mit RIPOL und DOSIS bundeseigene Informations-Systeme zur Verfügung stellt, die Polizeiaufgaben aber grossmehrheitlich durch die Kantone wahrgenommen werden. Diese gemischte halb zentralistische, halb föderalistische Ueberwachungsorganisation (Georg Kreis, Staatsschutz in der Schweiz, Verlag Paul Haupt Bern, 1993, S. 206) erschwert es der Bewilligungsbehörde des Bundes, in aufbau- und ablauforganisatorischen Fragen direkt auf die Kantone einzuwirken, wenn nicht eine entsprechende gesetzliche Kompetenz dazu ausdrücklich geschaffen wird. Der Online-Datenaustausch hat direkte Auswirkungen auf die Ablauforganisation in den kantonalen Dienststellen. Die technischen und applikatorischen Vorgaben verändern die Verwaltungsstrukturen in der Organisationshoheit der Kantone zum Teil massgeblich (vgl. dazu VKB-Bericht, a.a.O., Seite 29). Insbesondere im Rahmen der Ueberprüfung der Notwendigkeit, Zweckmässigkeit und Verhältnismässigkeit eines kantonalen oder kommunalen Online-Anschlusses kommt die Bundesbewilligungsbehörde dadurch an ihre Beurteilungs- und Beeinflussungsgrenze. Damit entsteht ein schwieriges Spannungsverhältnis zwischen dem verantwortlichen Datenherr, welcher die Einhaltung aller gesetzlichen Vorgaben für einen Online-Anschluss gewährleisten muss, und der kantonalen oder kommunalen Benutzerorganisation, welche die entsprechenden Aufgaben, Kompetenzen und Verantwortungen sowie die dazu notwendigen aufbau- und ablauforganisatorischen Grundlagen in ihrem Verantwortungsbereich autonom festlegen kann.

9. In diesem Sinne kann der verantwortliche Datenherr auch nicht überprüfen, ob im antragstellenden Kanton oder kommunalen Gemeinwesen bezüglich Online-Anbindung einer Verwaltungseinheit die entsprechende politische Willensbildung stattgefunden hat und ein Online-Anschlussbegehren dem grundsätzlichen Einverständnis der politisch verantwortlichen Behörde entspricht. Eine solche Entscheidung könnte nur über ein kantonsintern festgelegtes eigenes Bewilligungsverfahren erreicht werden.

In diesem Zusammenhang wird auf die **Verordnung über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches vom 23. April 1996** (SRL Nr. 39b; Sicherheitsverordnung LU) des

Kantons Luzern hingewiesen. Diese Verordnung sieht für jeden Anschluss einer Dienststelle des Kantons an ein Kommunikationsnetz die Einholung einer Bewilligung beim zuständigen Departementsvorsteher vor. Im Zusammenhang mit der Bewilligungserteilung sind eine Risikobeurteilung vorzunehmen und Sicherheitsmassnahmen vorzuschlagen, der kantonale Datenschutzbeauftragte ist anzuhören und der departementseigene Informatik-Beauftragte hat für die Umsetzung und Durchsetzung zu sorgen. Damit wird auf Seiten der antragstellenden kantonalen Instanzen sichergestellt, dass die gesetzlichen Vorschriften und Grundsätze überprüft und der Online-Anschluss durch eine unabhängige, übergeordnete Verwaltungseinheit sanktioniert wird.

10. Die Rahmenbedingungen der Technik (Datenbanken, Internet und Intranet) fördern den direkten Datenaustausch zwischen Fachstellen des Bundes und der Kantone. Der Dienstweg über die übergeordnete Verwaltungsstelle als Führungsinstanz hat wenig bis keine Bedeutung mehr, weil zwischen den Führungsverantwortlichen und den Informatikverantwortlichen kein genügender Dialog stattfindet und deshalb auch die notwendigen Instrumente zur Führung und Problemerkennung nicht geschaffen werden. Es ist daher einfacher und schneller, auf der technischen Ebene Lösungen zu realisieren, die einen hohen Nutzen bringen. Der (notwendige) Einbezug der Führungsebene wird dabei (insbesondere auch wegen ihres fehlenden Fachwissens im technischen Umfeld) zunehmend als störend, schleppend und hinderlich empfunden (vgl. dazu auch VKB-Bericht, Seite 27). Dies kann im Bereich von Online-Anschlüssen zu technisch orientierter Bewilligungspraxis führen, welche vornehmlich von der technischen Machbarkeit, nicht mehr aber von der Notwendigkeit, Zweckmässigkeit und Verhältnismässigkeit eines Anschlusses bestimmt wird.

11. Für die Bewilligung von Online-Anschlüssen von Schweizerischen Vertretungen im Ausland wie auch der Interpol-Stellen sind dem Experten keine Verfahrensanweisungen bekannt. Der entsprechende Bewilligungsprozess soll direkt zwischen den zuständigen Generalsekretariaten EJPD und EDA festgelegt worden sein.

12. Die im Benutzer- und Wartungsreglement vom Mai 1987 sowie in den Richtlinien betreffend Einführung von RIPOL2 vom 25. Juni 1990 enthaltenen Zuständigkeiten und dazu erwähnten Organisationseinheiten stimmen nicht mehr mit den tatsächlichen Organisationsstrukturen überein. Dies erschwert einerseits die Transparenz hinsichtlich Aufgaben, Kompetenzen und Verantwortung, anderseits schafft dies einen organisationsrechtlich freien, d.h. verantwortungslosen Bereich.

329 Empfehlungen und Massnahmenvorschläge für RIPOL und DOSIS

1. Der Gesetzgeber muss sich der Delegationsproblematik stärker bewusst werden. Die fortschreitende technische Entwicklung im Kommunikationsbereich erfordert vom Gesetzgeber resp. vom Gesetzesredaktor prägnante und eindeutige juristische Begriffe, welche eine schleichende Erweiterung von Online-Anschlüssen über den ursprünglichen gesetzgeberischen Willen hinaus ausschliessen. Generalklauseln und Delegationskompetenzen sind exakt zu hinterfragen und deren Auswirkungen zu analysieren. Der politische Wille bezüglich Bewilligungskompetenz muss insofern präzise formuliert werden, als der Gesetzgeber klar und unmissverständlich festzulegen hat, bis auf welche Behördenstufe hinunter er eine Delegation von Online-Bewilligungen zulassen will. Generalklauseln wie in Art. 351bis Abs. 3 Buchstabe h StGB („weitere Justiz- und Verwaltungsbehörden“) sind zu vermeiden, wenn der Gesetzgeber einen Numerus clausus von Online-Benutzern durchsetzen will.

2. Die an der Nutzung und Verbreitung sowie an einem umfassenden Einsatz eines Informationssystems direkt interessierte Verwaltungseinheit (Bundesamt, Sektion, Abteilung, etc.) sollte dann nicht gleichzeitig Bewilligungsinstanz für Online-Anschlüsse sein, wenn sie diesbezüglich in einem Interessenkonflikt steht oder der Anschein eines Interessenkonfliktes entstehen könnte. Eine übergeordnete Verwaltungseinheit ist als unabhängige Bewilligungsinstanz zur Erteilung von Online-Anschlussbewilligungen besser geeignet, weil sie keine direkten Interessen vertritt.

3. Das EJPD hat die generelle Delegation von Bewilligungsentscheiden auf die unterste operative Verwaltungseinheit in allen betroffenen Bereichen zu überprüfen. Die Online-Anschlussbewilligung muss von einer der Wichtigkeit und Tragweite des Bewilligungsentscheides sowie der Sensibilität der Daten adäquaten, unabhängigen Bewilligungsinstanz vorgenommen werden. Als Minimalanforderung sollten alle Erstanschlüsse von Verwaltungsstellen des Bundes und Erstanschlüsse von kantonalen oder kommunalen Verwaltungsstellen auf der Stufe des Direktors des zuständigen Bundesamtes bewilligt werden. Das EJPD hat bezüglich der Bewilligungsinstanz gegenüber Schweizerischen Vertretungen im Ausland sowie den ausländischen Interpolstellen (RIPOL: Staatsvertragsgrundlagen) oder anderen ausländischen Polizeistellen (DOSIS: EUROPOL-Uebereinkommen) die stufen- und interessengerechte Bewilligungsinstanz festzulegen und allenfalls eine Aenderung der entsprechenden Verordnungen des Bundesrates in die Wege zu leiten.

4. Die Online-Bewilligungsverfahren sind vom EJPD in Form von Ablaufdiagrammen (Prozessbeschreibungen) für alle im Polizeibereich involvierten zuständigen Bundesämter übergeordnet und möglichst einheitlich festzulegen. Als Prozessbeschreibungen sollen sie mindestens den Status von Departementsweisungen erhalten und allenfalls an die Standards der ISO-Norm angelehnt werden. Sie sind zudem mit den bestehenden Prozessbeschreibungen des RZ EJPD abzustimmen.

5. Das EJPD hat zu prüfen, welche Minimalanforderung an die Gesuche kantonaler oder kommunaler Behörden bezüglich Antragstelle und übergeordneter kantonaler/kommunaler Kontrollinstanz zu formulieren sind, damit der Sensibilität und den datenschutzrechtlichen Grundanforderungen an die Notwendigkeit, Zweckmässigkeit und Verhältnismässigkeit genügend Nachachtung verschafft wird. Diese Anforderungen sind in entsprechende Erlasse aufzunehmen.

6. Das EJPD hat durch entsprechende gesetzliche Regelungen dafür zu sorgen, dass vor der Initialisierung von Informatik-Pilotprojekten im Polizeibereich die notwendige formelle Gesetzesgrundlage geschaffen wird, wenn besonders schützenswerte Personendaten bearbeitet werden. Es hat zudem in Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten zu prüfen, ob im Datenschutzgesetz explizit eine Zusatzbestimmung für die Durchführung von Pilotprojekten aufzunehmen ist, welche als formelle gesetzliche Grundlage die Mindestanforderungen an Pilotprojekte in der Bundesverwaltung im Bereich sensibler Daten festlegt.

7. Es ist seitens des EJPD zu prüfen, ob die Durchsetzung der gesetzlichen Grundlagen für einen Online-Anschluss sowie die Sicherstellung und Aktualisierung der technischen und organisatorischen Schutzmassnahmen über konkrete Nutzungsverträge zwischen dem zuständigen Bundesorgan als verantwortlichem Datenherr und den systemnutzenden Bundes- resp. Kantons- oder Kommunalverwaltungseinheiten erreicht werden kann.

8. Das EJPD hat im Rahmen der kantonalen Polizeidirektorenkonferenz die Problematik der Antragstellung für Online-Anschlüsse durch die unterste Verwaltungsstufe mit den zuständigen Polizeidirektoren (Regierungsräte) der Kantone zu diskutieren und gegebenenfalls gemeinsame Minimalstandards für ein kantonsinternes Bewilligungsverfahren als Vorstufe zur Antragstellung an die zuständige Bundesbehörde festlegen lassen.

9. Das BAP muss das Benutzer- und Wartungsreglement RIPOL vom Mai 1987 sowie dasjenige für DOSIS vom 20. Dezember 1996 an die tatsächlichen und rechtlichen Gegebenheiten (Organisationsänderungen; Aenderungen DOSIS-Vo mit Inkrafttreten am 1.1.1998, so u.a. Art. 4 Bearbeitungsreglement bezüglich Datenherkunft) anpassen. Dabei hat es die vom EJPD gemäss Ziffer 3 oben festzulegenden Grundsätze der Bewilligungsdelegation mitzuberücksichtigen. Das Bewilligungsverfahren, die konkret zuständige Verwaltungseinheit, die zu prüfenden Voraussetzungen sowie die Dokumentation und Archivierung entsprechender Entscheide sind in Abstimmung mit dem EJPD zu regeln. Zudem muss in den Reglementen, soweit erforderlich, die neue Aufbauorganisation des BAP (kriminalpolizeiliche Zentralsstellen im BAP) berücksichtigt werden. (Forderung zum Teil mit Vorbereitung eines neuen Bearbeitungsreglementes DOSIS vom 20.3.1998 erfüllt).

10. Das Bundesamt für Informatik (BFI) hat zu prüfen, ob für Online-Anschlüsse an Bundes-Informatiksysteme im Projektführungshandbuch HERMES95 entsprechende Ergänzungen einzufügen sind, welche die obigen Massnahmen nachhaltig unterstützen und die Grundsätze der Transparenz, Effizienz und Qualität in der Realisierung von Online-Anschlüssen bei Informatikvorhaben (inkl. Pilotprojekten) im Bund sicherstellen.

33 ISIS und ISIS-PLUS

331 Gesetzliche Grundlagen und Grundsätze

Innere Sicherheit (ISIS)

a) Verordnung über das provisorische Staatschutz-Informations-System (ISIS-Verordnung) vom 31. August 1992 mit Aenderung vom 2. Dezember 1996 (SR 172.213.60).
b) Verordnung über die Bearbeitung von Personendaten im präventiven Staatsschutz (Datenschutzverordnung-Staatsschutz) vom 14. Juni 1993 (SR 235.14).
c) Weisung des EJPD über die Durchführung des Staatsschutzes vom 9. September 1992 mit Aenderung vom 22. Dezember 1993.
d) Weisungen des EJPD über das provisorische Staatsschutz-Informations-System (ISIS-Weisungen) vom 31. August 1992.
e) ISIS-Bearbeitungsrichtlinien des Chefs der Bundespolizei vom 1.2.1995 (Weisung Nr. 082) mit Anhang 1 vom 22. Mai 1997 (Vollzugsweisung betreffend Registrierung der Mitgliedschaft bei staatsschutzrelevanten Organisationen/Gruppierungen), Anhang 2 vom 1.6.1994 (Check- und Punkteliste gesicherte/ungesicherte Vorgangsdaten) und Anhang 3 (undatiert; Richtlinie über Zuordnung von Datenbank und Vorgangskategorie).
f) Weisung des Chefs der Bundespolizei über die Erfassung von Personen/Organisationen in den Datenbanken STA/NSS vom 21.9.1995 (Weisung Nr. 086) mit Memos vom 6.10.1995 und 24.2.1997 zu Weisung Nr. 086.

Daraus ergeben sich zusammengefasst folgende Grundsätze:

331.1 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (noch nicht in Kraft gesetzt)

Vorerst ist bezüglich Rechtsgrundlagen festzuhalten, dass das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21.3.1997 trotz Nichtzustandekommen des fakultativen Referendums und entsprechender Verfügung der Schweizerischen Bundeskanzlei vom 29.12.1997 (vgl. BBl 1997 IV 1627 ff.) vom Bundesrat im Zeitpunkt der Abfassung des Expertenberichts noch nicht in Kraft gesetzt worden war. Gemäss Auskunft der Bundeskanzlei und des Bundesamtes für Justiz wird mit der Inkraftsetzung des BWIS vorerst bis zur Volksabstimmung über die Initiative „SOS“ zugewartet. Diese Abstimmung ist auf den 7.6.1998 angesetzt. Wird die Initiative abgelehnt, so soll das Gesetz frühestens auf den 1.10.1998, eventuell auf den 1.1.1999 in Kraft gesetzt werden. In der Zwischenzeit hat der Bundesrat BWIS auf den 1.7.1998 in Kraft gesetzt. Die entsprechenden Ausführungsbestimmungen (Verordnungen des Bundesrates) sollen anschliessend folgen (vgl. dazu auch Ziffer 357.). Diese Verordnungen sind noch nicht bekannt. Das BWIS bringt auf der Basis neuer gesetzlicher Grundlagen die entsprechenden Grundsätze für die Bewilligungspraxis und die Handhabung des Staatschutz-Informationssystems ISIS.

Der Bundesrat bestimmt gestützt auf Art. 11 Abs. 1 des BWIS durch Verordnung, welche Vorgänge und Feststellungen die Kantone und die in Art. 13 genannten Behörden und Amtsstellen unaufgefordert zu melden haben. Er umschreibt auch den Umfang der Informationspflicht und das Verfahren der Auskunftserteilung. Die Informationsbeschaffung wird sichergestellt durch

- Auswerten öffentlich zugänglicher Quellen,
- Einholen von Auskünften,
- Einsicht in amtliche Akten,

- Entgegennahme und Auswerten von Meldungen,
- Nachforschen nach der Identität oder dem Aufenthalt von Personen,
- Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen,
- Feststellen der Bewegungen und der Kontakte von Personen.

Die gesammelten Informationen müssen nach den Grundsätzen von Art. 15 Abs. 1 BWIS ausgewertet werden. Die Sicherheitsorgane dürfen besonders schützenswerte Personendaten und Persönlichkeitsprofile nur im Rahmen der Verordnung bearbeiten (Art 15 Abs. 2 BWIS). Das Bundesamt (Polizeidienst der Bundesanwaltschaft [Bundespolizei, BuPo]) bearbeitet diejenigen Daten, welche jederzeit rasch greifbar sein müssen, mit einem elektronischen Informationssystem (= formelle gesetzliche Grundlage für ISIS). ISIS steht nur den mit Aufgaben nach dem BWIS betrauten Personen des Bundesamtes, den anderen Polizei- und Strafverfolgungsbehörden des Bundes sowie den Sicherheitsorganen der Kantone über ein Abrufverfahren zur Verfügung. Die Definition der Voraussetzungen für den Anschluss der kantonalen Sicherheitsorgane an ISIS wird an den Bundesrat delegiert, die Zugriffsrechte regelt das Departement (Art. 15 Abs. 3 BWIS). Die Daten, die ausserhalb eines gerichtspolizeilichen Ermittlungsverfahrens beschafft werden, und die Daten der gerichtlichen Polizei sind im Informationssystem getrennt zu bearbeiten. Dieses muss von anderen Informationssystemen der Polizei oder der Verwaltung getrennt geführt werden (Art. 15 Abs. 4 BWIS). Die Kantone bearbeiten die Daten, die sie beim Vollzug dieses Gesetzes erhalten, nach den Bestimmungen des Bundes. Sie bewahren sie getrennt von kantonalen Daten auf (Art. 16 Abs. 1 BWIS). Soweit die kantonalen Sicherheitsorgane eigene automatisierte Informationssysteme führen, gelten die Bestimmungen für das Informationssystem des Bundes sinngemäss. Die Betriebsordnung des kantonalen Systems muss vom Departement genehmigt werden (Art. 16 Abs. 2 BWIS). Soweit kantonale Sicherheitsorgane Daten nach diesem Gesetz bearbeiten, unterstehen sie dem Datenschutzrecht des Bundes (Art. 16 Abs. 3 BWIS).
Im neuen Gesetz vorgesehen ist auch eine Personensicherheitsprüfung (4. Abschnitt). Der Bundesrat kann unter gewissen, im Gesetz aufgeführten Voraussetzungen, Sicherheitsprüfungen vorsehen für Bedienstete des Bundes, Angehörige der Armee und Dritte, die an klassifizierten Projekten im Bereich der inneren oder äusseren Sicherheit mitwirken (Art. 19 BWIS). Die Kantone können für ihre Bediensteten, die unmittelbar bei Aufgaben des Bundes nach diesem Gesetz mitwirken, ebenfalls eine Sicherheitsprüfung durchführen. Der Bundesrat bezeichnet eine Fachstelle, welche die Sicherheitsprüfungen in Zusammenarbeit mit dem Bundesamt durchführt (Art. 21 BWIS).

Im 6. Abschnitt sind die organisatorischen Bestimmungen enthalten. Danach nimmt die Geschäftsprüfungsdelegation die parlamentarische Kontrolle wahr (Art. 25 Abs. 1 BWIS). Der Bundesrat sorgt dafür, dass die Tätigkeit des Bundesamtes auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit überprüft wird. Das EJPD erlässt dazu einen jährlichen Kontrollplan, der mit den parlamentarischen Kontrollen abzustimmen ist (Art. 26 BWIS). Ebenso legt der Bundesrat die Mindestanforderungen an die Kontrolle in den Kantonen fest. Die Durchführung der Kontrollen ist Sache der Kantone (Art. 26 Abs. 3 BWIS). Das Bundesamt hat die Pflicht, die Polizeidirektoren und Sicherheitsorgane laufend über die getroffenen und geplanten Massnahmen nach diesem Gesetz zu orientieren (Art. 27 Abs. 3 BWIS).

331.2 Verordnung über das provisorische Staatsschutz-Informations-System (SR 172.213.60)

Aus obenerwähntem Grunde ist derzeit in rechtlicher Hinsicht noch immer die Verordnung über das provisorische Staatsschutz-Informations-System (ISIS-Verordnung) vom 31. August 1992 die massgebliche gesetzliche Grundlage zur Beantwortung von Online-Fragen. Diese Verordnung stützt sich auf Art. 102 Ziffern 8-10 der Bundesverfassung (SR 101), Art. 24 des Bundesgesetzes

über den Datenschutz (SR 235.1) sowie die Artikel 15, 17 und 100 ff. des Bundesstrafrechtspflegegesetzes (SR 312.0). Die Geltungsdauer der Verordnung ist vom Bundesrat am 2. Dezember 1996 bis zum 31. Dezember 1999 verlängert worden (Art. 24 Abs. 2 ISIS-Vo). Eine formelle gesetzliche Grundlage für den Aufbau und den Betrieb des automatisierten Informationssystems ISIS und damit auch für das Bearbeiten von Personendaten resp. von besonders schützenswerten Personendaten im Sinne des Datenschutzgesetzes existiert somit im Zeitpunkt der Berichtsabfassung noch nicht. Das BWIS würde die entsprechenden gesetzlichen Grundlagen (Art. 15 Abs. 2 BWIS) schaffen (per 1.7.1998 bereits in Kraft gesetzt).

Gestützt auf Art. 1 ISIS-Verordnung betreibt der Polizeidienst der BuPo das provisorische informatisierte Staatsschutz-Informations-System (ISIS). Gestützt auf Art. 3 Abs. 4 ISIS-VO hat des EJPD in Weisungen festzulegen, welche Daten gespeichert werden dürfen. Es bezeichnet darin die einzelnen Datenkategorien. Die entsprechende Weisung (ISIS-Weisung) datiert vom 31. August 1992. Als Benutzer von ISIS sind nur die Bediensteten der BuPo zugelassen. Die Daten können zudem vom Bundesanwalt und seinem Substituten abgefragt werden. Zur Erfüllung gesetzlicher Aufgaben können im Einzelfall folgende weitere Bedienstete der Bundesanwaltschaft bestimmte Daten abfragen:

a) Bedienstete des Rechtsdienstes für die Mitwirkung bei der Durchführung von staatsschutz- und nicht-staatsschutzrelevanten Strafverfahren sowie bei der Erledigung von administrativen Aufgaben,
b) Bedienstete der zentralen Dienste für die Erledigung von administrativen Aufgaben,
c) Bedienstete des Sicherheitsdienstes der Bundesverwaltung für sicherheitspolizeiliche Aufgaben.

Das Departement kann Bediensteten des Bundesamtes für Polizeiwesen (BAP) die einzelfallweise Abfrage bestimmter Daten der Datenbank Staatsschutz (STA) und nicht-staatsschutzrelevante Strafverfahren (NSS) zur Erfüllung gesetzlicher Aufgaben erlauben (Art. 4 ISIS-Vo). Das Departement hat Weisungen über die Berechtigung dieser Benutzer nach Art. 4 zum Zugriff auf die Daten (Stammdaten und Vorgangskategorien) und über die Formen der Bearbeitung der Daten (anzeigen, eingeben, drucken, löschen) zu erlassen. Für jede Vorgangskategorie ist die Zugriffsberechtigung besonders festzulegen (Art. 5 Abs. 3 ISIS-Vo). Ebenso hat das Departement Weisungen über das gleichzeitige Abfragen von mehreren Suchbegriffen (Art. 8 Abs. 2 ISIS-Vo), über die Aufbewahrungsdauer der einzelnen Datenkategorien (Art. 13 Abs. 3 ISIS-Vo) und über die organisatorischen und technischen Massnahmen gegen unbefugtes Bearbeiten der Daten sowie über die automatische Protokollierung der eingegebenen Daten (Art. 20 Abs. 2 ISIS-Vo) zu erlassen. ISIS-Daten dürfen weder über Kommunikationseinrichtungen noch mittels Datenträger in andere Datenbanken kopiert werden (Art. 11 ISIS-Vo). Der Chef der BuPo trägt die Verantwortung für ISIS. Der zuständige Dienst des Rechenzentrums EJPD ist für den technischen Unterhalt und die Sicherheit sowie für die Einhaltung der Zugriffsberechtigungen verantwortlich (Art. 23 Abs. 1 und 2 ISIS-Vo).

331.3 Weisung über das provisorische Staatsschutz-Informations-System (ISIS-Weisung EJPD vom 31.8.1992)

In der ISIS-Weisung des EJPD vom 31.8.1992 sind die Grundlagen über die Dateneingabe, Qualitätskontrolle, Datenkategorien und Zugriffsberechtigungen, Protokollierung, Datensicherheit und weitere Punkte enthalten. Für die Frage eines Online-Anschlusses sind diese Weisungen nur am Rande von Interesse. So enthält Art. 3 Abs. 2 Buchstabe d eine Präzisierung hinsichtlich der Abfrage von Datenkategorien für das angeschlossene Bundesamt für Polizeiwesen. Der Bundesanwalt oder der Chef BuPo können danach dem BAP die Abfrage von Kurzpersonalien in den Datenbanken STA und NSS erlauben. Der Direktor des BAP bestimmt in Absprache mit dem

Bundesanwalt, welche Bediensteten Daten direkt abfragen dürfen. Abfragen, bei denen mehr als drei Suchbegriffe innerhalb eines Datenfeldes gleichzeitig verwendet werden, bedürfen der vorgängigen Zustimmung des Chefs der BuPo oder seiner Stellvertreter unter Angabe des Ziels der Abfrage und der Dauer der Bewilligung (Art. 4 Abs. 2). Im Zusammenspiel mit den datenliefernden Dienststellen von Bund und Kantonen ist auch Art. 7 von Interesse. Danach teilt der Kontrolldienst der BuPo die Löschung der Daten im ISIS zwecks Vernichtung der parallel geführten Daten und Akten der datenliefernden Dienststelle mit (Art. 7). Aus der Verordnung über die Bearbeitung von Personendaten im präventiven Staatsschutz (Datenschutz-Verordnung-Staatsschutz) ergibt sich für die Bearbeitung von Personendaten durch die kantonalen Staatsschutzorgane die Ergänzung, dass die Kantone die bei ihnen aufbewahrten Staatsschutzakten (Akten der Bundesanwaltschaft) gegen Zugriff durch Unbefugte schützen. Die Daten und Akten sind getrennt von den übrigen polizeilichen Informationen aufzubewahren. Daten auf elektronischen Datenträgern sind zu sichern. Der Zugriff auf die Daten und Akten ist durch die Kantone zu regeln (Art. 5 Abs. 2 Datenschutz-Vo Staatsschutz). Die Kantone vernichten für den eidgenössischen Staatsschutz unnötig gewordene Daten auf Mitteilung der Bundespolizei (Art. 5 Abs. 4 Datenschutz-Vo Staatsschutz).

331.4 Musterreglement EDV-Betriebsordnung für Kantone

Die BuPo hat bereits im April 1994 ein Musterreglement „EDV-Betriebsordnung“ für die Kantone erarbeitet und dabei die obgenannten Grundsätze für die Zusammenarbeit zwischen Bund und Kantonen im Bereich der eidgenössischen Staatsschutzaufgaben geregelt. Anhand des konkreten Beispiels der „EDV-Betriebsordnung des Spezialdienstes der Kantonspolizei Luzern für das Projekt INSEL“ vom 23.8.1994 können diese Grundsätze dargestellt werden.

In der Betriebsordnung wird festgehalten, dass das mit eidgenössischen Staatsschutzaufgaben betraute kantonale Organ (konkret: „Spezialdienst der Kantonspolizei Luzern“) ein automatisiertes Informationssystem „INSEL“ betreibt. Im Projekt INSEL werden die

a) Daten aus Strafverfahren in Bundeszuständigkeit,
b) Daten des eidgenössischen präventiven Staatsschutzes,
c) Daten in Erfüllung kantonaler Staatsschutzaufgaben im Zusammenhang mit dem Generalauftrag der Schweizerischen Bundesanwaltschaft,

bearbeitet. Die Daten des eidgenössischen (präventiven und repressiven) Staatsschutzes werden in einer Datenbank und getrennt von den anderen Daten bearbeitet. Auch die dazugehörige Geschäftskontrolle ist getrennt von der Staatsschutzdatenbank zu führen. Die generelle Berechtigung zum Zugriff auf die Datenfelder mit allgemeinen Informationen (Stammdaten; Art. 3 Abs. 2 Musterreglement) ist in einem separaten Anhang 1 geregelt. Die Daten des eidgenössischen Staatsschutzes dürfen weder über Kommunikationseinrichtungen noch mittels Datenträger in andere Datenbanken kopiert werden. Nach der Löschung eines ganzen Datensatzes sind die zugehörigen Akten zu vernichten. Die Archivierung der Staatsschutzakten obliegt der Bundesanwaltschaft. Der Spezialdienst der Kantonspolizei Luzern, der Polizei-Kommandant, der Departementsvorsteher sowie der Datenschutzbeauftragte des Kantons Luzern tragen die Verantwortung für die Datenbearbeitung im „Projekt INSEL“. Die EDV-Betriebsordnung ist vom damaligen Kommandanten der Kantonspolizei unterzeichnet. Das EJPD genehmigte das EDV-Betriebsreglement am 23.8.1994.

332 IST-Situation Online-Verbindungen

Benutzerzahl

Gemäss chronologischer Auflistung über die Online-Verbindungen ISIS (undatiert), deren Aktualität anlässlich der Befragung vom 11. Februar 1998 vom Vertreter der Schweizerischen Bundespolizei (BuPo) bestätigt wurde, sind seit Dezember 1993 bis heute insgesamt

200 Benutzer

an ISIS angeschlossen worden.

Benutzerkategorien

Alle angeschlossenen Benutzer legitimieren sich über die ISIS-Vo (Art. 4 Abs.1, Abs. 2 Bst. a, b und c sowie Art. 4 Abs. 3 ISIS-Vo) zur Nutzung von ISIS. **Es sind ausschliesslich Bundesverwaltungsstellen an ISIS angeschlossen. Ein Online-Anschluss von kantonalen Stellen (ISIS-Plus) ist bisher noch nicht erfolgt** (vgl. dazu auch Ziffer 337 nachfolgend). Das Informationssystem ISIS ist primär ein BuPo-internes System und wird dort bei der Bundespolizei (102 Anschlüsse), bei der Bundesanwältin und ihrem Substitut (2 Anschlüsse), im Rechtsdienst (5 Anschlüsse), bei den Zentralen Diensten (8 Anschlüsse) und im Sicherheitsdienst der Bundesverwaltung (7 Anschlüsse) eingesetzt. Als einzige BuPo-externe Verwaltungsstelle des Bundes ist das BAP angeschlossen. Es sind gemäss Dokumentation des Kontrolldienstes der BuPo vom 11.2.1998 insgesamt 76 Personen des BaP (50 Personen Zentralstellendienste; 26 Personen Interpoldienst) an ISIS angeschlossen. Die Zugriffsberechtigungen sind gestützt auf Art. 5 Abs. 3 ISIS-Vo durch die Weisung des EJPD über das provisorische Staatsschutz-Informations-System (ISIS-Weisung) vom 31.8.1992 (insbesondere in Anhang 2) festgelegt.

Im Speziellen gilt, dass sogenannte permanente ISIS-Aussenterminals der Bundespolizei in den Städten Basel, Freiburg, Genf und Zürich existieren. Diese sind gemäss Angaben der BuPo vom 19.2.1998 (Nachreichung von Unterlagen an den Experten) jeweils in Gebäuden der kantonalen Polizeikommandos untergebracht. Die Verbindungen an diese Aussenstellen erfolgen über Standleitungen direkt zur jeweiligen Anlage und die Datenübertragung wird mit einem sogenannten Greta-Coder verschlüsselt. Die Arbeitsstationen sind in abgeschlossenen Räumen installiert und strikt dem Zugriff durch Bedienstete der Bundespolizei vorbehalten. **Drittanschlüsse ausserhalb der Bundesverwaltung existieren nicht**. Im Falle von speziellen Bedrohungslagen wird für kurze Zeitspannen ISIS auch allfälligen kantonalen Polizeibeamten zur Verfügung gestellt, welche Staatsschutzaufgaben des Bundes übernehmen oder unterstützen (vgl. dazu ausführlich Ziffer 3.3.6).

Netzinfrastruktur und Sicherheitsmassnahmen

Alle angeschlossenen Verbindungspartner kommunizieren über bundeseigene Netzinfrastrukturen (LIS/EJPD). Die Kommunikation findet über TCP/IP statt (standardisierte Kommunikationsprotokolle). Die BuPo selber ist mit einer Karl-Bridge innerhalb des LIS abgeschottet, das Bundesamt für Polizeiwesen erhält die Daten End to End-verschlüsselt mittels Kryptobox auf einer Punkt-zu-Punkt-Leitung.

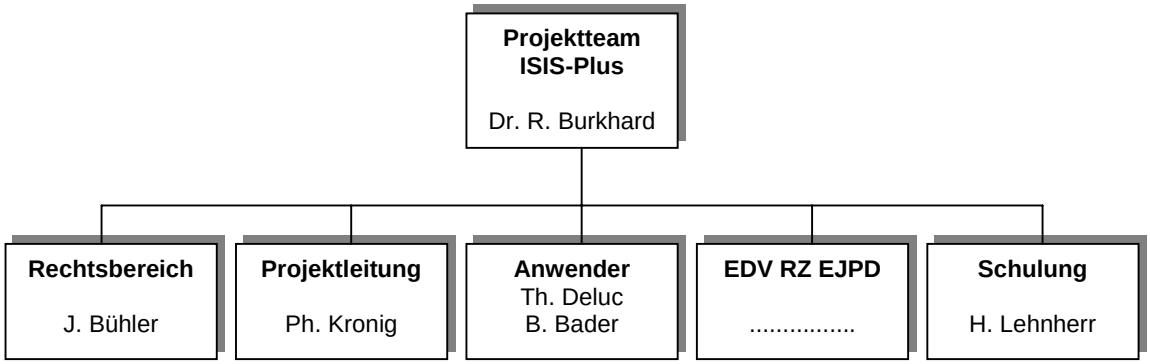
333 Anschlussverfahren

Da an ISIS derzeit nur der Datenherr selber (BuPo) sowie das Bundesamt für Polizeiwesen angeschlossen sind, stellt sich die Frage nach der Praxis bezüglich Online-Anschlüssen (noch) nicht im gleichen Ausmass wie bei den anderen Informationssystemen im Polizeiwesen. Das BAP wurde aufgrund von Art. 4 Abs. 3 ISIS-Vo und Art. 3 Abs. 2 Buchstabe d der ISIS-Weisung (Departement) an ISIS angeschlossen. Ausdrücklich festgelegt ist in der ISIS-Weisung, dass der Direktor des BAP in Absprache mit dem Bundesanwalt bestimmt, welche Bediensteten Daten direkt aus ISIS abfragen dürfen.

Im Hinblick auf die Erweiterung der Nutzung von ISIS und der erheblichen Ausdehnung der Benutzerkategorien auf die Staatsschutzorgane der Kantone und Städte (ISIS-Plus) muss das Online-Anschlussverfahren geregelt werden (vgl. dazu Ziffer 339).

334 Betrieb und Unterhalt

Der zuständige Dienst des Rechenzentrums EJPD ist für den technischen Unterhalt und die Sicherheit sowie für die Einhaltung der Zugriffsberechtigungen verantwortlich (Art. 23 Abs. 2 ISIS-Vo). Daneben besteht derzeit eine eigene Projektorganisation für die Vorbereitung des Anschlusses von Kantonen und Städten an ISIS im Projekt ISIS Plus. Dieses Projektteam erarbeitet das Konzept für die Projekterweiterung und die Anpassungen der Rechtsgrundlagen (vgl. Ziffer 337; Entwicklungsperspektiven).



335 Kostenbeteiligungen

Diese Frage ist derzeit nicht relevant, da das Informationssystem ISIS ausschliesslich für die Bundesstellen betrieben wird. Es steht noch nicht fest, welche Regelung für die Kostenbeteiligung seitens der Kantone/Städte für die Nutzung von ISIS vorgesehen wird. Immerhin schafft das BWIS in Art. 28 eine gesetzliche Grundlage, die Kantone für ihre in diesem Zusammenhang erbrachten Leistungen zu entschädigen. Für die Informatik-Kosten beim Aufbau und Betrieb von ISIS (PLUS) dürften diesselben Ueberlegungen wie bei RIPOL und DOSIS massgeblich sein. Zentrale Informationssysteme des Bundes werden solange von den Kantonen unterstützt und mitbetrieben, als sie nicht mit Kosten für den Aufbau und Betrieb des Informationssystems belastet werden. Dies gilt im Bereich ISIS natürlich speziell, werden doch hier durch das automatisierte Informationssystem vornehmlich Bundesaufgaben unterstützt. Aus dem Bericht der Bundesanwaltschaft und des Rechenzentrums EJPD vom 13.5.1996 zu Erweiterungen des ISIS (externe Anschlüsse der Kantone [ISIS Plus]) ist ansatzweise ersichtlich, dass die Kosten für die

notwendige Infrastruktur von den Kantonen und Städten, für Unterhalt und Reparatur vom Bund (Bundesanwaltschaft) getragen werden sollen (Bericht Seite 3).

336 Kantone und andere bundesverwaltungsexterne Anschlüsse

Wie in Ziffer 332 dargestellt, sind derzeit ausschliesslich Bundesstellen an ISIS angeschlossen. Im Falle von speziellen Bedrohungslagen werden aber für festgelegte Zeitspannen kantonale Polizeistellen, welche Staatsschutzaufgaben des Bundes übernehmen oder unterstützen, an ISIS angeschlossen.

Anhand des von der BuPo zuhanden des Experten dokumentierten zeitlich befristeten Anschlusses der Staatsanwaltschaft Basel-Stadt während der Erinnerungsfeier an den 1. Zionistenkongress in Basel von 1897, die vom 25. - 31. August 1997 in Basel stattfand, kann der vorübergehende Online-Anschluss kantonaler Polizeibehörden an ISIS dargestellt werden.
Auf Bundesebene koordiniert die BuPo die Beschaffung bedrohungsrelevanter Informationen und führt zwecks laufender Erarbeitung der Bedrohungslage zuhanden der verantwortlichen Behörden ein Lagezentrum. Hierfür benützt die BuPo vorallem auch ISIS. Die zeit- und bedürfnisgerechte Abfrage von Daten aus ISIS machte im Falle der Erinnerungsfeier an den 1. Zionistenkongress auch einen Online-Anschluss direkt in Basel notwendig. Zur Gewährleistung einer lückenlosen Abfragemöglichkeit in Basel war die personelle Unterstützung durch die Staatsanwaltschaft Basel-Stadt notwendig. In einer speziellen schriftlichen Vereinbarung der Schweizerischen Bundesanwaltschaft (Bundespolizei) und der Staatsanwaltschaft des Kantons Basel-Stadt wurden in der Folge für den Zeitraum vom 25.6. - 2.9.1997 alle wesentlichen Zusammenarbeits- und Zugriffsregelungen festgelegt. So umschreibt die genannte Vereinbarung

- Namentlich und abschliessend alle zugriffsberechtigten Polizeibeamtinnen und Polizeibeamten des Kantons Basel-Stadt,
- Die Zuständigkeit der BuPo zur Festlegung des Umfangs der Zugriffsrechte dieser Polizeibeamten,
- Die Instruktion der genannten Polizeibeamten durch die BuPo,
- Das Verbot zur selbständigen Weitergabe von abgefragten Daten an Dritte,
- Die Verpflichtung der genannten Polizeibeamten zur Unterzeichnung einer Verschwiegenheitserklärung,
- Die Unterstellung der genannten Polizeibeamten unter die Weisungs- und Befehlsgewalt des Chefs der BuPo für die Dauer ihrer Einsätze,
- Das massgebliche Disziplinarrecht und die übrigen beamtenrechtlichen Verhältnisse.

Mittels speziellem Formular (ISIS Account Antrag) vom 15.7.1997 wurden seitens des Stellvertreters des Chefs der Bundespolizei zuhanden des systemverantwortlichen Supervisors die detaillierten Zugriffsrechte (beschränkt im konkreten Falle auf "abfragen") festgelegt.

Die Einräumung zeitlich beschränkter Online-Zugriffe an kantonale Polizeibeamte mit Staatsschutzaufgaben ist durch dieses Vorgehen zweckmässig und transparent nachvollziehbar institutionalisiert. Die Aufgaben, Kompetenzen und Verantwortung sind in der genannten Vereinbarung klar geregelt. Was hingegen fehlt ist die Festlegung dieses Online-Bewilligungsverfahren in verbindlicher und schriftlicher Form in einem geeigneten Erlass (Verordnung, Weisung, o.a.). Nur dadurch wird sichergestellt, dass die Einräumung zeitlich beschränkter Online-Anschlüsse an kantonale Polizeibehörden, welche vorübergehend Staatsschutzaufgaben des Bundes wahrnehmen, immer nach dem gleichen Verfahren und gestützt auf dieselben Unterlagen (Formulare, Checklisten) und Beurteilungskriterien (Zweckmässigkeit, Verhältnismässigkeit, Notwendigkeit) erfolgt. Wie im Bereich anderer Informationssysteme im Polizeiwesen bereits festgestellt, fällt auch im Bereich ISIS auf, dass die

direkt interessierte und betroffene Verwaltungsstelle des Bundes für ihre eigenen Zwecke, Bedürfnisse und Aufgaben den Online-Anschluss eines Dritten bewilligt. Eine unabhängige Bewilligungsinstanz existiert nicht.

337 Entwicklungsperspektiven

Rechtsetzungsebene
Im Zusammenhang mit der Ausführungsgesetzgebung zum BWIS besteht die Vorgabe, die Verordnung über das informatisierte Staatsschutz-Informationssystem (ISIS-Verordnung) zu revidieren. In diesem Erlass sollen auch die Ausführungsbestimmungen zum Anschluss der Kantone ans Informationssystem ISIS-Plus geregelt werden. Die entsprechende Planung im EJPD sieht vor, alle auf das BWIS gestützten Ausführungserlasse in einem Paket in den Bundesrat zu bringen, damit der Komplex Staatsschutzgesetzgebung bestenfalls auf den 1. Oktober 1998 in Kraft gesetzt werden kann. Diese Vorgabe bedingt gemäss den zuständigen Planungsbeauftragten in der BuPo die Ausarbeitung der ISIS-Verordnung sowie interne Konsultationen bis Ende Mai 1998, externe Konsultationen (z.B: EDSB) und allfällige Ueberarbeitungen bis Ende Juni 1998 sowie die Aemterkonsultation und Anpassungsarbeiten bis August 1998 (Schreiben BuPo vom 19.2.1998).

Informatikebene
Bereits im Aktionsprogramm „Innere Sicherheit“ 1994 war vorgesehen, die Kantone an ISIS anzuschliessen. Im BWIS wurde die gesetzliche Grundlage für den Anschluss anderer Polizei- und Strafverfolgungsbehörden des Bundes sowie der Sicherheitsorgane der Kantone über ein Abrufverfahren (Art. 15 Abs. 3 BWIS) geschaffen. Erst ein Anschluss der Kantone an ISIS ermöglicht es nach Meinung der BuPo und der Bundesanwaltschaft, dass diese auf eigene Registraturen im Staatsschutzbereich verzichten können. Nur so könne die Gefahr der Vermischung kantonaler Daten mit Daten des Bundes verringert werden. Die Konferenz der kantonalen Polizeikommandanten und mehrere Polizeikommandanten haben in Einzelvorstössen in den letzten Jahren gefordert, dass der Anschluss ihrer Spezialdienste an das ISIS raschmöglichst erfolge (EJPD-interner Entwurf an den Bundesrat zur Revision ISIS-Verordnung vom 22.10.1996). Gestützt auf den Grobkonzeptbericht zur Erweiterung von ISIS vom 13.5.1996 ergibt sich, dass unter ISIS-Plus der versuchsweise Anschluss von 9 Kantonen und Städten (Staatsanwaltschaft Basel-Stadt, Polizeikorps der Kantone Freiburg, Genf, Luzern, St. Gallen, Tessin, Waadt und Zürich sowie der Stadt Bern) an das bestehende ISIS, insbesondere auch der Zugang zu den Teilsystemen Staatsschutz (STA), nicht staatsschutzrelevante Strafverfahren (NSS) und Dokumentation (DOK) vorgesehen ist. Mit Hilfe der bestehenden Benutzerverwaltung soll eine selektive Zugriffsregelung gewährleistet werden. Die Datenerfassung und Datenkontrolle wird wie bis anhin durch die Bundesanwaltschaft (Vorauswertung und Kontrolldienst) sichergestellt. Den Kantonen und Städten ist das Verändern von Daten nicht erlaubt. Die Uebertragung der Daten erfolgt wiederum über das EJPD WAN in die lokalen LAN-Netze über TCP/IP zu den berechtigten Arbeitsstationen. Total sollten rund 50 Mitarbeiter der Kantone angeschlossen werden. In organisatorischer Hinsicht ist vorgesehen, dass die Verantwortung für ISIS weiterhin beim Chef der Bundespolizei bleibt. Der Zugriff soll in der ISIS-Vo und in der ISIS-Weisung geregelt werden, weshalb diese beiden Erlasse anzupassen sind. Im Rahmen der Sicherheitsmassnahmen wird ausdrücklich vorgesehen, dass ein vom Polizeikommandanten und dem Chef der Bundespolizei unterschriebener ISIS-Plus Zugangs-Antrag die Zugriffsberechtigung der einzelnen Benutzer auf die Teilsysteme regeln soll.

Durch Vorentscheid des Departementsvorstehers EJPD im November 1996 ist der Anschluss weiterer Organe der Kantone und Städte noch vor Inkrafttreten des BWIS vorerst zurückgestellt worden. Dieser Aufschub hängt seinerseits zusammen mit dem Zuwarten der Inkraftsetzung des BWIS durch den Bundesrat bis zur Volksabstimmung über die Initiative „SOS“ (vgl. Ziffer 3.3.1).

338 Zusammenfassung und Bewertung

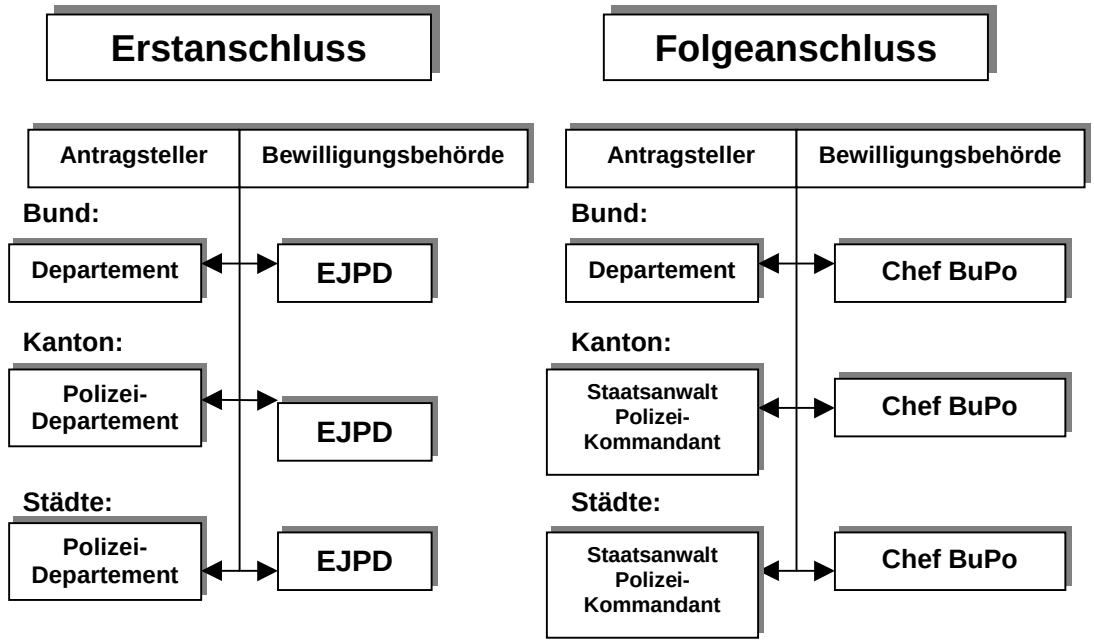
1. Das Informationssystem ISIS wird innerhalb der Bundesverwaltung primär von der Bundespolizei als Datenherr selber genutzt. Die BuPo betreibt vier Aussenstellen in den Städten Basel, Freiburg, Genf und Zürich. Dabei handelt es sich um Online-Verbindungen, die Nutzung erfolgt jedoch ausschliesslich durch Bedienstete der Bundespolizei. Als einziger externer Systemnutzer hat das BAP mit 76 Benutzern Zugriff auf ISIS. Andere Bundes- oder Kantonsorgane sind derzeit nicht permanent an ISIS angeschlossen.

2. Für die zuständigen Bundesorgane stellt sich erst nach Inkrafttreten des BWIS die konkrete Frage bezüglich Bewilligungspraxis und Online-Anschlussverfahren. Erste Anschlüsse dürften voraussichtlich Ende 1998 oder anfangs 1999 nach Inkrafttreten der entsprechenden Ausführungsbestimmungen zum BWIS realisiert werden. Es besteht damit im sensiblen Bereich ISIS die Chance, von Anfang an die Aufgaben, Kompetenzen und Verantwortlichkeiten sowie das Verfahren und die im Rahmen eines Online-Anschlusses zu prüfenden Fragen klar zu definieren.

3. Wie in den anderen Bereichen der polizeilichen Informationssysteme gilt es auch im Bereich ISIS zu berücksichtigen, dass die in übergeordneten Erlassen (Gesetz, Verordnung) aufgestellten Grundsätze für Online-Anschlüsse durch eine immer weiter nach unten delegierte Verantwortung verloren zu gehen drohen, indem durch die Delegation von Online-Bewilligungen auf die Anwendungsebene andere Interpretationen und Interessen den ursprünglichen Gesetzgeberwillen aushöhlen können. Zudem kann dadurch ein Interessenkonflikt (gleichzeitig Systembetreiber, Informationsbearbeiter, Bewilligungsinstanz) entstehen. Diese Grundsätze können aufgrund der steten Weiterdelegation sowie der Festschreibung in verschiedenen Erlassen in der Einzelfallanwendung (Bewilligungserteilung) auf unterster Verwaltungsstufe damit letztlich auch unbeachtet bleiben. Es ist angezeigt, dass die für einen Online-Anschluss relevanten Entscheidungskriterien, das Verfahren, die Zuständigkeiten konzentriert und von entsprechend übergeordneter Verwaltungsstufe einheitlich festgelegt werden. Dies ist insbesondere auch deshalb notwendig, weil für zeitlich beschränkte Online-Anschlüsse von kantonalen Polizeibehörden, welche vorübergehend Staatsschutzaufgaben des Bundes wahrnehmen, heute bereits ein BuPo-internes Verfahren existiert und angewendet wird, in welchem keine unabhängige Stelle den Online-Anschlussantrag prüft und bewilligt.

4. Das Bewilligungsverfahren für den Online-Anschluss von Staatsschutzorganen der Kantone und Städte ist für den Zeitpunkt des Inkrafttretens des BWIS und der Erweiterung der Systemnutzung durch diese Staatsschutzorgane noch nicht geregelt. Die entsprechenden Arbeiten sind im Rahmen der Verordnungsanpassungen derzeit im Gang. Zu beachten ist dabei, dass im Bereich ISIS sehr strenge Anforderungen an die Benutzer der Bundesverwaltung gestellt werden. Es werden auch besonders schützenswerte Daten gespeichert und bearbeitet. Aufgrund dieser Ausgangslage rechtfertigt es sich, die politischen Behörden (Polizeidirektoren der Staatsschutzorgane von Kantonen und Städten) direkt in das Bewilligungsverfahren für einen Erstanschluss auf Kantons- und Städteebene einzubeziehen. Art. 7 Abs. 3 und 4 BWIS könnte insoweit ergänzt werden, als für Erstanschlüsse von externen Staatsschutzorganen des Bundes, der Kantone oder der Städte auf der Antragstellerseite die politischen Verantwortungsträger (Bund: Departementsvorsteher; Kantone und Städte: Polizeidirektoren) eingebunden werden müssen, auf der Entscheidseite eine unabhängige Bewilligungsinstanz (Z.B: Generalsekretariat EJPD) vorzusehen wäre. Die gestützt auf einen Erstentscheid zusätzlich zu realisierenden Folgeanschlüsse könnten

alsdann vom verantwortlichen Chef der BuPo (als Datenherr und oberster Verantwortlicher des Informationssystems ISIS) auf Antrag des zuständigen Polizeikommandanten oder Staatsanwalts bewilligt werden.



5. Die Staatsschutzorgane der Kantone und Städte müssen über entsprechende EDV-Betriebsordnungen, welche vom EJPD (Art. 16 Abs. 2 und 3 BWIS) zu genehmigen sind, an dieselben strengen Benutzungsbedingungen gebunden werden, wie sie für die Anwender in der Bundesverwaltung gelten. Die von der BuPo bereits erarbeitete Muster-EDV-Betriebsordnung ist ein sehr guter Ausgangspunkt. Es wird für die Durchsetzung der darin gegenüber den Staatsschutzorganen der Kantone und Städte festgelegten Grundsätze nach Inkrafttreten des BWIS eine genügende gesetzliche Grundlage (Art. 16 Abs. 2 BWIS) geben. Es zeigt sich, dass über solche EDV-Betriebsordnungen die Minimalstandards der Bundesvorgaben vom Datenherr und Informationssystem-Betreiber gegenüber dem externen Benutzer durchgesetzt werden können, wenn der Gesetzgeber dies ausdrücklich vorsieht.

6. In den Kantonen bestehen offensichtlich zum Teil separate automatisierte Informationssysteme im Bereich des eidgenössischen (präventiven und repressiven) Staatsschutzes und im Bereich Strafverfahren in Bundeszuständigkeit. Diese Systeme sind in zweierlei Hinsicht von Interesse. Einerseits werden hier parallel zum ISIS staatsschutzrelevante Informationen in dezentralen kantonalen Informationssystemen bearbeitet, ohne dass eine direkte Online-Verbindung zum ISIS besteht. Das führt zu Datenredundanzen zwischen den Staatsschutzorganen des Bundes und der Kantone mit der Gefahr, dass die Daten in den verschiedenen Systemen (ISIS, Kantonssysteme) nur mit grossem Aufwand aktuell gehalten und aufeinander abgestimmt werden können. Die Löschung der Daten auf den dezentralen Systemen auf Anordnung der Bundespolizei ist andererseits mit einem erheblichen Kontrollaufwand seitens der Bundespolizei verbunden, müssen doch die Daten des eidgenössischen Staatsschutzes und die Daten aus Bundesstrafverfahren nach Aufforderung durch die Bundespolizei oder nach Ablauf ihrer Aufbewahrungsdauer von den kantonalen Instanzen selbständig gelöscht werden (Art. 15 ISIS-Vo und Art. 7 ISIS-Weisungen). Aufgrund der Interview-Ergebnisse vom 11. Februar 1998 mit der

Bundespolizei muss davon ausgegangen werden, dass derzeit niemand die Einhaltung all dieser in den konkreten EDV-Betriebsordnungen für die kantonalen Spezialdienste festgehaltenen Grundsätze überprüfen kann. Der Hauptgrund liege darin, dass zuwenig Personal für diese Kontrollaufgabe zur Verfügung stehe (Befragungsnotiz Experte vom 11.2.1998). Diese Tatsache ist insofern bedenklich, als auf Stufe Bund sehr restriktive Regelungen für die Benutzung von ISIS bestehen. In den Kantonen werden ebenfalls Daten von Staatsschutzrelevanz bearbeitet und gespeichert. Die Einhaltung der restriktiven Regelungen (insbesondere auch die Löschung auf Anordnung der BuPo) auf Kantonsebene ist aber nicht sichergestellt, obwohl hier ebenfalls Bundesaufgaben wahrgenommen werden.

Mit der Anbindung der Staatsschutzorgane der Kantone und Städte an das Informationssystem ISIS über entsprechende Online-Anschlüsse wird eine Konzentration der Daten in einem einzigen System ermöglicht. Dies reduziert den Kontrollaufwand, wenn die dezentralen Systeme in den Kantonen keine Daten im Bereich Staatsschutzaufgaben mehr enthalten. Ebenso dürfte dadurch auch die Ueberprüfung der Einhaltung von Datenschutzbestimmungen vereinfacht werden, da der Zugriff und die Abfrage auf diese Daten einheitlich und zentral geregelt und verwaltet werden können. In diesem Sinne ist eine zügige Realisierung von Online-Anschlüssen von Organen der Kantone und Städte, welche Staatsschutzaufgaben des Bundes wahrnehmen, unter gleichzeitigem Abbau und Löschung der vorhandenen dezentralen Staatsschutzinformationen zu unterstützen.

7. Die Regelung in Art. 3 Abs. 2 Buchstabe d ISIS-Weisung EJPD, wonach der Direktor des BAP in Absprache mit dem *Bundesanwalt* bestimmt, welche Bediensteten des BAP Daten direkt abfragen dürfen, ist zumindest unpräzise. Als Datenherr kann aufgrund der geltenden Gesetzesgrundlagen nur der eigentlich Verantwortliche, im konkreten Fall der Chef der Bundespolizei (Art. 23 Abs. 1 ISIS-Vo) über Anschlüsse befinden. Er trägt die Verantwortung, während der Bundesanwalt die Aufsicht wahrnimmt. Innerhalb von ISIS ist der Bundesanwalt lediglich Benutzer von ISIS (Art. 4 Abs. 2 ISIS-Vo). Er kann also nicht als Benutzer über die definitiven Anschlussbewilligungen entscheiden. Auch der Direktor des BAP kann nicht „bestimmen“, welche Bediensteten des BAP Daten direkt abfragen dürfen. Er kann im Rahmen seiner Zuständigkeit höchstens BAP-intern jene Mitarbeiter bestimmen, für welche ein Antrag bei der BuPo für einen Online-Anschluss eingereicht wird. Die Voraussetzungen für den Anschluss und die Bewilligung zur Nutzung von ISIS-Daten sind allein vom Chef BuPo zu prüfen resp. zu erteilen. In diesem Sinne sollte Art. 3 Abs. 2 Buchstabe d der ISIS-Weisungen des EJPD präzisiert werden, wobei insbesondere zusätzlich die Ausführungen hinsichtlich unabhängiger Bewilligungsinstanz (Ziffer 3.3.8, Lit. c) einzubeziehen sind.

8. Während in anderen Bereichen (RIPOL; DOSIS) auf Verordnungsstufe die Finanzierung und Kostenbeteiligung zwischen Bund und Kantonen geregelt ist, fehlen bisher differenzierte Bestimmungen hierzu im Bereich ISIS. Auf Gesetzesstufe regelt BWIS in Art. 28 nur die Abgeltung der von den Kantonen im Auftrag des Bundes erbrachten Leistungen. In der laufenden Ueberarbeitung und Anpassung der ISIS-Verordnung an das BWIS sind die Finanzierungsfragen zu regeln. Dabei sind die Erkenntnisse aus dem VKB-Bericht (a.a.O., S. 30 ff.) in eine entsprechende Finanzierungsregelung miteinzubeziehen und die heute bereits geltenden Grundsätze (Art. 22 RIPOL-Vo; Art. 20 DOSIS-Vo) wenn immer möglich analog anzuwenden.

339 Empfehlungen und Massnahmenvorschläge

1. Das EJPD hat für den Online-Anschluss von Staatsschutzorganen des Bundes, der Kantone und Städte die Aufgaben, Kompetenzen und Verantwortlichkeiten (Bewilligungsbehörden), das Verfahren (Bewilligungsverfahren und Antragsteller), die zu prüfenden Anschlusskriterien (Bewilligungsgründe), die minimalen Anforderungen an die Dokumentation (formeller Bewilligungsentscheid) und die Ablage (Bewilligungsarchivierung) festzulegen. Dabei ist eine verantwortungs- und stufengerechte Zuordnung der Bewilligungskompetenz vorzusehen, indem beispielsweise für Erstanschlüsse von externen Staatsschutzorganen des Bundes, der Kantone oder der Städte auf der Antragstellerseite auch der politische Verantwortungsträger (Polizeidirektoren), auf der Entscheidseite eine unabhängige Bewilligungsinstanz bestimmt werden. Dazu empfiehlt sich die Festlegung und Durchsetzung einheitlicher Prozessablaufbeschreibungen gegenüber allen Amtsstellen, welche im Bereich Online-Anschlüsse im Polizeiwesen betroffen sind (vgl. Beispiele im Bericht).

2. Die dezentralen Informationssysteme von Kantonen oder Städten im Bereich Staatsschutz sind zügig durch Online-Anschlüsse an ISIS abzulösen und die dezentralen Staatsschutzdatenbestände - soweit vorhanden - zu löschen.

3. Das EJPD hat gestützt auf Art. 16 Abs. 2 BWIS die bestehende Muster-EDV-Betriebsordnung für kantonale oder städtische Staatsschutz-Informationssysteme im Bereich ISIS zu überarbeiten und an die neuen Vorgaben von BWIS anzupassen.

4. Das EJPD hat im Rahmen der Anpassung der ISIS-Vo an BWIS auch die Frage der Finanzierung und Kostenbeteiligung zwischen Bund und übrigen Staatsschutzorganen (Kantone und Städte) zu regeln.

5. Das EJPD hat die ISIS-Weisungen in Art. 3 Abs. 2 Buchstabe d im Sinne der obigen Ausführungen unter Ziffer 3.3.8 Buchstabe g zu präzisieren.

34 ZAR

341 Gesetzliche Grundlagen und Grundsätze

Aufenthalt und Niederlassung von Ausländern

a) Bundesgesetz über Aufenthalt und Niederlassung der Ausländer vom 26. März 1931 (ANAG mit Aenderung Stand 11.11.1997; SR 142.20),
b) Vollziehungsverordnung zum Bundesgesetz über Aufenthalt und Niederlassung von Ausländern vom 1. März 1949 (ANAV mit Aenderung Stand 1.10.1996; SR 142.201),
c) Verordnung über Einreise und Anmeldung von Ausländerinnen und Ausländern vom 14.1.1998 (mit Aenderungen Stand 3.2.1998; SR 142.211),
d) Verordnung über die Meldung wegziehender Ausländer vom 20. Januar 1971 (mit Aenderungen Stand am 1.10.1996; SR 142.212),
e) Verordnung über das Zentrale Ausländerregister vom 23. November 1994 (mit Aenderungen Stand am 1.4.1996; SR 142.215),
f) Weitere Verordnungen ohne direkten Bezug zur Fragestellung Online-Anschlüsse (SR 142.241; SR 142.281; SR 142.291; SR 143.5 und SR 823.21).

Daraus ergeben sich zusammengefasst folgende Grundsätze:

341.1 Bundesgesetz über Aufenthalt und Niederlassung der Ausländer

In Art. 25 ANAG hat der Gesetzgeber dem Bundesrat im Rahmen der Uebergangs- und Schlussbestimmungen die Kompetenz eingeräumt, die zur Durchführung des ANAG erforderlichen Vorschriften zu erlassen. Ihm steht die Oberaufsicht über die Handhabung der fremdenpolizeilichen Vorschriften des Bundes zu. Der Bundesrat ist insbesondere befugt,das Zusammenarbeiten der fremdenpolizeilichen mit anderen Behörden, insbesondere mit denen des Arbeitsnachweises, und die Befugnisse des Bundesamtes für Wirtschaft und Arbeit (BWA) gegenüber den kantonalen Arbeitsnachweisen in Fragen des Arbeitsmarktes zu regeln (Art. 25 Abs. 1 Buchstabe d).

Das Bundesamt für Ausländerfragen (BFA) ist für alle keiner anderen eidgenössischen Stelle zugewiesenen fremdenpolizeilichen Obliegenheiten des Bundes zuständig (Art. 15 Abs. 3 ANAG).

Jeder Kanton bezeichnet eine kantonale Fremdenpolizeibehörde. Diese ist zuständig für alle fremdenpolizeilichen Obliegenheiten, die nicht einer Bundesbehörde zustehen oder durch die kantonale Gesetzgebung einer anderen Behörde übertragen werden (Art. 15 Abs. 1 ANAG). Die Kantone erlassen die zur Durchführung dieses Gesetzes auf ihrem Gebiet erforderlichen Vorschriften; sie bezeichnen die zuständigen Behörden und bestimmen deren Befugnisse und Obliegenheiten (Art. 25 Abs. 3 ANAG).

Eine formelle gesetzliche Grundlage für den Aufbau, die Führung und den Anschluss von Verwaltungsstellen des Bundes und der Kantone an ein automatisiertes Ausländerinformationssystem (Zentrales Ausländerregister: ZAR) existiert noch nicht.

Gestützt auf den Bundesbeschluss vom 20.6.1997 wurde das Datenschutzgesetz vom 19.6.1992 in seinem Artikel 38 modifiziert. Der eingefügte Absatz 4 sieht vor, dass im Asyl- und Ausländerbereich die Frist nach Absatz 3 bis zum Inkrafttreten des totalrevidierten Asylgesetzes sowie der Aenderung des Bundesgesetzes über Aufenthalt und Niederlassung der Ausländer verlängert wird (Eingefügt durch Ziff. II des BB vom 20. Juni 1997, in Kraft seit 1. Jan. 1998; AS 1997 2372; BBl 1997 I 877).

341.2 Verordnung über das Zentrale Ausländerregister (ZAR-Verordnung)

Das Bundesamt für Ausländerfragen (BFA) führt in Zusammenarbeit mit den interessierten Bundesstellen und den Kantonen ein automatisiertes Register (Zentrales Ausländerregister ZAR) der Ausländer (Art. 1 ZAR-Vo). Das ZAR hat der Rationalisierung der Arbeitsabläufe, der Kontrolle im Rahmen der Ausländergesetzgebung, der Erstellung von Statistiken über Ausländer und Ausländerinnen sowie in besonderen Fällen der Erleichterung der Amtshilfe zu dienen (Art. 2 ZAR-Vo). Das Bundesamt erhebt entweder selber die zur Aufgabenerfüllung notwendigen Personendaten oder lässt sie durch verschiedene Drittbehörden erheben (Art. 3 Abs. 1 ZAR-Vo). Es sind dies namentlich:

- Kantone und Gemeinden (Art. 4 ZAR-Vo)
- Bundesamt für Polizeiwesen (Art. 5 Abs. 1 Buchstabe a)
- Bundesamt für Flüchtlinge (Art. 5 Abs. 1 Buchstabe b)
- Bundesamt für Wirtschaft und Arbeit (BWA) (Art. 5 Abs. 1 Buchstabe c)
- Bundesamt für Statistik (Art. 5 Abs. 1 Buchstabe d)
- Schweizerische Auslandvertretungen (Art. 5 Abs. 1 Buchstabe e)
- Grenzposten (Art. 5 Abs. 1 Buchstabe f)

Die Personendaten werden über am Rechner angeschlossene Datenendstationen (online), stapelweise auf elektronischen Datenträgern oder schriftlich mit Meldeformularen gemeldet (Art. 6 ZAR-Vo). Das Bundesamt legt fest, unter welchen Voraussetzungen die Personendaten automatisiert gemeldet werden können und wie sie in diesem Falle zu überprüfen (Plausibilitätstests) sind. Es erlässt über die Meldung von Personendaten entsprechende Weisungen (Art. 6 Abs. 2 und 3 ZAR-Vo).

341.3 Die Bekanntgabe von Personendaten im Abrufverfahren

(Art. 7 ZAR-Vo) durch das BFA ist an folgende Behörden zulässig:

Behörde	**Abrufbereich**
Fremdenpolizeibehörden der Kantone und Gemeinden	Ganzer Zuständigkeitsbereich
Beschwerdedienst des EJPD	Beschwerdeinstruktion
Bundesamt für Wirtschaft und Arbeit und **Kantonale und kommunale Arbeitsmarktbehörden**	Aufgaben gemäss Verordnung über die Begrenzung der Zahl der Ausländer
Grenzposten	Durchführung von Personalkontrollen und Erteilung von Ausnahmevisa
Schweizerische Auslandvertretungen	Prüfung von Visumsgesuchen
Zentrale Ausgleichsstelle der AHV	Bildung der AHV-Nr.
Schweizerische Ausgleichskasse	Abklärung der Leistungsgesuche ausgereister Ausländer Berechnung ihnen zustehender Leistungen
Bundesamt für Flüchtlinge	für die Aufgaben nach Asylgesetz
Polizeibehörden der Kantone und Gemeinden	fremdenpolizeiliche Kontrollaufgaben Personenidentifikation bei sicherheits- und kriminalpolizeilichen Ermittlungen
Bundesamt für Statistik	Volkszählung Aufgaben nach Bundesstatistikgesetz
Bundesanwaltschaft 1. Ausländerdienst 2. Bundespolizei	 Handhabung der politischen Fremdenpolizei (Einreisesperren, Ausweisungen) Personenidentifikation bei sicherheits- und gerichtspolizeilichen Ermittlungen

Bundesamt für Polizeiwesen	
1. Sektion Bürgerrecht	Erfüllung der Aufgaben nach Bürgerrechtsgesetz
2. Zentralpolizeibüro	Personenidentifikation im Bereich des interkantonalen und internationalen polizeilichen Nachrichtendienstes (Zentralstellendienste und Interpol)
3. Hauptabteilung internationale Rechts- und Amtshilfe	Personenidentifikation für Auslieferungsverfahren Rechts- und Amtshilfe stellvertretende Strafverfolgung und Strafvollstreckung Kontrolle der RIPOL-Eingaben

341.4 Die Bekanntgabe von Personendaten durch die Kantone und Gemeinden
(Art. 13 ZAR-Vo)

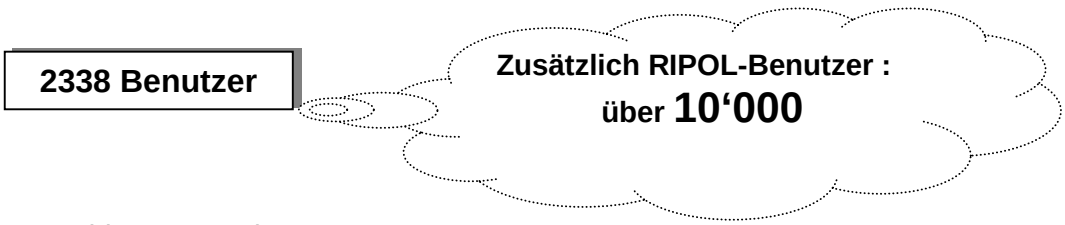
Die genannten Behörden dürfen Personendaten, die im Verfahren nach dem ANAG erhoben oder verwendet werden, anderen Behörden nur bekanntgeben, wenn das Amtsgeheimnis und die kantonalen und kommunalen Vorschriften über den Datenschutz es zulassen und keine schutzwürdigen Interessen des Ausländers oder der Ausländerin beeinträchtigt werden.

341.5 Datensicherheit
(Art. 16 ZAR-Vo)

Alle Behörden, welche mit dem ZAR zusammenarbeiten, treffen in ihrem Bereich die angemessenen organisatorischen und technischen Massnahmen zur Sicherung der Personendaten. Das Bundesamt erlässt Weisungen über die Anforderungen an die Datensicherheit und sorgt für die Koordination gemäss den Empfehlungen des Bundesamtes für Informatik. Personendaten, Programme und Programmdokumentationen sind vor unbefugtem Zugriff, vor unbefugter Veränderung und Zerstörung sowie vor Entwendung zu schützen.

342 IST-Situation Online-Verbindungen

<u>Benutzerzahl</u>
Gemäss chronologischer Auflistung über die Online-Verbindungen ZAR vom 27.1.1998, deren Aktualität anlässlich der Befragung vom 3. Februar 1998 von den Vertretern des Bundesamtes für Ausländerfragen bestätigt wurde, sind seit September 1988 bis heute insgesamt



an ZAR angeschlossen worden.

Zusätzlich sind über 10'000 Benutzer via RIPOL-Anschluss an ZAR angekoppelt (beschränkter ZAR-Zugriff, vgl. Ziffer 316).

Benutzerkategorien

Alle angeschlossenen Benutzer stützen ihre Anschlusslegitimation auf die ZAR-Vo (Art. 1, Art. 7 Abs. 1 und Abs. 2 ZAR-Vo) zur Nutzung von ZAR. Für den Anschluss von 26 Benutzern des Rechenzentrums EJPD wird kein Rechtsgrund aufgeführt. Ein solcher lässt sich denn auch weder aus dem ANAG, noch aus ANAV oder der ZAR-Vo ableiten. Dieser Anschluss ergibt sich allein aus der Tatsache der Pflege, des Betriebs und der Wartung der ZAR-Anwendung. Auch im Anhang 1 (Datenkatalog) ist das RZ EJPD nicht als zugriffsberechtigte Organisationseinheit aufgeführt.

Von der Struktur der Benutzer her betrachtet fällt auf, dass neben den Bundesstellen sowie den kantonalen Fremdenpolizeistellen insbesondere diverse städtische Einwohnerdienste (Städte Bern, Biel, Chur, St. Gallen, Thun, Winterthur, Zürich) und Gemeinden (St. Moritz, Arosa, Polizeiposten Engelberg, städtisches Arbeitsamt Zürich, städtisches Arbeitsamt Winterthur, Chavannes-près-Renens, regionale Fremdenbüros von Bellinzona, Mendrisio, Faido, Gordola, Chiasso, Biasca, Locarno, Magadino, Taverne, Lugano, Cevio, Caslano; Prefecturen von Romont, Murten, Estavayer-le-Lac, Tafers, Châtel-St-Denis, Bulle, Yverdon und Einwohnerkontrollen von Adliswil, Uster und Yverdon) angeschlossen sind. Dabei sind insbesondere im Kanton Tessin sowie im Kanton Freiburg starke Gemeindepräsenzen zu verzeichnen. Mit weiteren Gemeinde-Einwohnerkontrollen sind Online-Anschlüsse geplant, jedoch noch nicht realisiert (Emmenbrücke, Kriens, Fällanden, Köniz, Le Locle, Wettingen). Derzeit sind rund 70 Gemeinden oder Städte mittels Online-Anschluss mit ZAR verbunden (vgl. dazu auch Dokument „Rücklauf der Umfrage Mutationsmeldungen“ des BFA vom 27.1.1998).

Netzinfrastruktur und Sicherheitsmassnahmen

Innerhalb der Bundesverwaltung wird auf den departements- oder bundeseigenen Netzwerkinfrastrukturen zum überwiegenden Teil mit einer End-to-End Software-Chiffrierung gearbeitet. Die Anschlüsse der Kantone erfolgen vom Zentralrechner RZ EJPD aus bis zum kantonalen Knotenrechner (Eintrittspunkt im Kantonshauptort) über das Wide Area Network (WAN) des EJPD unter Einsatz von hardwaremässiger Chiffrierung (Gretacoder oder andere). Die Feinverteilung über die kantonalen Netzinfrastrukturen erfolgt wiederum über End-to-End Software-Chiffrierung.

343 Anschlussverfahren

In Art. 6 ZAR-Vo wird vom Bundesrat festgelegt, dass das Bundesamt (BFA) festzulegen hat, unter welchen Voraussetzungen die Personendaten automatisiert gemeldet werden können und wie sie bei automatisierter Meldung vor der Uebermittlung zu überprüfen sind (Plausibilitätstests). Das BFA hat Weisungen über die Meldung der Personendaten durch die Bundesstellen, Kantone und Gemeinden sowie durch die schweizerischen Vertretungen im Ausland zu erlassen und die Meldeformulare zu genehmigen (Art 6. Abs. 2 und 3 ZAR-Vo).

Das Bearbeitungsreglement des BFA vom 16. November 1995 regelt nähere Einzelheiten im Rahmen der Datenbearbeitung im ZAR. Eine Darstellung des Online-Bewilligungsverfahrens für Neuanschlüsse oder Erweiterungen bestehender Anschlüsse an ZAR ist aber auch im Bearbeitungsreglement nicht explizit dargestellt. Einzelne Grundsätze lassen sich jedoch aus der Projektorganisation ZAR, der Aufgabenumschreibung, den Kontroll- und Zugriffsbestimmungen sowie den Sicherheitsanforderungen ableiten.

343.1 Aufbauorganisation

Das Projekt ZAR bedient sich folgender Aufbauorganisation:

Ein Projektausschuss ZAR (PA ZAR)

- steuert, plant, koordiniert und überwacht den Projektablauf,
- sorgt für die Bekanntgabe von Informationen über den Projektstand ZAR an die Direktion BFA,
- setzt die Prioritäten in Anbetracht der Anforderungen der Benutzer und der verfügbaren Ressourcen fest und
- untersucht die neuen Anforderungen unter den Gesichtspunkten der Datenschutz- und Datensicherheitsvorschriften.

Projektausschuss ZAR

- Benutzerprojektleiter (Vorsitz)
- EDV-Projektleiter
- Chef Informatik EJPD
- Leiter Bereich Systementwicklung RZ EJPD
- 1 Vertreter Abteilung Betriebszentrum BFI
- 1 Vertreter Vereinigung FREPO-Chefs
- Datenschutz- und Datensicherheitsberater BFA
- StV Leiter Bereich Zentrales Ausländerregister BFA

Das Projektteam ZAR-3

- prüft und stellt die Datenschutz- und Datensicherheitsvoraussetzungen sicher
- erarbeitet die Detailspezifikationen
- plant den Ressourceneinsatz
- erarbeitet die notwendigen Entscheidungsgrundlagen zuhanden des PA ZAR und
- qualifiziert die Ergebnisse

Projektteam ZAR-3

- EDV-Projektleiter (Vorsitz)
- Benutzerprojektleiter
- Stv. Benutzerprojektleiter
- Problemorientierte Vertreter der externen Benutzer (FREPO-, Gemeinde-, Arbeitsamt- bzw. Grenzstellenvertreter)
- Datenschutz- und Datensicherheits-berater BFA

Die Arbeitsgruppe Meldewesen

- ***prüft und erteilt die Anschlussgesuche***

- optimiert das Melde- und Mutationswesen (organisatorisch und technisch),
- sorgt für die Einführungsplanung.

Arbeitsgruppe Meldewesen

- Benutzerprojektleiter
- EDV-Projektleiter
- Stv. Leiter Bereich ZAR
- Vertreter der kantonalen und kommunalen FREPOstellen
- Vertreter des Schweiz. Verbandes der Einwohner- und Fremdenkontrollchefs
- Vertreter des RZ EJPD Bereich Systemtechnik & IT –Betrieb Telematik & Engineering

Die Arbeitsgruppe II /ZAR-3

- formuliert die anwenderbezogenen Aenderungsanträge und Anforderungen,
- setzt die Prioritäten bezüglich anwenderbezogener Anforderungen und
- überprüft die von den Systementwicklern erstellten anwenderbezogenen Arbeitsergebnisse.

Arbeitsgruppe II /ZAR-3

- Sektionschef Ressourcen (Vorsitz)
- Benutzerprojektleiter
- EDV-Projektleiter
- Chef Informatik EJPD
- Vertreter der kantonalen und kommunalen FREPOstellen
- Vertreter des Schweiz. Verbandes der Einwohner- und Fremdenkontrollchefs
- Vertreter des RZ EJPD Bereich Systemtechnik & IT Betrieb Telematik & Engineering
- Vertreter BFA (Datenschutzberater BFA, Abteilung Einreise und Aufenthalt, Sektion ZAR
- Vertreter des BFF

343.2 Ablauforganisation

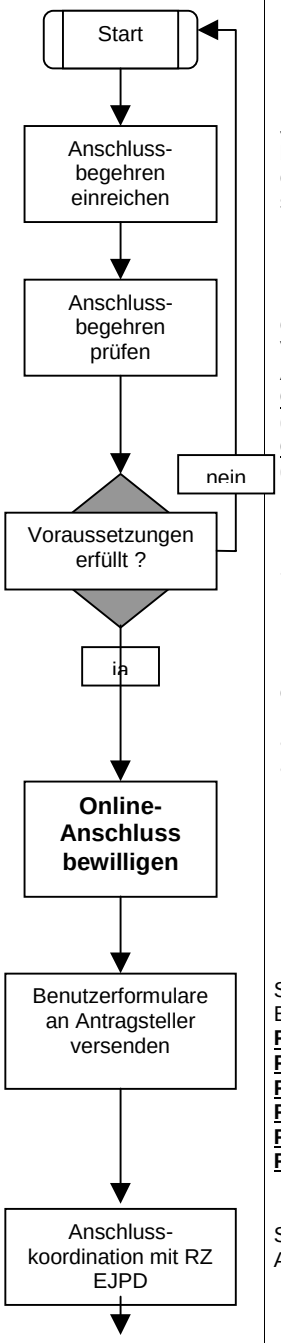
Die Authentizierung der technischen Anlagen und die Identifizierung der Benutzer erfolgt in der allgemeinen Benutzerverwaltung des RZ EJPD auf dem Tandem Host; erst danach darf der Zugriff auf die Grundmaske des ZAR erfolgen (Ziffer 2.5. des Bearbeitungsreglements). Im Zugriffsprofil des Datenkatalogs wird die Zugriffsberechtigung der Organisationseinheiten auf die Datenfelder festgelegt. Die Zugriffsstufen legen fest, ob nur angefragt oder mutiert werden kann. Zudem können die Datenabfrage und die Mutation auf einzelne Personenkategorien beschränkt werden. Das Zugriffsprofil jedes Systembenutzers wird durch Zugehörigkeit zu einer Organisationseinheit eingeschränkt. Jede Organisationseinheit erhält nur diejenigen Zugriffe, welche für die Erfüllung ihrer gesetzlichen Aufgaben unbedingt notwendig sind. Innerhalb der einzelnen Organisationseinheiten wird das Zugriffsprofil jeder Mitarbeiterin oder jedes Mitarbeiters gemäss den zu erledigenden Aufgaben bestimmt. Die Zugriffsvergabe, welche in Ergänzung zum Datenkatalog gemäss Anhang zur ZAR-Vo in der Zugriffstabelle nach Online-Funktion und Benutzer im Anhang 3 zum Bearbeitungsreglement festgelegt ist, erfolgt durch die Sektion ZAR im

BFA. Die Sektion ZAR kann die Zugriffsvergabe auch an die Verbindungspersonen für das ZAR in den Organisationseinheiten übertragen (Ziffer 2.6. Bearbeitungsreglement). Derzeit erfolgt aber keine Delegation der Zugriffsvergabe an externe Organisationseinheiten. Die externen Verbindungspersonen verwalten lediglich die Personalien ihrer Organisationseinheiten. Für die Einhaltung der Datenschutzbestimmungen beim Betrieb des ZAR ist grundsätzlich das BFA als Inhaber der Datensammlung verantwortlich. Vorbehalten bleibt die Verantwortung des Rechenzentrums EJPD und der an das ZAR angeschlossenen Stellen für die Datensicherheit in ihren Aufgabenbereichen (Ziffer 1.3. Bearbeitungsreglement). Im BFA ist der Amtsinformatiker als Benutzerprojektleiter für das ZAR verantwortlich (Ziffer 1.3. Bearbeitungsreglement). Der Datenschutzberater im BFA ist über alle Aenderungen und über die Planung von weiteren Ausbauschritten des ZAR zu informieren; er macht dabei auf die Erfordernisse des Datenschutzes aufmerksam (Ziffer 1.4. Bearbeitungsreglement). Er beantwortet Fragen im Zusammenhang mit dem Datenschutzgesetz bei der Anwendung des ZAR und überprüft zudem regelmässig die verordnungsmässige Vergabe der Zugriffe (siehe auch Weisungen über die Datenschutzberatung im EJPD). Grundsätzliche Entscheide werden durch die Amtsleitung getroffen. Gemäss provisorischer Weisung über die Protokollierung bei der Abfrage von Daten des Zentralen Ausländerregisters mittels eines Abrufverfahrens vom 2. November 1994 hat der Datenschutzberater des BFA dem Generalsekretär EJPD jährlich Bericht über seine Kontrolle zu erstatten (Ziffer 6).

Anlässlich der persönlichen Befragung der ZAR-Verantwortlichen des BFA am 3. Februar 1998 wurde der Ablauf eines Online-**Neuanschlusses** an ZAR wie folgt dargestellt. Die anschlussinteressierte Organisationseinheit (Bundesverwaltung, Kantons- oder Gemeindeverwaltung) hat ein schriftliches Anschlussgesuch an das BFA, Sektion ZAR, einzureichen. Die reduzierte Arbeitsgruppe Meldewesen (RZ EJPD/BFA) plant die Online-Anschlüsse und prüft die interessierten Organisationseinheiten innerhalb einer Amtsstelle auf die datenschutzrelevanten Einschränkungen. Das Anschlussgesuch wird gestützt auf eine interne Checkliste (Dokument: „raccordementrce.doc“) geprüft, wobei bei Neuanschlüssen oder politisch heiklen Anschlussbegehren die Direktion entscheidet (vgl. Checkliste „ZAR3-Neuanschluss an ZAR-3“ vom 18.2.1998), in allen anderen Fällen die zuständige Kontaktperson des BFA (Chef ZAR). Als politisch heikle (und damit in die Entscheidskompetenz des Direktors delegierte) Anschlussbegehren stuft das BFA gestützt auf seine ergänzenden Ausführungen vom 20. Mai 1998 Onlineanschlüsse ins Ausland und an Polizeibehörden ein. Der Datenschutzberater BFA, allenfalls der Eidgenössische Datenschutzbeauftragte, nehmen zu den Anschlussgesuchen Stellung. Im Falle eines positiven Anschlussentscheides versendet die Sektion ZAR (Abteilung EDV-Projekte) die notwendigen Formulare zuhanden des Antragstellers (vgl. Formularsammlung BFA: „Anschlussbegehren“, „Fragebogen Amtsstellenprofil“ „Benutzerverwaltung“, „Bestandesmutationen“, „Zugriffsprofilverwaltung“, „Unterschrift“). Nach Eingang der entsprechenden Formulare erfolgt seitens der Abteilung EDV-Projekte der Sektion ZAR des BFA die Kontaktaufnahme mit dem RZ EJPD zwecks Koordination des Anschlusstermins. Der Gesuchsteller wird anschliessend hinsichtlich Anschlusstermin, Schulung und Produktionsaufnahme durch die Abteilung projektbezogene Ausbildung und Beratung in der Sektion ZAR des BFA orientiert, die Systeminfrastruktur wird erfasst und die Benutzerprofile brieflich verschlossen an den verantwortlichen Schulungsleiter weitergegeben. Anschliessend erfolgen die Tests mit dem neuen Amtsstellenprofil und den Test-User-Nummern sowie das Aufgebot zur Schulung. Es werden keine Online-Zugriffe freigegeben, solange nicht eine entsprechende Schulung mit den zugriffsberechtigten Anwendern durchgeführt wurde. Anlässlich der Schulung erhält der neue Benutzer ein verschlossenes Couvert mit seiner Benutzerkennzahl und seinem persönlichen Passwort. Während der Startphase überwacht die Sektion ZAR des BFA (projektbezogene Ausbildung und Beratung) die produktive Nutzung.

Gemäss den provisorischen Weisungen über die Protokollierung bei der Abfrage von Daten des ZAR mittels eines Abrufverfahrens vom 2. November 1994 prüft der Datenschutzberater des BFA

einmal pro Monat die Protokollierungsdatei im RZ EJPD (Ziffer 2.8 Bearbeitungsreglement). Zudem hat er dem Generalsekretär EJPD jährlich Bericht über seine Kontrolle des ZAR zu erstatten (Weisung Ziffer 6). Gestützt auf die Beantwortung der Expertenzusatzfragen ergibt sich aus der Antwort des BFA vom 20. Mai 1998, dass mit der Einführung einer Abfrageprotokollierung im ZAR und eines neuen Kontrollverfahrens der Datenschutzberater BFA seit 1. Januar 1998 über einen direkten Zugriff auf die Protokollierungsdatei verfügt. Die Weisung vom 2.11.1994 ist noch in Kraft, muss aber an das neue Verfahren noch angepasst werden. Die Prüfung der Protokollierungsdatei erfolgt aufgrund des Benutzerhandbuches „Dokumentation Anfrageprotokollierung“ des RZ EJPD. Die Kontrolle findet durch wiederkehrende Stichproben und auf Hinweis oder nach einer besonderen Anfrage statt. Es wird kein Prüfungsbericht erstellt. Hingegen soll ein Standardbrief entworfen worden sein, welcher vom Datenschutzberater BFA an diejenigen Dienststellen gesandt wird, welche kontrolliert worden sind, soweit die Protokollierung einen Handlungsbedarf ergeben hat. Während im Jahr 1996 ein schriftlicher Jahresbericht an das GS EJPD abgefasst wurde, ist im Jahr 1997 der Datenschutzberater GS EJPD durch verschiedene mündliche Berichte informiert worden.

Bundesamt für Ausländerfragen		Bewilligungsverfahren für Online-Anbindung ZAR	Prozess 0xx	
Input	**Ablauf**	**Beschreibung und Hilfsmittel**	**Verant-wortung**	**Output**
Verwaltungs-internes Anschluss-gesuch Verwaltungs-externes Anschluss-gesuch (Kantone, Gemeinden etc.)		Jede (bundesverwaltungsinterne oder bundesverwaltungsexterne) Organisations-einheit, die Anschluss an ZAR wünscht, stellt ein schriftliches Gesuch mit kurzer Begründung an die Sektion ZAR des BFA.	Gesuchsteller für Online-Anschluss	Anschluss-begehren
		Die Arbeitsgruppe Meldewesen ZAR prüft, ob alle rechtlichen und tatsächlichen Voraussetzungen für einen Online-Anschluss gegeben sind. **Checkliste x00.001a (ZAR3-Neuanschluss)** **Checkliste X00.001b (raccordementrce.doc)**	Arbeitsgruppe Meldewesen ZAR des BFA	Vorprüfung Anschluss-voraussetzung
Anmelde-begründung Gesuchsteller		Der Datenschutzberater BFA (allenfalls der Eidg. Datenschutzbeauftragte) nehmen Stellung zum Gesuch	Datenschutz-berater BFA Eidg. Daten-schutzbeauf-tragter	Stellungnahme
		Die Arbeitsgruppe Meldewesen ZAR fällt eine Entscheidung und • informiert die Direktion BFA	Arbeitsgruppe Meldewesen ZAR	Anschluss-entscheid
		• holt einen Bewillilgungsentscheid der Direktion BFA ein, wenn ein Neuanschluss oder ein politisch heikler Erweiterungsanschluss zu entscheiden sind. **Checkliste x00.002 (Entscheidzuständigkeit Direktion BFA).**	Direktion BFA	Anschluss-entscheid
		Sektion ZAR versendet die Benutzerformulare an Gesuchsteller. **Formular 1:** Anschlussbegehren **Formular 2:** Fragebogen Amtsstellenprofil **Formular 3:** Benutzerverwaltung **Formular 4:** Bestandesmutationen **Formular 5:** Zugriffsprofilverwaltung **Formular 6:** Unterschrift	Sektion ZAR Abteilung EDV-Projekte	
		Sektion ZAR koordiniert die Anschlussarbeiten mit dem RZ EJPD.	Sektion ZAR Abteilung EDV-Projekte RZ EJPD	Anschlussplan Aktivitätenplan Terminplan Ressourcenplan

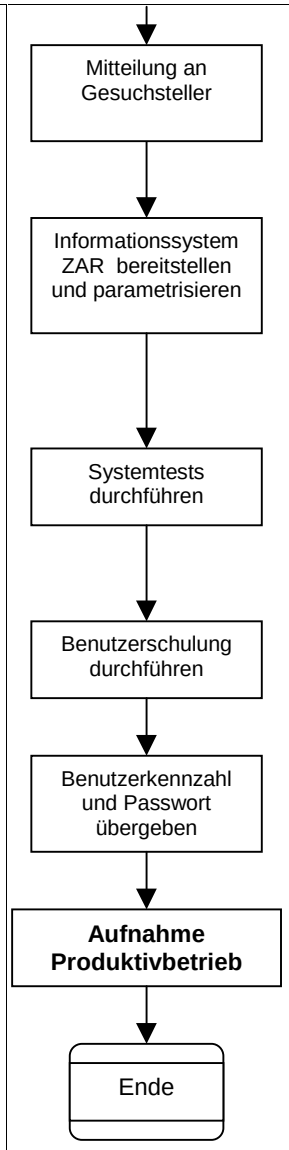
Anschlussplan Aktivitätenplan Terminplan Ressourcen-plan		Sektion ZAR orientiert den Gesuchsteller über Anschlusstermin, Schulung und Produktionsaufnahme Die Systeminfrastruktur, die Benutzerprofile sowie die notwendigen Zugriffs-berechtigungen werden durch die Sektion ZAR erfasst. Das RZ EJPD erstellt die Systembetriebsbereitschaft und schliesst den Gesuchsteller über die Kommunikationsinfrastruktur an ZAR an. Sektion ZAR und RZ EJPD koordinieren und führen die vorbereitenden Systemtests mit dem neuen Amtsstellenprofil und den Test-User-Nummern durch. Die definitive Betriebsbereitschaft wird erstellt. Sektion ZAR führt mit den Benutzern der neu angeschlossenen Organisations-einheit die obligatorische Benutzer-schulung durch. Uebergabe der Benutzerkennzahl und des persönlichen Passwortes an jeden neuen ZAR-Benutzer in verschlossenem Couvert an der Benutzerschulung. Die neu angeschlossene Organisationseinheit nimmt nach Abschluss der Schulung den Produktivbetrieb auf.	Sektion ZAR Abteilung pro-jektbezogene Ausbildung und Beratung Sektion ZAR RZ EJPD Sektion ZAR RZ EJPD Sektion ZAR Abteilung pro-jektbezogene Ausbildung und Beratung Neue Organisations-einheit	Anschlussplan Zugriffsrechte, Amtsstellenprofil Organisations-struktur, Datenkommuni-kation und Verschlüsselung Testprotokolle Betriebsbereit-schaft Benutzer-schulung und –einführung Benutzer-kennzahl Benutzer-passwort Produktivbetrieb
Version 1.0	**Was** Prozesserstellung	**Wann erstellt** **Von wem** 13.4.1998 FI	**Geprüft** 20.4.1998 xy	**Freigabe** 30.4.1998 zz

Abbildung: mögliche Prozessbeschreibung aufgrund der bekannten Ablaufaktivitäten für die produktive Inbetriebnahme eines Online-Anschlusses von ZAR.

Die im Vernehmlassungsverfahren vom BFA ergänzte und aktualisierte Fassung dieser Prozessbeschreibung befindet sich im Dokument „Nachtrag 1, Auswertungen und Zusammenfassung des verwaltungsinternen Vernehmlassungsverfahrens vom 30.7.1998)

344 Betrieb und Unterhalt

ZAR-3 wird projektmässig bearbeitet. Die zuständigen Gremien sind in Ziffer 343.1 (Aufbauorganisation) dargestellt. Die laufenden Ergänzungen, Anpassungen und Erweiterungen werden durch das Projektteam ZAR-3 sowie die Arbeitsgruppe II / ZAR-3 erhoben und gegenseitig abgestimmt. Für den Unterhalt und den Betrieb des Zentralrechners sowie die Kommunikationsinfrastruktur ist das Rechenzentrum EJPD zuständig. Für die Knotenrechner sowie die kantonale Kommunikationsinfrastruktur sind die zuständigen kantonalen Informatik- und Kommunikationseinheiten verantwortlich. Die Benutzerorganisationen sorgen für die Einhaltung der angemessenen organisatorischen und technischen Sicherheitsmassnahmen.

Anlässlich der Befragung der ZAR-Verantwortlichen im BFA am 3. Februar 1998 hat sich ergeben, dass die Durchsetzung von organisatorischen und technischen Datenschutz- und Datensicherheitsmassnahmen bei den kantonalen und kommunalen Behörden aufgrund fehlender gesetzlicher Grundlagen und mangels organisatorischer Zuständigkeit für diese Verwaltungseinheiten schwierig ist. Es gibt keine gesetzliche Grundlage für die Inspektion und Kontrolle solcher Massnahmen bei den ZAR-Benutzern ausserhalb der Bundesverwaltung. Das BFA bedient sich sogenannter „Höflichkeitsbesuche bei den ZAR-Benutzern“ und kann lediglich über informelle Gespräche und Sensiblisierung auf die Verantwortung und die Durchsetzung dieser Grundsätze hinwirken.
Zu einer ähnlichen Beurteilung kommt auch die Verwaltungskontrollstelle des Bundesrates in ihrem Bericht vom 22. Dezember 1997/9. Februar 1998 (VKB-Bericht). Vorfälle haben gezeigt, dass der Schutz sensibler Personendaten nicht in allen Fällen gewährleistet ist, weil die Zugriffsberechtigungen für Nutzer an der Peripherie nicht durchwegs genügend geregelt sind (VKB-Bericht Kapitel 41, Ziffer 12, Seite 34).

345 Kostenbeteiligungen

Die beteiligten Kantone und die anderen am ZAR angeschlossenen Behörden übernehmen die Anschaffungs- und Betriebskosten ihrer Geräte. Der Bund finanziert die Erschliessung und den Betrieb der Datenleitungen zu einem zentralen Anschlusspunkt (Hauptverteiler) am Kantonshauptort. Die Kantone übernehmen die Installations- und Betriebkosten für die Feinverteilung innerhalb der Kantone. Die für den bundesexternen Gebrauch vorgesehenen Datenstationen müssen den technischen Vorschriften der Computeranlage des Bundes entsprechen. Das Departement legt die Einzelheiten fest (Art. 21 Abs. 1 und 2 ZAR-Vo).

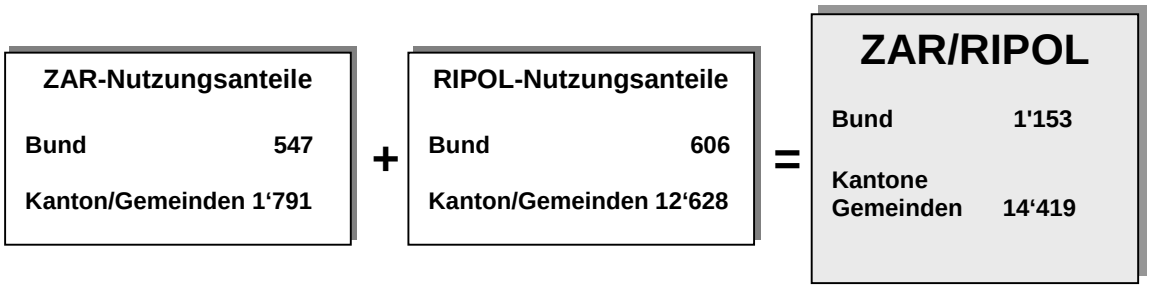
346 Kantone und andere bundesverwaltungsexterne Anschlüsse

Die insgesamt 2338 angeschlossenen Benutzer des Informationssystems ZAR verteilen sich zwischen Bund und Kantons-/Kommunalstellen wie folgt. 547 Benutzer (23.4%) gehören dem Bund resp. dem Fürstentum Liechtenstein (Landesverwaltung Fremdenpolizei / Passamt Liechtenstein) an, 1791 Benutzer sind Mitarbeitende der kantonalen oder kommunalen Behörden (76.60%).

ZAR-Nutzungsanteile

Bundesverwaltungs-**EXTERN**	**76.6%**	**1‘791 Benutzer**
Bundesverwaltungs-**INTERN**	**23.4%**	**547 Benutzer**

Diese Anschlusszahlen sind aber erheblich zu erhöhen, weil über das automatisierte Fahndungssystem RIPOL die dort angeschlossenen Benutzer auf ZAR zugreifen können. Gemäss Darlegungen der ZAR-Verantwortlichen des BFA anlässlich der Befragung am 3.2.1998 besteht die beschränkte Zugriffsmöglichkeit auf ZAR-3 direkt aus RIPOL insbesondere für die Polizeibehörden.
Aus den Darstellungen im Kapitel 3.1.6 (Informationssystem RIPOL) ergibt sich, dass 95.4 % oder 12‘628 bundesverwaltungsexterne Benutzer der Kantone und der kommunalen Behörden an RIPOL angeschlossen sind. Diese Zahl wird durch das Schreiben des BFA vom 20. Mai 1998 insofern bestätigt, als das BFA darin selber die aktuelle Zugriffszahl von RIPOL-Benutzern auf circa 12'000 beziffert. Im Anhang 4 ist ergänzend zur chronologischen Auflistung die vom BFA am 20. Mai 1998 eingereichte Uebersicht zu den angeschlossenen Organisationseinheiten aufgenommen. 24 Benutzeranschlüsse sind für schweizerische Vertretung im Ausland und 30 Anschlüsse für Interpolstellen eingerichtet.



Die Aufbereitung von ZAR-Daten geschieht in separaten Bildschirmmasken des Informationssystems RIPOL. Die Abfrage ist auf jene Daten beschränkt, die mit dem Ausländerrecht direkt in Zusammenhang stehen (Aktive Ausländer, Einreiseentscheide, Rückweisungen an der Grenze). Dies gilt nach Aussagen des BFA für das Bundesamt für Flüchtlinge, die Städte-Polizeibehörden, Grenzstellen, Beschwerdedienst EJPD, RZ EJPD, Bundesamt für Polizeiwesen, Kantonale Polizeidienste, Bundesanwaltschaft, Gemeindepolizeibehörden, Bundesamt für Ausländerfragen. Mithin handelt es sich durch die Verknüpfung von RIPOL und ZAR um gegen 15'000 ZAR-Benutzer. Seit dem 1.9.1997 sollen aufgrund eines Entscheides der Eidgenössischen Datenschutzkommission vom 27.6.1997 alle ZAR / ZAR-RIPOL-Zugriffe (ZAR-RIPOL-Zugriffe bereits früher) protokolliert werden. Der Einstieg in das ZAR erfolgt mittels einer persönlichen Benutzernummer und eines persönlichen Passwortes, welches systembedingt alle zwei Monate geändert werden muss. Die Anmeldung im System wird protokolliert. Bei der Bearbeitung von ZAR-Daten werden bei jeder Aenderung eines Records insbesondere Datum und Zeitpunkt der letzten Aenderung sowie der Benutzer (User ID), welcher diese vorgenommen hat, festgehalten (Bearbeitungsreglement BFA vom 16.11.1995, Ziffer 2.5.).

347 Entwicklungsperspektiven

Am 28. August 1997 hat das BFA verwaltungsintern zur Stellungnahme über die Revision der ZAR-Verordnung eingeladen. Die Revision ist aufgrund der vorgesehenen Inbetriebnahme der beiden Teilsysteme **EVA** (**E**lektronische **V**isum-**A**usstellung) und **EPOS** (**E**lektronisches **P**ersonenregistratur **O**nline **S**ystem) notwendig geworden. Beide Systeme sind Anwendungen des ZAR, was deren Regelung in der ZAR-Verordnung ermöglicht. Durch das Verfahren EVA soll ein Informationssystem zur elektronischen Erfassung der Visumsgesuche und Ausstellung der Visa realisiert werden (vgl. Bericht Konzept, Managementübersicht Seite 5). Dieses sieht vor, Online-Verbindungen zu den schweizerischen Auslandvertretungen zu schaffen. Die Verbindungen des

Rechners im RZ EJPD zu den Auslandvertretungen werden über einen Switchrechner im RZ EDA realisiert. Die andern zur Visumerteilung ermächtigten Stellen, d.h. die Grenzposten, die kantonalen Fremdenpolizeibehörden, das Bundesamt für Ausländerfragen und das Bundesamt für Flüchtlinge sind direkt an den Rechner des RZ EJPD angeschlossen. Als wesentliche Neuerung soll erreicht werden, dass die Konsultation des Bundesamtes für Aussenwirtschaft, des Bundesamtes für Polizeiwesen und der Bundesanwaltschaft durch das BFA bezüglich Visumsgesuche ausländischer Personen in Zukunft auf elektronischem Weg erfolgen soll. Gemäss Revisionserläuterungen handelt es sich aber hier nicht um einen Online-Anschluss, da die Daten nur im Einzelfall bekanntgegeben werden (Visum-Uebersteuerung, vgl. Konzeptbericht Seite 32, Ziffer 411.5). Im weiteren ist vorgesehen, künftig auch Grenzkontrollrapporte im ZAR zu erfassen und den zuständigen Behörden zur Online-Abfrage zur Verfügung zu stellen. Dies erfordert eine Erweiterung des Datenkataloges von ZAR mit neuen Datenfeldern. Zudem ist der Anschluss der Asylrekurskommission (zum Inkasso der Verfahrenskosten) vorgesehen. Neu soll auch in einer separaten Bestimmung die Ermächtigung und Aufforderung an das BFA ergehen, in einem Bearbeitungsreglement die organisatorischen und technischen Massnahmen gegen unbefugtes Bearbeiten der Daten und für die automatische Protokollierung der Datenbearbeitung zu regeln (neu Art. 17 Abs. 2 ZAR-Vo).

Ab April 1999 ist eine Pilotbetriebsaufnahme für die Neuapplikation EVA im BFA sowie bei folgenden Amtsstellen vorgesehen:

- Fremdenpolizeibehörden des Kantons BE
- Flughafenpolizei Zürich
- Grenzposten Basel-Weil
- Auslandvertretungen London und Moskau

Gestützt auf die vom Experten am 14. April 1998 gestellten Zusatzfragen hält das BFA mit Schreiben vom 20. Mai 1998 zu den Entwicklungsperspektiven ZAR ergänzend fest, dass der Weiterausbau des ZAR vom Generalsekretariat EJPD mit Schreiben vom 3. Dezember 1997 gestoppt worden ist, da die Projekte ZAR-Erweiterung und ZAR-Auswertung im Rahmen eines neuen Projektes „Ausländer 2000“ gesamtheitlich zu bearbeiten seien. Das BFA hat daraufhin u.a. mit Schreiben vom 4. Februar 1998 darum ersucht, diesen Entscheid aufzuheben. Im wesentlichen bringt das BFA folgende Aspekte ein:

- Sachliche Notwendigkeit im Zusammenhnag mit einer sicherheits- und datenschutzbedingten Einschränkung des Mutationsprofils (kantonale FrePo-Behörden und BAP);
- Eliminierung von Doppelspurigkeiten (Doppelerfassung, Realtime-Transfer, Grenzkontrollrapporte, elektronische Schnittstelle zu FREPO-Behörden der Gemeinden => Einführung eines elektronischen Briefkastens);
- Dringend gebotene Anpassung der statistischen Erfassung von Einreisesperren;
- Rationalisierung der Arbeitsabläufe (z.B. in den Bereichen Datenverarbeitung Familienangehörige sowie kantonale Wegweisungsverfügungen und deren Ausdehnung durch das BFA);
- Unbefriedigende Situation, dass die vom BFA dem Bundesamt für Statistik (BFS) gelieferten Ausländerdaten daselbst mit moderneren Mitteln besser aufbereitet werden können als im BFA, was dem BFS eine umfassendere und bessere Auskunftserteilung gestattet als dem zuständigen BFA;
- Die aktuellen Bearbeitungsvorgänge bei der Informationsgewinnung, Informationshaltung und Informationsverteilung vermögen – weil veraltet – nicht mehr

zu befriedigen; es sind teilweise Programme aus den frühen 70er Jahren im Einsatz, die Abläufe sind zu kompliziert und die Betriebs- und Wartungskosten sind unverhältnismässig hoch;

- Gemäss Weisung des Vorstehers EJPD die registermässig erfasste Namensschreibweise nach Zivilstandsrecht bis Ende 2000 gewährleistet werden muss;
- Bei Realsierung des Projektes AVOR ist mit jährlich wiederkehrenden Gebühreneinnahmen in der Höhe von rund 2 Mio Franken zu rechnen, was mittelfristig die Investitionskosten mehr als aufwiegen wird.

Eine Teilrevision der ZAR-Verordnung ist für Herbst 1998 vorgesehen. Damit soll insbesondere eine Rechtsgrundlage für die Zusatzsysteme EVA, EPOS und AVOR geschaffen werden. In die Verordnung sollen ebenfalls Ausführungsbestimmungen mit Blick auf die Teilrevision ANAG aufgenommen werden, namentlich im Bereich des Datenschutzes.
Es ist vorgesehen, die beiden Zusatzsysteme EVA und EPOS im 1. Quartal 1999 zu realisieren. Es sind bis heute keine Beziehungen zwischen diesen Ausbauschritten (Realisierung Zusatzsysteme EVA und EPOS) und dem geplanten „Ausländersystem 2000“ hergestellt worden. Eine Planung zum „Ausländersystem 2000“ liegt bis heute nicht vor. Eine diesbezügliche Grundsatzdiskussion unter Leitung des GS EJPD ist vorgesehen.

348 Zusammenfassung und Bewertung

1. Das Online-Bewilligungsverfahren ist lediglich im Bearbeitungsreglement des BFA in seinen Grundsätzen geregelt. Wie in den anderen Bereichen der polizeilichen Informationssysteme gilt es auch im Bereich ZAR zu berücksichtigen, dass die in übergeordneten Erlassen (Gesetz, Verordnung) aufgestellten Grundsätze für Online-Anschlüsse verloren zu gehen drohen, wenn die Bewilligungszuständigkeit immer weiter nach unten auf die operative Anwendungsebene delegiert wird. Dadurch können andere Gewichtungen und Interpretationen sowie die primären Anwenderinteressen den ursprünglichen Gesetzgeberwillen überlagern. Zudem kann durch die fehlende Unabhängigkeit der Bewilligungsinstanz ein Interessenkonflikt (gleichzeitig Systembetreiber, Informationsbearbeiter, Bewilligungsinstanz) entstehen. Es ist angezeigt, dass die für einen Online-Anschluss relevanten Entscheidungskriterien, das Verfahren, die Zuständigkeiten konzentriert und von entsprechend übergeordneter Verwaltungsstufe einheitlich festgelegt werden. Dem Gesichtspunkt der unabhängigen Bewilligungsinstanz ist stärkere Beachtung zu schenken.

2. Das Online-Bewilligungsverfahren würde an Verständlichkeit, Uebersicht und Klarheit gewinnen, wenn die Bewilligungsprozesse entsprechend dem in Ziffer 343.2 dargestellten Modell aufgezeichnet würden. Die Aufgaben, Kompetenzen und Verantwortlichkeiten können in diesem komplexen Bereich nur verbindlich und transparent festgelegt werden, wenn mit einer klaren graphischen-textlichen Ablaufdarstellung gearbeitet wird. Diese Darstellungsform würde sowohl innerbetrieblich als auch nach aussen viele offene Fragen und Unklarheiten eindeutig regeln und darstellen.

3. Das BFA erlässt zuhanden der Benutzerorganisationen Sicherheitsweisungen. Deren lückenlose und qualitativ hochstehende Durchsetzung kann vom BFA als Datenherr in den kantonalen oder kommunalen Organisationseinheiten mangels rechtlicher Grundlagen und infolge fehlender Zuständigkeit nicht sichergestellt werden. Es gibt keine gesetzliche Grundlage für Sicherheitsinspektionen des verantwortlichen Datenherrs des Bundes in den kantonalen oder kommunalen Benutzerorganisationen. Diese Tatsache stellt ein erhöhtes Sicherheitsrisiko beim Betrieb der

Informatikapplikation ZAR dar. Es wäre möglich, auf Gesetzesstufe entsprechende Regelungen für Kontrollzuständigkeiten zu erlassen. So hat beispielsweise der Gesetzgeber im Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG) vom 7. Oktober 1994 sowohl die Zusammenarbeit zwischen Bundes- und Kantonsbehörden umschrieben (Art. 12 ZentG) als auch in den Schlussbestimmungen den Bundesrat ermächtigt, in der Verordnung die Einzelheiten der Datenverarbeitung durch die Zentralstellen und die Koordination der Systeme, das Zugriffsrecht und den Umfang des Zugriffs durch Stellen des Bundes und der kantonalen Behörden sowie die Aufbewahrungsdauer der Daten, Kontrollen und Schutzbestimmungen zu erlassen (Art. 15 ZentG).

4. Die Anschlussgesuche an ZAR werden von den zuständigen operativen Verantwortlichen der betreffenden kantonalen oder kommunalen Organisationseinheiten eingereicht. Zuständige Personen im BFA prüfen nicht, ob die vorgesetzten Stellen oder die politischen Verantwortungsträger (z.B: Regierungsrat; Departementsvorsteher; Gemeinderat) das Anschlussgesuch kennen und ausdrücklich damit einverstanden sind. Zudem ist es für die verantwortlichen Stellen im BFA schwierig, die Verhältnismässigkeit und die Notwendigkeit von Online-Anschlüssen kantonaler oder kommunaler Organisationseinheiten zu überprüfen und allenfalls eine Reduktion derselben durchzusetzen, da sie mangels rechtlicher Grundlagen und infolge fehlender Zuständigkeit keinen Einfluss auf die ablauf- und aufbauorganisatorischen Rahmenbedingungen dieser Organisationseinheiten nehmen können.

5. Im Zusammenhang mit der geplanten Pilotbetriebsaufnahme EVA im April 1999 ist einmal mehr grundsätzlich zu prüfen, inwieweit solche Pilotbetriebe, welche später regelmässig in einen produktiven Systembetrieb überführt werden, einer gesetzlichen Grundlage bedürfen. Eine entsprechende Regelung sollte – sofern sie auf Verordnungsstufe genügt – in die laufende Revision der ZAR-Verordnung übernommen werden. Im übrigen verweisen wir auf die Ausführungen in Ziffer 328 (7. Punkt) und Ziffer 329 (6. Punkt), welche die generelle Schaffung einer formellen gesetzlichen Grundlage für Pilotprojekte mit besonders schützenswerten Personendaten und Persönlichkeitsprofilen vorschlagen.

6. Für den Anschluss von derzeit 26 Benutzern des RZ EJPD fehlt aufgrund der uns zur Verfügung stehenden Unterlagen eine gesetzliche Grundlage. Diese sollte auch dann ausdrücklich in der ZAR-Vo geschaffen werden, wenn Projektleiter und Systemadministratoren nur im Rahmen ihrer Aufgaben der Weiterentwicklung sowie des Betriebs und Unterhalts der Applikation ZAR auf das System zugreifen. Die Regelung kann ähnlich erfolgen wie in der neuen Verordnung über die Meldestelle für Geldwäscherei (MGwV) vom 16. März 1998, welche auf den 1. April 1998 in Kraft getreten ist. In Art. 9 Abs. 2 Lit. f ist für diese Kategorie von Benutzern (Projektleiter und Systemadministratoren) eine Anschlussmöglichkeit explizit statuiert worden.

7. Aus der chronologischen Auflistung von Online-Anschlüssen an ZAR können für einzelne Städte oder Gemeinde sehr hohe Anschlusszahlen eruiert werden (z.B: Personenmeldeamt Stadt Zürich: 134 Benutzer). Anhand der tatsächlichen Nutzungsintensität, welche aus den Systemloggins ermittelt werden kann, sollte die Verhältnismässigkeit und Notwendigkeit dieser Anschlusszahlen überprüft und in Absprache mit der betroffenen Organisationseinheit allenfalls reduziert werden.

8. Die provisorischen Weisungen über die Protokollierung bei der Abfrage von Daten des ZAR mittels eines Abrufverfahrens vom 2.11.1994 müssen aufgrund des neuen

Kontrollverfahrens sowie des seit 1.1.1998 bestehenden direkten Zugriffs des Datenschutzberaters BFA auf die Protokollierungsdatei umgehend revidiert werden.

9. Das EJPD hat zu prüfen, ob die heutige Praxis in der Umsetzung dieser Weisungen vom 2. November 1994 durch die Datenschutzberater der darin namentlich bezeichneten Bundesämter, - im vorliegenden Fall des BFA – dem Sinn und Zweck der Regelung genügt. Wenn keine schriftlichen Berichte zu den monatlich vorgeschriebenen Prüfungen der Protokollierungsdateien erstellt werden und von der im Jahre 1996 noch praktizierten Schriftlichkeit eines Jahresberichtes der Datenschutzberater der Aemter an den Datenschutzbeauftragten des GS EJPD abgewichen wird und neuerdings mündliche Berichte entgegengenommen werden, können sowohl der Nachweis deren Durchführung als auch die bei diesen Prüfungen festgestellten Mängel oder eben auch die Feststellung der vollständigen Korrektheit nicht transparent und nicht nachvollziehbar gemacht werden. Diese Tatsache schwächt die Stellung des EJPD gegen aussen als auch die Stellung der Datenschutzberater der Bundesämter verwaltungsintern. In diesem Zusammenhang ist eine Abstimmung mit dem Bundesamt für Informatik vorzunehmen, denn gemäss Ziffer 7 der Weisungen werden diese solange provisorisch angewendet, bis das BfI den Auftrag des Bundesrates vom 29.6.1994 betreffend die Festlegung von geeigneten Protokollierungsformen bei der Abfrage von Datenbanken mit besonders schützenswerten Daten ausgeführt hat. Ebenfalls sollte in dieser Frage der Eidgenössische Datenschutzbeauftragte angehört werden.

349 Empfehlungen und Massnahmenvorschläge

1. Das EJPD hat das Bewilligungsverfahren für den Online-Anschluss von Behörden, welche mit dem ZAR zusammenarbeiten, die Bewilligungsbehörden, die zu prüfenden Anschlusskriterien (Bewilligungsgründe), die minimalen Anforderungen an die Dokumentation (formeller Bewilligungsentscheid) und die Ablage (Bewilligungsarchivierung) festzulegen. Dabei ist eine verantwortungs- und stufengerechte Zuordnung der Bewilligungskompetenz vorzusehen und auf der Entscheidseite eine unabhängige Bewilligungsinstanz vorzusehen. Dabei empfiehlt sich die Festlegung und Durchsetzung einheitlicher Prozessablaufbeschreibungen gegenüber allen Amtsstellen, welche im Bereich Online-Anschlüsse im Polizeiwesen betroffen sind.

2. Das EJPD hat zu prüfen, ob im Bereich ZAR gesetzliche Grundlagen zur Durchführung von Sicherheitsinspektionen und zur Sicherstellung der Datenschutz- und Datensicherheitsstandards des Bundes durch den jeweils verantwortlichen Datenherrn bei den kantonalen oder kommunalen Benutzerorganisationen zu schaffen sind.

3. Das EJPD hat durch entsprechende gesetzliche Regelungen dafür zu sorgen, dass vor der Initialisierung von Informatik-Pilotprojekten im Polizeibereich die notwendige formelle Gesetzesgrundlage geschaffen wird, wenn besonders schützenswerte Personendaten bearbeitet werden. Es hat zudem in Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten zu prüfen, ob im Datenschutzgesetz explizit eine Zusatzbestimmung für die Durchführung von Pilotprojekten aufzunehmen ist, welche als formelle gesetzliche Grundlage die Mindestanforderungen an Pilotprojekte in der Bundesverwaltung im Bereich sensibler Daten festlegt.

4. Das EJPD hat für die Schaffung einer genügenden gesetzlichen Grundlage für den Anschluss von 26 Benutzern des RZ EJPD an ZAR zu sorgen.

5. Das EJPD hat die Praxis der Berichterstattung und der Durchführung von Protokolldateienprüfungen gemäss provisorischer Weisungen über die Protokollierung bei der Abfrage von Daten des ZAR mittels eines Abrufverfahrens vom 2.11.1994 durch die Datenschutzberater der Bundesämter und des Datenschutzbeauftragten des EJPD zu überprüfen, erhöhte Transparenz und Nachvollziehbarkeit durch Abfassung schriftlicher Berichte zu gewährleisten und die notwendigen Abstimmungen mit dem BfI und dem Eidgenössischen Datenschutzbeauftragten vorzunehmen.

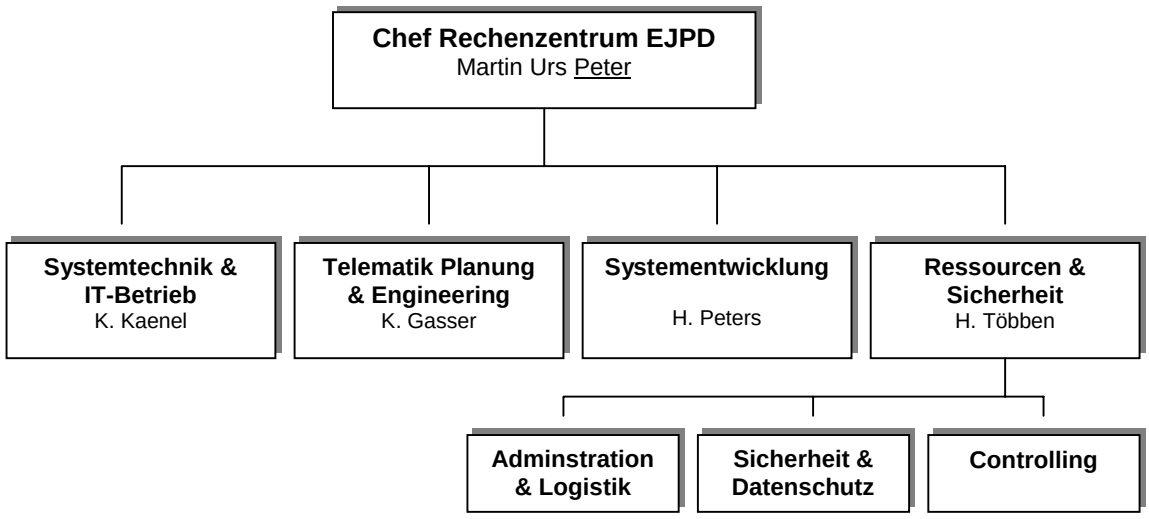
6. Das BFA hat die bestehenden Online-Anschlüsse an ZAR gestützt auf die tatsächliche Nutzungsintensität gemäss aktuellen Systemloggins nach den Grundsätzen der Verhältnismässigkeit und Notwendigkeit zu überprüfen und allenfalls in Abstimmung mit der zuständigen Benutzerorganisation zu reduzieren.

35 Rechenzentrum EJPD

Im Anschluss an die Befragung der ZAR-Verantwortlichen im Bundesamt für Ausländerfragen (BFA) führte der Experte auch mit dem Bereichsleiter Ressourcen & Sicherheit des Rechenzentrums EJPD (RZ EJPD) ein ausführliches Gespräch. Im wesentlichen standen dabei die Aufgaben des RZ EJPD im Bereich der Entwicklung, des Betriebs und Unterhalts der Polizeianwendungen, die Mitwirkung beim technischen Anschluss neuer Systembenutzer, die Sicherheit im Rechenzentrum und im Bereich der Netzinfrastruktur sowie die Parallelität von zwei Bundesnetzen (KOMBV und EJPD WAN) zur Diskussion. In den nachfolgenden Kapiteln sind die wesentlichen Erkenntnisse zusammengefasst.

351 Aufbauorganisation

Das Rechenzentrum EJPD mit Standort an der Industriestrasse 1 in Zollikofen steht unter der Leitung des Chefs Rechenzentrum EJPD. Es ist in vier Dienstleistungsbereiche gegliedert.



Im Zusammenhang mit dem Untersuchungsbereich Online-Anschlüsse sind insbesondere die Bereiche Systementwicklung und Ressourcen/Sicherheit von Interesse.

Der Bereich Systementwicklung stellt die Planung, Konzeption, Entwicklung, Realisierung und Wartung von Anwendungen sicher. Die Gruppe SE1 (Systementwicklung 1) ist auf die Entwicklung von Anwendungen auf der TANDEM-Plattform spezialisiert. Sie zeichnet insbesondere verantwortlich für das dreisprachige Zentrale Ausländerregister (ZAR), die Entwicklung von EVA (Elektronische Visum Ausstellung) sowie VOSTRA (vollautomatisiertes Strafregister). Die Gruppe SE3 ist zuständige für das nationale Fahndungssystem RIPOL und die neue Identitätskarte (IDK95), die Gruppe SE4 betreut alle Ermittlungsapplikationen der kriminalpolizeilichen Dienste (insbesondere DOSIS, ISIS, ISOK etc.).

Der Bereich Ressourcen & Sicherheit ist intern für eine optimale Administration & Logistik gegenüber den Benutzern verantwortlich. Hier werden die Querschnittsfunktionen Alarmwesen, Bestellungen, Budget, Desk Top Publishing, Empfang, Finanzen, Gebäude, Geschäftsverwaltung, Kursorganisation, Materialverwaltung, Personaladministration und Public Relations betreut. Hier werden auch die Online-Anschlussgesuche der externen Benutzer sowie die Formularanmeldungen der Bundesämter im EJPD für Anschlusserweiterungen entgegengenommen, koordiniert und bearbeitet. Die Gruppe Sicherheit & Datenschutz beschäftigt sich mit der Ermittlung und Bewertung von Risiken im Informatikumfeld. Auf den 1.4.1998 ist eine Pensumserhöhung von bisher 50% auf neu 250% vorgenommen worden, um die zahlreichen Sicherheitsaufgaben besser abzudecken. Diese Gruppe schlägt insbesondere Sicherheitsmassnahmen vor, setzt sie in Zusammenarbeit mit den anderen Bereichen um und kontrolliert deren Einhaltung. Die Gruppe koordiniert die Vorkehrungen zum Schutz der Persönlichkeit und der Grundrechte von Personen, deren Daten bearbeitet werden. Das Controlling zeichnet für die Kostenrechnung des RZ EJPD verantwortlich. Im weiteren unterstützt das Controlling die RZ-Leitung bei der Steuerung und Kontrolle von Informatik-Vorhaben und Informatik-Anwendungen hinsichtlich deren Wirtschaftlichkeit.

352 Ablauforganisation für Online-Anschlussbegehren

Das Rechenzentrum EJPD verfügt über ein Organisationshandbuch, welches die relevanten Abläufe und Prozesse des Dienstleistungserbringers RZ EJPD beschreibt. Der Anschluss von Benutzern an die diversen Applikationen ist in der Prozessbeschreibung „Anschlussbegehren LAN/WAN“ und „Anschlussbegehren Betrieb“ beschrieben. Die Prozessbeschreibungen datieren vom 15.6.1995 und wurden letztmals am 21.6.1995 geändert. Sie sind nachwievor gültig und seit dem 15.6.1995 in Kraft. Die Prozessbeschreibungen, welche ihre sinnvolle Ergänzung in entsprechenden Prozessbeschreibungen der zuständigen Bundesämter als Datenherren finden sollten, stellen Schritt für Schritt die innerhalb des RZ EJPD durchzuführenden Aktivitäten sowie die dafür zuständigen Sachbearbeiter dar. Diese Prozessbeschreibungen stellen einen überprüfbaren und damit intern auch stetig verbesserbaren Ablaufbeschrieb aller notwendigen Aktivitäten für einen Online-Anschluss im RZ EJPD dar.

353 Standort Rechenzentrum EJPD

353.1 Beurteilung der Standortsicherheit Zollikofen

Die Leitung des RZ EJPD hat im Jahre 1996 eine externe Sicherheitsüberprüfung für den gesamten Bereich der Rechenzentrumstätigkeiten durchführen lassen. Der als vertraulich klassifizierte Bericht, welcher dem Experten in der Version 1.1 vom 24.5.1996 vorliegt und von der BDS Berz Droux Scherler AG, Ingenieurunternehmung / Sicherheitsberatung, in Bern verfasst wurde, enthält eine umfassende Analyse der Schwachstellen und einen Massnahmenkatalog zur Erreichung eines minimalen bzw. optimalen Sicherheitsniveaus.

Im persönlichen Gespräch mit dem Bereichsleiter Ressourcen & Sicherheit des Rechenzentrums EJPD (RZ EJPD) am 3.2.1998 hat sich ergeben, dass nach seinen Einschätzungen sowohl Standort wie Sicherheitsinfrastruktur im Rechenzentrum EJPD nicht resp. noch nicht den höchsten Sicherheitsanforderungen genügen. Diese Darstellungen werden durch den externen Sicherheitsbericht der Firma BDS AG vom 24.5.1996 bestätigt. Danach war es zumindest im Zeitpunkt der externen Begutachtung ohne Einbruch möglich, bis zum RZ-Eingang in Zollikofen zu gelangen. Sabotage- oder Racheakte könnten innert Minuten erfolgen. Die Interventionszeit der Polizei in Zollikofen war und ist vermutlich auch noch heute zu gross. Der Brandschutz an beiden Standorten wies wesentliche Lücken auf (z.B: mangelhafte Abschottung), die Klima-Anlage in Zollikofen war nicht korrekt ausgeführt worden, sodass im Brandfall u.a. auch ätzende Gase bis in den RZ-Raum hätten vordringen können. Die Begutachtungsfirma kam zum Schluss, dass **im physischen Bereich des Rechenzentrums EJPD das festgestellte Sicherheitsniveau nicht haltbar ist und zu einem zwingenden Handlungsbedarf führt**.

Am 1. Juli 1997 besichtigte die Geschäftsprüfungsdelegation das Rechenzentrum EJPD in Zollikofen. Dabei konnte sie selber feststellen, dass die üblichen personenbezogenen Sicherheitsmassnahmen (Eintrittskontrollen, Schleusen, Badges etc.) vorhanden sind und greifen. Das Rechenzentrum EJPD verfügt beim Zutrittsschutz über ein Zonenkonzept. Als physisches Zugangsmedium dienen die persönlichen Badges der Mitarbeitenden. Die Computerräume als inneres Herzstück der Räumlichkeiten des RZ EJPD sind durch zwei Spezialtüren mit Direktalarmierung beim Sicherheitsdienst der Bundesverwaltung resp. der Polizei gesichert (zu weiteren Sicherheitsmassnahmen und sicherheitstechnischen Einrichtungen, vgl. Stellungnahme des RZ EJPD vom 22.7.1998, Seite 2). Hingegen sind der Delegation damals auch die räumlichen Gegebenheiten, insbesondere die Lage des Rechenzentrums in unmittelbarer Nähe der SBB-Linie Bern-Olten (Sicherheitsrisiko; Transport gefährlicher Stoffe) sowie die Einsehbarkeit der Produktions- und Rechenzentrumsräume (Fensterfronten) aufgefallen. Diese Situation liess bereits damals die Frage nach entsprechender Anfälligkeit der Produktionsräume des RZ EJPD aufkommen, insbesondere die Verwundbarkeit des Rechnerraumes gegen terroristische oder andere kriminelle Angriffe. In den Produktionsräumen des RZ EJPD laufen sehr sensible Informatikanwendungen. Der Sicherheitsbericht der Firma BDS AG, welcher in Kapitel 5 rund 20 Massnahmen im physischen Bereich auflistet, kommt abschliessend zur Feststellung, dass zur Eliminierung der Schwachstellen im Kapitel 5 **ein Standortwechsel notwendig** wäre. Als Massnahme wird dieser Vorschlag jedoch als nicht realisierbar qualifiziert (Bericht S. 20, Ziffer 5.1.4).

353.2 Umsetzungsmassnahmen

Aus dem Sicherheitsbericht BDS wie auch aus der Stellungnahme der Führung RZ EJPD zuhanden des Experten vom 28.2.1998 kann zudem entnommen werden, dass die Umsetzung der vorgeschlagenen Massnahmen in mehreren Fällen bereits begonnen hat. Teilweise sind die Massnahmen schon Bestandteil von aktuellen Projekten des RZ EJPD oder können in aktuelle Projekte integriert werden. Zusätzlich hatten die Führungskräfte des RZ EJPD im Laufe der Auftragsbearbeitung durch die Firma BDS AG bereits Sofortmassnahmen durchgesetzt oder in Auftrag gegeben. Mit der Zusammenlegung mehrerer Informatikorganisationen und der Inbetriebnahme neuer Projekte war das RZ EJPD einem starken Wachstum unterworfen. Dies führte dazu, dass bei den Informatiksystemen und –anwendungen mittels Einzelmassnahmen ein überdurchschnittlicher Schutz realisiert wurde. Eine gesamtheitliche Sicht der Informatiksicherheit konnte aber nicht realisiert werden (was die Firma BDS AG später mit „Schwachstellen in der Organisation“ wertete). Mit der Ernennung eines Sicherheitsbeauftragten wurde der Grundstein für eine neue Konzeption gelegt. Die Departementsleitung wurde sensibilisiert und das Projekt RZ-Sicherheit gestartet.

Mit der Anpassung der Organisation des Rechenzentrums EJPD per 1. September 1997 wurden die Strukturen bereinigt und 200 Stellenprozente für Datenschutz & Sicherheit gesprochen. Mit dieser Massnahme können gemäss Aussagen der RZ-Leitung im Jahre 1998 die restlichen Massnahmen aus der Sicherheitsüberprüfung BDS erledigt werden. Zur Verifikation dieser Arbeiten ist eine zweite externe Ueberprüfung der Sicherheitsmassnahmen im RZ EJPD geplant. Infolge der teilweisen Freistellung von Schlüsselpersonen des Rechenzentrums EJPD für das Projekt NOVE-IT der Bundesverwaltung wird die Durchführung der erneuten externen Sicherheitsüberprüfung voraussichtlich erst 1999 erfolgen. (Anmerkung der Führung RZ EJPD: *"Hier sei angemerkt, dass Exponenten von Nove-IT Sicherheitsbedenken und Sicherheitsmassnahmen weniger hoch gewichten als das RZ EJPD und teilweise grundsätzlich in Frage stellen*").

Im Zeitpunkt der Bearbeitung des Expertenberichts werden im Rechenzentrum in Zollikofen und am Bundesrain 20 Bauarbeiten realisiert, die mit vertretbarem Kostenaufwand Sicherheitsmassnahmen umsetzen. Die Bauprojektleitung geht von einer Erledigung der Arbeiten an beiden Standorten bis Ende KW 16/1998 aus (zum Stand der Umsetzung, vgl. Stellungnahme RZ EJPD vom 22.7.1998, Seite 2). Die Departementsleitung EJPD hat ausserdem gemäss Aussagen der Leitung RZ EJPD über die mittelfristige Aufgabe des Standortes Zollikofen entschieden und dies der Koordinationsstelle Bauwesen Zivil mit Schreiben vom 30.9.1996 durch den Generalsekretär EJPD schriftlich mitgeteilt:

„Bedingt durch die immer stärkere Abhängigkeit der Verwaltung von der Informatik muss die Departementsleitung der Informatiksicherheit heute deutlich mehr Gewicht zumessen. Bundesrat Koller hat mich deshalb persönlich mit dem Projekt RZ-Sicherheit beauftragt, welches auch eine externe Sicherheitsüberprüfung durch die Firma Berz Droux Scherler AG (BDS) des Rechenzentrums beinhaltete. Gestützt auf diese Ueberprüfung hat das EJPD die folgenden Grundsatzentscheide gefällt:

- Angesichts der knappen Finanzlage des Bundes und der ins HOZ (Gewerbezentrum Hostettler Zollikofen) investierten Bundesgelder bleibt das RZ EJPD längstens bis zum Ablauf des Mietvertrages im Jahre 2006 an der Industriestrasse 1.
- Sollte aber der Vermieter in der Uebergangsphase einem unverträglichen Mitmieter (z.B. Technodancing) Räumlichkeiten im HOZ vermieten, müsste ein vorzeitiger Standortwechsel erfolgen oder die betreffenden Räume durch den Bund übernommen werden.
- Die durch die externe Ueberprüfung aufgedeckten physischen Mängel sind nach Möglichkeit zu beheben. Der KBZ (Koordinationsstelle Bauwesen Zivil) werden hierzu die Vorschläge der BDS zur Realisierung beantragt.
- Der KBZ wird beantragt in ihren Bedarfsplänen einen neuen Standort für das RZ EJPD spätestens auf das Jahr 2006 hin aufzunehmen. Beim neuen Standort sind die betrieblichen und sicherheitsmässigen Bedürfnisse des Rechenzentrums EJPD vollumfänglich abzudecken.
- Sollte allenfalls früher ein geeignetes Gebäude frei werden (zum Beispiel durch Aufgabe eines anderen Rechenzentrums) kann das RZ EJPD mit einer Vorlauffrist von mindestens einem Jahr den Standort wechseln."

Abschliessend hält die Führung des RZ EJPD fest, dass die Informatiksicherheit im RZ heute wie folgt umschrieben werden kann:

- Sehr gute Mitarbeiterausbildung und –sensibilisierung
- Sehr gute Situation im technischen Bereich
- Gute organisatorische Grundlage
- Bekannte Mängel im physischen Bereich (Standort Zollikofen)

Der Frage Standort-Sicherheit in Zollikofen muss besondere Beachtung geschenkt werden. Das Rechenzentrum in Zollikofen genügt insbesondere den Gebäudesicherheitsstandards nicht. Diese Tatsache wird dem aufmerksamen Leser der Informatik-Fachpresse drastisch vor Augen geführt. In der Handelszeitung vom 4. Februar 1998 (Ausgang Nr. 6 Seite 53, Rubrik News) werden Produktetests der schwedischen Armee mit der sogenannten „Elektronik-Bombe“ beschrieben. Die „Bombe“ ist lautlos, hat in einem Aktenkoffer Platz und dennoch eine fatale Vernichtungskraft: Das

schwedische Militär hat seine Tests mit einer „Elektronik-Bombe“ aus russischer Produktion durchgeführt. Sie zerstört jeden Computer in ihrem Umkreis. Bei dieser „Bombe“ handelt es sich um ein kaum 100‘000 Dollar teures Gerät, das kurze Mikrowellen-Impulse mit einer Energie von bis zu zehn Gigawatt aussenden kann, was der Leistung von zehn Nuklearreaktoren entsprechen soll. Die Bombe hat eine Reichweite von einigen Dutzend Metern; ein etwas grösseres Modell bringt es auf einige hundert Meter. In Pistolenform gibt es diese Waffe ebenfalls. Einsetzen lässt sich die „stille“ Waffe gegen jede Art von Computer, ob in einem Kampfjet, einem Rechenzentrum einer Bank oder einem Kraftwerk. Die Energieimpulse lassen sozusagen die Schaltkreise „durchschmoren“. Entsprechend gefährlich ist ein solches System in den Händen von Terroristen. Laut Rüstungsexperten ist eine derartige Waffe international bislang aber noch nicht zum Einsatz gekommen. Immerhin haben mehrere Länder die Technik erworben, wird berichtet. Seit dem Golfkrieg sollen zum Beispiel Cruse Missiles des US-Militärs mit solchen Systemen ausgerüstet worden sein (Handelszeitung 4. Februar 1998, Seite 53).

Die vorgesehene Konsolidierung der Rechenzentren in der Bundesverwaltung sollte auch nach Ansicht des Bundesamtes für Informatik einen raschen Standortwechsel des RZ EJPD z.B. in die geschützten Räumlichkeiten des Departements Verteidigung, Bevölkerungsschutz und Sport (VBS) ermöglichen (vgl. Stellungnahme vom 22.7.1998, Seite 1, Ziffer 2).

354 Sicherheitsstandards im RZ EJPD

354.1 Security Policy

Das Rechenzentrum EJPD hat im Bereich der Informatiksicherheit des gesamten Rechenzentrums eine Security Policy RZ EJPD vom 19.7.1997 statuiert. Diese definiert die Zuständigkeit, Aufgaben und Kompetenzen rund um die Informatiksicherheit und legt die Sicherheitsgrundsätze sowie die dazu notwendige Organisation dar. Für die Informatiksicherheit des gesamten Rechenzentrums ist die RZ-Leitung verantwortlich. Sie definiert und aktualisiert die Security Policy des RZ EJPD, die auf den folgenden vier Säulen der Informatiksicherheit basiert:

- **Verfügbarkeit** (Zuverlässigkeit, Stabilität, Datensicherung),
- **Vertraulichkeit** (Zugriffsschutz, Abhörsicherheit),
- **Integrität** (Verlässlichkeit, Richtigkeit),
- **Nachvollziehbarkeit** (Auditing, Log-in).

Alle Sicherheitsmassnahmen des RZ EJPD sollen sich an den Grundsätzen der Rechtmässigkeit, Verhältnismässigkeit, Erforderlichkeit und Zweckmässigkeit orientieren. Zur Durchsetzung der Security Policy verfügt die RZ-Leitung periodische Ueberprüfungen (Z.B: Leistungs-, Qualitäts- und Zeitkontrollen, Kontrollen der Arbeitsprozesse). Ein Sicherheitsbeauftragter ist verantwortlich für alle Beschreibungen, Anleitungen, Vorschriften und Massnahmen (Sicherheitsportfolio). Die Linienvorgesetzen sind für die Umsetzung der Security Policy und der geltenden Vorschriften in ihren Bereichen und Gruppen verantwortlich. Jeder Mitarbeitende hat im Rahmen der Aufgabenerfüllung die Security Policy und die geltenden Vorschriften anzuwenden.

Im Bereich der produktiven Systeme und des zuständigen Personals gilt insbesondere, dass die Produktionssysteme das höchste Sicherheitsniveau erreichen müssen, Datenbestände von Geschäftssystemen vor Einsichtnahme, Aenderung oder Kopieren durch Unberechtigte zu schützen sind, Geschäftsdaten vor dem Zugriff durch Betriebs-, Wartungs- und Entwicklungspersonal geschützt werden müssen, produktive Daten nur aufgrund eines schriftlichen Auftrages des Dateninhabers weitergegeben oder zugänglich gemacht werden dürfen, für Tests mit Geschäftsdaten in jedem Falle eine Genehmigung des Dateninhabers notwendig ist und sich jeder Benutzer mittels eigener persönlicher Kennung und Passwort zu autorisieren hat.

Sobald Schulungs- oder Testsysteme produktive Daten enthalten oder physisch auf einem Produktionssystem laufen, gelten die gleichen Bestimmungen wie auf der Produktion. Jede Sicherheitsfunktion ist zu protokollieren und die Protokolle müssen analysiert werden können.

354.2 Umsetzungsmassnahmen

In ihrer Stellungnahme vom 28.2.1998 weist die Führung des RZ EJPD ausdrücklich darauf hin, dass mit dem Erlass der Security Policy vom 19.8.1997, der Erstellung des Sicherheitsportfolios und der Reorganisation im RZ EJPD per 1.9.1997 wesentliche Massnahmenpunkte der externen Sicherheitsstudie BDS umgesetzt wurden. Auch die Weisung 02 des Bundesamtes für Informatik betreffend Grundschutz von Informatiksystemen und –anwendungen vom 19.4.1995 sei damit zu 90% umgesetzt. Für die Hostapplikationen wurde die Emulation TAXI entwickelt, welche sowohl auf TANDEM- als auch auf DEC-Systemen eingesetzt wird und eine End-zu-End Softwarechiffrierung enthält. Zugriffe auf TANDEM-Systemebene werden durch das Sicherheitsprodukt SECOM auf den einzelnen RZ-Mitarbeiter bezogen. Der Zutrittsschutz für den Rechnerraum Zollikofen wird in KW 14/1998 baulich verstärkt. Die Interventionszeit in Zollikofen kann nicht reduziert werden. Brandschutzabschottungen in Zollikofen sind im Frühjahr 1997 nachgebessert worden. In KW 12/1998 erfolgen die baulichen Verbesserungen am Bundesrain und in KW 15/1998 eine erneute Kontrolle in Zollikofen. Die Klima-Anlage in Zollikofen wird in KW 11/1998 bis KW 16/1998 entsprechend umgebaut und der Ueberspannungsschutz und die Erdleitung der Hauptverteilung sind überprüft worden. Im weiteren wird detailliert zu den einzelnen Massnahmenpunkten der Sicherheitsstudie Stellung genommen und der Stand der Umsetzung dargestellt.

354.3 Schlussbeurteilung Sicherheitsstandards

Zusammenfassend lässt sich feststellen, dass mit der Initialisierung einer externen Sicherheitsbegutachtung des RZ EJPD wesentliche Erkenntnisse über die bestehende Situation gewonnen werden konnten. Insbesondere im Bereich Rechenzentrum Zollikofen sind umfangreiche Zusatzmassnahmen im physischen Bereich notwendig geworden. Auch im logischen Bereich sowie in der Aufbauorganisation haben sich erhebliche Massnahmen aufgedrängt. Durch die Verstärkung des Bereichs Ressourcen und Sicherheit sind personell wie organisatorisch die notwendigen Massnahmen eingeleitet worden. Die sukzessive Umsetzung der Detailmassnahmen ist im Gang und auf gutem Wege.

(Die Kommission hat auf Antrag der Sektion diese Passage aus Gründen des Staatsschutzes nicht veröffentlicht.)

Die Absicherung der Datenbestände und der Systeminfrastruktur gegen unberechtigte Zugriffe und Datenmanipulationen durch Mitarbeiter des RZ EJPD ist ebenfalls fortgeschritten. Durch den

Einsatz des Sicherheitsprogrammes SECOM, welches auf allen TANDEM-Systemen aktiviert ist (Stellungnahme RZ EJPD vom 26.2.1998, Seite 4, zu Ziffer 4.3.), soll die Weisung Informatiksicherheit Nr. S02 des Bundesamtes für Informatik vom 19.4.1995 zu 90% umgesetzt sein. Zu beachten bleibt, dass laufende Sicherheitsüberprüfungen und Kontrollen durch eine unabhängige Instanz trotzdem notwendig bleiben, verfügen doch auch solche Sicherheitsapplikationen immer über die sogenannte „Super-Super-User“ Berechtigung, welche weitestgehende System- und Datenmanipulationen zulässt. Die entsprechenden aufbauorganisatorischen Massnahmen (Bereich Ressourcen & Sicherheit) im RZ EJPD sind seit dem 1.9.1997 getroffen worden und entsprechende Kontrollen können in diesem Bereich laufend durchgeführt werden. Durch die geplante, erneute externe Ueberprüfung der Sicherheitsmassnahmen im RZ EJPD ist Gewähr für eine kontinuierliche Anpassung und Umsetzung der Sicherheitsmassnahmen gegeben. Der Experte erachtet das Hinausschieben der erneuten Sicherheitsüberprüfung auf frühestens 1999 infolge prioritärem Ressourcenbedarf im Projekt NOVE-IT als falsch.

355 Sicherheitsüberprüfung der Mitarbeiter RZ EJPD

Die Mitarbeitenden des RZ EJPD arbeiten als Systemverantwortliche, Operator, Analytiker, Programmierer, Projektleiter, Kommunikationsspezialisten und in weiteren Funktionen sehr nahe und direkt an der gesamten Informatikinfrastruktur, den relevanten Programmen und den sensiblen Daten der betreuten und zu entwickelnden Informatiksysteme des Polizeiwesens. In ihrer dienstlichen Tätigkeit erlangen sie damit umfassende Kenntnisse über Strukturen, Modelle, Daten, Abläufe und wesentliche Informationen in einem sehr sensiblen Bereich staatlicher Aufgaben. Dem Rechenzentrum wurden denn auch für die Unterstützung der diversen Bundesämter in Informatikangelegenheiten Personen zugewiesen (z.B: 1995 für die Zentralstelle Organisierte Kriminalität; vgl. Schreiben RZ EJPD vom 31.5.1995 an das GS EJPD). Die Mitarbeitenden des RZ EJPD erfüllen damit in ihren verschiedensten Aufgaben einzelne oder mehrere Voraussetzungen, wie sie in der Verordnung über die Sicherheitsprüfung in der Bundesverwaltung vom 15. April 1992 (SR 172.013) definiert sind. So ist gemäss Art. 2 dieser Verordnung jene Person einer Sicherheitsprüfung zu unterziehen, die in der vorgesehenen dienstlichen Tätigkeit u.a.:

a) ....
b) regelmässig Zugang zu Geheimnissen der inneren oder äusseren Sicherheit der Eidgenossenschaft hat und der Spionage ausgesetzt ist;
c) .....
d) in der Bekämpfung der Spionage, des Terrorismus oder des organisierten Verbrechens tätig ist;
e) als Mitarbeiter bei einer Sicherheitsprüfstelle wegen seines regelmässigen Zugangs zu besonders schützenswerten Personendaten die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen kann.

Der Bundesrat genehmigt die Liste der Aemter, deren voraussichtliche Inhaber einer Sicherheitsprüfung unterzogen werden (Art. 2 Abs. 2 der Verordnung).

Auf dieser Liste sind die Mitarbeitenden des Rechenzentrums nicht enthalten, obwohl sie in ihren verschiedenen Aufgaben die Voraussetzungen einer Sicherheitsprüfung zum Teil mehrfach erfüllen. Die Führung des RZ EJPD hat bereits mit Schreiben vom 31.5.1995 das Generalsekretariat EJPD darauf aufmerksam gemacht, dass die RZ-Leitung den Beschluss gefasst habe, das gesamte RZ-Personal (interne und externe Mitarbeitende) sowie das Hausdienstpersonal der Sicherheitsprüfung zu unterstellen. Seither sind aber keine konkreten Schritte unternommen worden. Der Personalchef im Generalsekretariat des EJPD hat der RZ-Leitung mit Schreiben vom 10.2.1998 mitgeteilt, dass gemäss der geltenden Verordnung vom 15.4.1992 sowie der Liste des EJPD betreffend sicherheitsrelevanter Aemter für die Bediensteten des Rechenzentrums EJPD generell keine Sicherheitsüberprüfung vorgenommen werden dürfe.

Der Experte teilt diese Ansicht nicht. Die Voraussetzungen für eine Sicherheitsprüfung sind einerseits gestützt auf die Definitionen in Art. 2 der Verordnung für alle Mitarbeitenden im Rechenzentrum – zum Teil sogar mehrfach – erfüllt, anderseits ergeben sie sich aus den tatsächlichen Gegebenheiten im Bereich Entwicklung, Betrieb, Unterhalt und Verwaltung von Applikationen und Datenbeständen im Polizeibereich. Das EJPD hat dem Bundesrat lediglich die Ergänzung der besagten Liste mit allen Mitarbeitenden des RZ EJPD zu beantragen. Die Gründe dafür hat die Leitung des RZ EJPD bereits vor 3 Jahren schriftlich geliefert. Die Ergänzung der Liste sowie die Sicherheitsprüfung aller Mitarbeitenden des RZ EJPD sollte ohne Verzug in die Wege geleitet werden.

356 Auslandanschlüsse

Aus der chronologischen Auflistung von Online-Verbindungen im Bereich RIPOL vom 26.11.1997 des BAP ist ersichtlich, dass auch schweizerische Vertretungen im Ausland (24) und Interpol-Stellen (30) über das WAN EJPD/KOMBV4 resp. WAN EJPD/SITA über TCP/IP, X.25 und ISDN an RIPOL angeschlossen sind. Zum Teil soll software-basierende End-to-End Chiffrierung und/oder Link-Chiffrierung (Back-Bone WAN EJPD) eingesetzt werden.

(Die Kommission hat auf Antrag der Sektion diese Passage aus Gründen des Staatsschutzes nicht veröffentlicht.)

Der Verbindungsverlauf führt bei sämtlichen Anschlüssen via X.25 Paket-Netze (9.6 Kbit/s bis 19.2 Kbit/s). Die Verschlüsselung wird mit Payload-Paket Chiffrierung (128 Bit-Schlüssel) der Firma Gretag durchgeführt.

(Die Kommission hat auf Antrag der Sektion diese Passage aus Gründen des Staatsschutzes nicht veröffentlicht.)

357 Parallele Kommunikationsnetze KOMBV-KTV und EJPD-WAN

Es ist unbestritten, dass die Anwendungen im Polizeibereich und die dafür bereitzustellende Kommunikationsinfrastruktur mit hohen Sicherheitsvorkehrungen vor unberechtigten Zugriffen Dritter zu schützen sind. Aus diesem Grunde hat das EJPD für seine Anwendungen ein eigenes, logisch abgetrenntes Netz (EJPD-WAN) aufgebaut. Dieses stellt die sternförmige Verkehrsbeziehung des RZ EJPD mit 26 Partnern (Kantone) dar. Eine Verkehrsbeziehung besteht hier ausschliesslich zwischen den entsprechenden Behörden und dem Rechenzentrum EJPD. Eine Verkehrsbeziehung der Partner untereinander sowie zu externen Netzen wie Internet ist nicht möglich. Das EJPD-WAN wird deshalb auch als eine „Mehrzahl individueller, geschlossener Benutzernetze“ bezeichnet (vgl. zum Ganzen: Stellungnahme RZ EJPD vom 22.7.1998, Seite 3 und 4). In den meisten Fällen werden aufgrund der relevanten Benutzergruppen die Kommunikationsverbindungen zu den Kantonen in die Gebäulichkeiten der Kantonalen Polizeikorps geführt. Jedenfalls aber existiert durch dieses eigenständige Netz im Polizeibereich eine Doppelspurigkeit zum KOMBV-KTV.

Die Kantone sind über Eintrittsknoten in den Kantonshauptorten an das KOMBV-KTV angekoppelt und tauschen über dieses Basisnetz alle Informationen und Daten ausserhalb des Polizeibereichs aus. Diese Aufteilung in zwei logisch getrennte Bundesnetze stösst insbesondere bei den Kantonen, aber auch bei einer Reihe von Bundesstellen auf Unverständnis und Kritik, da dadurch Mehraufwand und Mehrkosten (doppelte Infrastrukturen, Absicherungen, Zuständigkeiten, Verantwortungen etc.) verursacht werden. Die Diskussionen entbrennen immer wieder an der Frage nach angemessenem Netzschutz versus applikationsbasiertem Schutz (Anwendungsverschlüsselung). Insbesondere die Polizeistellen des Bundes befürchten, dass eine Zusammenlegung der Bundesnetze die Uebertragungssicherheit für ihre Applikationen nicht mehr garantieren kann (vgl. zum Ganzen: VKB-Bericht, Seite 25-27, 31, 33 und 36; vgl. zum Ganzen: Stellungnahme RZ EJPD vom 22.7.1998, Seite 3 und 4), während andere Bundesorgane darauf hinweisen, dass durch eine gemeinsame Führung im Bereich der IT-Infrastruktur (Reorganisation der Informatik in der Bundesverwaltung; Projekt NOVE-IT) die organisatorischen Voraussetzungen für die Zusammenlegung der Netzwerke KOMBV-KTV und WAN-EJPD geschaffen würden (vgl. Stellungnahme BfI vom 22.7.1998, Seite 2, Ziffer 3).

Der Experte unterstützt die im Bericht der Verwaltungskontrolle des Bundesrates festgehaltene Empfehlung, die beiden logisch getrennten Bundesnetze KOMBV-KTV und EJPD-WAN zusammenzulegen. Da zum Teil sehr divergierende technische Argumente und Ansichten von beteiligten Bundesstellen eingebracht werden, kann der Beizug und die Beauftragung einer externen Kommunikationsunternehmung durch den Bundesrat zu einer Entspannung der zum Teil emotional belasteten Fragestellung führen. Doppelspurigkeiten bei der Kommunikationsinfrastruktur des Bundes sind sowohl wirtschaftlich wie auch sicherheitstechnisch kaum vertretbar. In diesem Streitpunkt ist nach nunmehr jahrelangen Diskussionen in jedem Falle aber – ob mit oder ohne Beizug einer externen Beratungsfirma - ein schneller und klarer Führungsentscheid des Bundesrates notwendig.

358 Empfehlungen und Massnahmenvorschläge

Aufgrund der im Kapitel 3.5 für das Rechenzentrum EJPD dargestellten Situation stehen folgende vier Massnahmen/Empfehlungen im Vordergrund:

1. Der Standort des Rechenzentrums (Zollikofen) ist sobald als möglich unter Ausschöpfung aller bundesinternen oder bundesexternen Möglichkeiten und Varianten zu wechseln.

2. Das Rechenzentrum EJPD ist so rasch als möglich einer erneuten externen Sicherheitsüberprüfung zu unterziehen, in welcher die ergriffenen Massnahmen auditiert und allenfalls noch bestehende Sicherheitslücken erneut aufgezeigt werden. Den Sicherheitsaspekten des Rechenzentrums EJPD ist bezüglich Ressourcenbedarf des RZ EJPD höherer Stellenwert als dem Projekt NOVE-IT beizumessen.

3. Die Mitarbeitenden des Rechenzentrums sind entsprechend dem Antrag der Leitung des RZ EJPD sofort einer Sicherheitsprüfung zu unterziehen. Das EJPD hat für eine Ergänzung der entsprechenden Liste durch den Bundesrat zu sorgen.

4. Der Bundesrat hat – allenfalls unter Beizug einer externen Spezialfirma - die notwendige Beurteilung der verschiedenen Einwände für oder gegen eine Zusammenlegung der beiden Bundesnetze KOMBV-KTV und EJPD-WAN vorzunehmen und gestützt darauf umgehend über das weitere Vorgehen (Zusammenlegung oder Aufrechterhaltung des Parallelbetriebs) zu entscheiden.

4 Abschliessende Gesamtbeurteilung

Im Rahmen dieses Expertenberichtes ist die Praxis der zuständigen Bundesstellen bei der Erteilung von Online-Anschlussbewilligungen im Polizeibereich untersucht und dargestellt worden. Es sind lediglich vier Informatik-Systeme (RIPOL, DOSIS, ISIS, ZAR) sowie der Bereich des Systembetriebs durch das Rechenzentrum EJPD begutachtet worden. Obwohl noch zahlreiche weitere Informations-Systeme im Polizeibereich existieren, bei welchen ebenfalls Online-Anschlüsse von Drittbenutzern realisiert werden, lassen sich doch aufgrund dieser vier ausgewählten Informatik-Systeme gewisse übereinstimmende Erkenntnisse herausschälen.

Die Regelung der Bewilligung von Online-Anschlüssen ist bisher eher untergeordnet behandelt worden. In allen Bereichen ist die Frage durch eine stetige Weiterdelegation an die unterste operative Verwaltungseinheit oder im Rahmen der Wahrnehmung der operativen Verantwortung durch die entsprechende Verwaltungseinheit gelöst worden. Eine für alle Informationssysteme des Polizeiwesens übergeordnete und generelle Regelung der Bewilligungspraxis mit dem dabei zu beachtenden Verfahren, den adäquaten Zuständigkeiten und der Beachtung des Grundsatzes der Unabhängigkeit der Bewilligungsinstanz fehlt. Dies bedeutet nicht, dass die verantwortlichen Verwaltungseinheiten schlecht oder ungenügend gearbeitet hätten. Es zeigt aber, dass dem Bereich der Anschlussbewilligungen nicht der Stellenwert beigemessen wurde, welchem ihm im sehr sensiblen, mit besonders schützenswerten Personendaten und Persönlichkeitsprofilen arbeitenden Polizeiinformationsbereich eigentlich zukommen sollte. Die strengen gesetzlichen Voraussetzungen zur Nutzung von Polizeiinformationssystemen (Notwendigkeit, Verhältnismässigkeit und Zweckmässigkeit) dürfen nicht ausgehöhlt werden. Sie müssen in einem klar definierten Verfahren, das den Anspruch auf Unabhängigkeit und Berücksichtigung der gesetzlichen Voraussetzungen sicherstellt, garantiert werden. Besondere Schwierigkeiten ergeben sich dabei in der Zusammenarbeit zwischen dem Bund und den kantonalen oder kommunalen Benutzerorganisationen, wenn diese Bundesaufgaben wahrnehmen und dafür auf die Polizeiinformationssysteme zugreifen. Hier ist durch ein entsprechendes Online-Bewilligungsverfahren sicherzustellen, dass auch die politische Führung von den Anschlussbegehren ihrer unterstellten Behörden Kenntnis hat und ihnen zustimmt. Anderseits müssen auch in diesen Bereichen die datenschutz- und datensicherheitsrelevanten Massnahmen durchgesetzt werden können. Dazu sowie für die Durchführung von sogenannten Pilotprojekten mit besonders schützenswerten Personendaten bedarf es neuer gesetzlicher Grundlagen. Bestehende Online-Anschlüsse sind einer dauernden Ueberprüfung hinsichtlich Notwendigkeit und Verhältnismässigkeit zu unterstellen. Nicht oder wenig benutzte Online-Anschlüsse sind aufzuheben. Das Rechenzentrum EJPD ist als Betreiberin und Entwicklerin der Polizeiinformationssysteme in die Gesamtbetrachtung einzuschliessen. Hier sind insbesondere den Fragen Standortsicherheit in Zollikofen, Sicherheitsprüfung aller RZ-Mitarbeitenden, umgehend neue, externe Sicherheitsprüfung und Zusammenlegung der logisch getrennten Kommunikationsnetze KOMBV-KTV und EJPD-WAN die notwendige Beachtung zu schenken. Im Einzelnen wird auf die jeweiligen Kapitel „Empfehlungen und Massnahmenvorschläge“ verwiesen.

Nach Abschluss der Bearbeitung der vorliegenden Thematik und entsprechender Behandlung in der Geschäftsprüfungskommission gehen alle im Besitze des Experten befindlichen Unterlagen an die Parlamentarische Verwaltungskontrollstelle (PVK) zurück.

Luzern, 30. Juli 1998

Lic.iur. Lukas Fässler
Rechtsanwalt

Nachtrag 1

Auswertungen und Zusammenfassung des verwaltungsinternen Vernehmlassungsverfahrens

zum Expertenbericht

Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens vom 30. Juni 1998

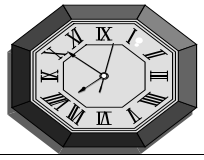
Dokument	G:\DatALL\Fl\Eigene Dateien 04.98\Eigene Dateien\ONLINE\Nachtrag 1 zum Expertenbericht.doc
Version:	1.0
Datum:	20/11/1998
Ersetzt Dokument vom:	
Autor:	© lic.iur. Lukas Fässler, Rechtsanwalt, Hirschmattstrasse 36, 6002 Luzern
Letzte Änderung von:	30.7.1998
Autorisiert:	Sektion Behörden der GPK-S; PVK; betroffene Bundesämter sowie GS EJPD und GS FD; lic.iur. Lukas Fässler, Luzern
Freigabe am:	1.8.1998

Inhaltsverzeichnis

1 EINLEITUNG

Der Bericht „Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens“ zuhanden der Sektion „Behörden“ der Geschäftsprüfungskommission des Ständerates wurde vom Experten per 30. Juni 1998 abgeschlossen. Am 1. und 2. Juli 1998 orientierte der Experte mündlich das Bundesamt für Polizeiwesen, die Bundespolizei, das Bundesamt für Ausländerfragen sowie das Rechenzentrum EJPD über die wesentlichen Berichtsergebnisse. Im Anschluss an diese Erläuterung wurde das bundesverwaltungsinterne Vernehmlassungsverfahren eröffnet. Die Frist zur Stellungnahme lief bis 23. Juli 1998.

Nachfolgende Uebersicht zeigt jene Bundesorgane, welche zur Stellungnahme eingeladen wurden und davon in schriftlichen Eingaben Gebrauch gemacht haben:

Vernehmlassungs-einladung	Mündliche Expertenerläuterung	Schriftliche Stellungnahme	Bemerkungen
EJPD Generalsekretariat 2.7.1998	Keine	~~22.7.1998 Keine materielle Stellungnahme Weiterleitung der Aemterstellungnahmen~~	Keine
FD Generalsekretariat 2.7.1998	Keine	~~Keine~~	Keine
Bundesamt für Informatik 2.7.1998	Keine	22.7.1998 ☑	Keine
Eidg. Datenschutz-beauftragter 2.7.1998	Keine	7.7.1998 ☑	**Fristverlängerung bis 31.8.1998** 
Rechenzentrum EJPD 1.7.1998	Mündliche Erläuterung mit Abgabe des schriftlichen Berichts am 1.7.1998 an Herrn Többen	22.7.1998 ☑	Keine
Bundespolizei	Mündliche Erläuterung mit Abgabe des schriftlichen Berichts am 1.7.1998 an Herrn Herrli	21.7.1998 ☑	Keine

Bundesamt für Polizeiwesen 2.7.1998	Mündliche Erläuterung mit Abgabe des schriftlichen Berichts am 1.7.1998 an Herrn Lobsiger	22.7.1998 	Keine
Bundesamt für Ausländerfragen 2.7.1998	Mündliche Erläuterung mit Abgabe des schriftlichen Berichts am 1.7.1998 an Herrn Direktor Huber	21.7.1998 	Keine

2 STELLUNGNAHMEN IM VERNEHMLASSUNGSVERFAHREN

Soweit die Stellungnahmen der Bundesorgane Ergänzungen oder Anpassungen materiellen oder formellen Inhalts enthalten, sind diese in der Version 4.0 des Expertenberichts vom 30.7.1998 berücksichtigt worden.

Ergänzende Argumentationen sowie den Empfehlungen und Massnahmen-vorschlägen des Expertenberichts entgegenstehende Meinungsäusserungen sind
– soweit überhaupt vorhanden - den entsprechenden Anhängen 1-5 in vorliegender Zusammenfassung zu entnehmen.

Zusammenfassend kann festgestellt werden, dass die antwortenden Bundesorgane den Tatsachendarstellungen, Grundsätzen, Empfehlungen und Massnahmenvorschlägen zustimmen. Es ergeben sich einzelne Präzisierungen in den Abläufen sowie ergänzende Ausführungen zu tatsächlichen und rechtlichen Gegebenheiten (insbesondere zu den seit Berichtsabschluss per 1.7.1998 in Kraft gesetzten neuen gesetzlichen Grundlagen [BWIS]), die jedoch insgesamt die Aussagen des Expertenberichts nicht in Frage stellen.

Besonders hervorzuheben ist die in jeder Phase der Expertenarbeiten vorhandene konstruktive Zusammenarbeit mit den Verantwortlichen der untersuchten Bundesorgane. Ihre Mitarbeit war insbesondere im Rahmen der Zusammenstellung aller notwendigen Unterlagen, der Aufnahme der IST-Situation (chronologischer Raster) sowie bei den Interviews zeitintensiv und sehr wertvoll. Besonders hervorzuheben ist die Stellungnahme des Bundesamtes für Ausländerfragen, in welcher die vom Experten erarbeitete Prozessbeschreibung zum Online-Bewilligungsverfahren (Seite 67 und 68 des Expertenberichts) bereits überarbeitet und in angepasster Form beigelegt wurde.

11 Bundespolizei

Stellungnahme vom 21.7.1998

12 Bundesamt für Ausländerfragen

Stellungnahme vom 21.7.1998 inkl. ergänzte Prozessbeschreibung für das Online-Bewilligungsverfahren

13 Bundesamt für Polizeiwesen

Stellungnahme vom 22.7.1998

14 Rechenzentrum EJPD

Stellungnahme vom 22.7.1998

15 Bundesamt für Informatik

Stellungnahme vom 22.7.1998

16 Eidgenössischer Datenschutzbeauftragter

Stellungnahme vom 22.7.1998

Luzern, 30. Juli 1998

Lic.iur. Lukas Fässler
Rechtsanwalt