GESETZBLATT

der Deutschen Demokratischen Republik

BERLIN, 22. MÄRZ 1989 · SONDERDRUCK NR. 1316

Anordnung zur Gewährleistung der Datensicherheit

vom 23. Februar 1989

Herausgeber: Sekretariat des Ministerrates der Deutschen Demokratischen Republik – Verlag: (610/62) Staatsverlag der Deutschen Demokratischen Republik – Lizenz-Nr. 751 – Gesamtherstellung: Staatsdruckerei der Deutschen Demokratischen Republik (Rollenoffsetdruck)

Anordnung zur Gewährleistung der Datensicherheit

vom 23. Februar 1989

Zur Gewährleistung der Datensicherheit in der Deutschen Demokratischen Republik wird im Einvernehmen mit den Leitern der zuständigen zentralen Staatsorgane folgendes angeordnet:

§ 1

Geltungsbereich

(1) Diese Anordnung regelt Aufgaben, Rechte und Pflichten sowie Verfahren zur Gewährleistung von Sicherheit, Ordnung und Geheimnisschutz bei der Anwendung der elektronischen Datenverarbeitung und -übertragung einschließlich der Datenerfassung, -speicherung und -ausgabe sowie des Datentransports (nachfolgend Datensicherheit genannt).

(2) Diese Anordnung gilt für

- Staatsorgane,
- Kombinate, wirtschaftsleitende Organe, Betriebe, Genossenschaften, Einrichtungen und gesellschaftliche Organisationen (nachfolgend Staatsorgane und Betriebe genannt).

(3) Für die Übertragung von Daten durch die Teilnahme am öffentlichen Datenübertragungsdienst im Fernmeldenetz der Deutschen Post sowie für die Übertragung von Daten durch Nutzung der von der Deutschen Post überlassenen Übertragungswege sind die dazu erlassenen Bestimmungen anzuwenden.[1]

(4) Weitere rechtliche Regelungen zu Sicherheit, Ordnung und Geheimnisschutz einschließlich des Gesundheits- und Arbeitsschutzes sowie Brandschutzes, sofern sie die Durchführung der elektronischen Datenverarbeitung betreffen, sind entsprechend für die Datensicherheit anzuwenden.

§ 2

Begriffsbestimmungen

Im Sinne dieser Anordnung gelten folgende Begriffsbestimmungen:

1. **Datensicherheit** ist Bestandteil der Sicherheit, der Ordnung und des Geheimnisschutzes der sozialistischen Gesellschaft. Sie betrifft den Datenverarbeitungsprozeß mit seinen notwendigen Bestandteilen sowie die volkswirtschaftlichen und gesellschaftlichen Aufgaben und Prozesse in dem Maße, wie diese über die Verarbeitung der Daten mittels Rechentechnik beeinflußt werden können. Darin ist der Schutz von Daten der Bürger in Übereinstimmung mit den bestehenden Rechtsvorschriften einbezogen. Datensicherheit ist für eine bestimmte EDV-Anwendung gegeben, wenn die Erfassung, Übertragung, Speicherung, Verarbeitung und Ausgabe sowie der Transport von Daten und Informationen entsprechend den dafür geltenden Rechtsvorschriften, technischen, technologischen und organisatorischen Normen und Festlegungen erfolgt und damit die volle Funktionsfähigkeit der Rechentechnik und die effektive Nutzung der elektronischen Datenverarbeitung unterstützt wird. Die Verhinderung von Störungen, vor allem im Ergebnis von
   - unberechtigten Manipulationen sowie
   - Ausforschungen, Offenbarungen bzw. unberechtigten Kenntnisnahmen

   der Daten, Software oder Vorschriften und
   - Beschädigungen bzw. Zerstörungen
   - unberechtigten Nutzungen und Veränderungen sowie
   - Diebstählen

   der Datenträger, Software, Rechentechnik oder Übertragungstechnik, ist zu gewährleisten.
2. **Rechentechnik** sind technische Geräte zum maschinellen Ausführen arithmetischer und logischer Verknüpfungen von Daten und Informationen, wie EDV-Anlagen, Kleindatenverarbeitungsanlagen, Büro-/Personalcomputertechnik und gleichartige Geräte sowie Terminals.
3. **Zentrale Rechentechnik** sind in Einrichtungen der Datenverarbeitung einzeln oder im Rechnerverbund installierte EDV-Anlagen des Einheitlichen Systems elektronischer Rechentechnik (ESER), Kleindatenverarbeitungsanlagen des Systems der Kleinrechner (SKR) sowie gleichartige Rechentechnik.
4. **Dezentrale Rechentechnik** sind Büro-/Personalcomputertechnik und gleichartige Geräte sowie Terminals, die einzeln, im Verbund untereinander sowie mit zentraler Rechentechnik betrieben werden können.
5. **Datenträger** sind Speichermedien, die Daten und Informationen in einer maschinenlesbaren Form aufbereitet enthalten oder aufnehmen können, wie z. B. programmierbare elektronische Bauelemente, Lochbänder und -karten, Magnetbänder, Magnetbandkassetten, Disketten, Wechsel-, Fest- und optische Platten.
6. **Einrichtungen der Datenverarbeitung** sind Betriebe bzw. strukturelle Einheiten von Staatsorganen und Betrieben zur Durchführung von Datenverarbeitungsprozessen mit zentraler Rechentechnik.
7. **Objekte der Datenverarbeitung** sind Gebäude, Raumgruppen bzw. Räume, in denen Rechen- und Übertragungstechnik und die für ihre Funktion notwendigen Anlagen, Einrichtungen, Software usw. untergebracht sind. Bei zentraler Rechentechnik bestehen sie in der Regel aus mehreren Räumen, sind funktionell untergliedert und besitzen eine entsprechende Objektbegrenzung. Bei dezentraler Rechentechnik bestehen sie in der Regel aus mindestens einem funktionell oft mehrfach genutzten Raum.
8. **Übertragungstechnik** ist die Gesamtheit der technischen Nachrichtenmittel für die elektronische Datenübertragung beim Anwender bis zur festgelegten Schnittstelle der Deutschen Post.
9. **Lokale Rechnernetze** sind logische und physische Verknüpfungen von Rechentechnik innerhalb eines begrenzten Geländes. Sie dienen der Übertragung von Informationen und werden unter Verantwortung des Nutzers als genehmigungsfreie Fernmeldeanlagen betrieben. Die Datenübertragung zur Kommunikation mit Rechentechnik außerhalb der lokalen Rechnernetze erfolgt unter Nutzung des einheitlichen staatlichen Fernmeldenetzes der Deutschen Post über eine definierte Schnittstelle und ist genehmigungspflichtig.

§ 3

Verantwortung der Leiter zur Gewährleistung der Datensicherheit

(1) In die Vorbereitung neuer Aufgaben und Vorhaben der elektronischen Datenverarbeitung und -übertragung, die Entwicklung neuer EDV-Anlagen, Kleindatenverarbeitungsanlagen und andere Mittel der elektronischen Datenverarbeitung sowie Software sind Voraussetzungen für Lösungen zur Gewährleistung der Datensicherheit einzubeziehen. Die sich daraus ergebenden personellen, organisatorischen und materiell-technischen Konsequenzen sind herauszuarbeiten, mit den Erneuerungspässen, Pflichtenheften und Grundsatzentscheidungen zu bestätigen sowie in die Pläne einzuordnen.

(2) Die Minister, die Leiter der anderen zentralen Staatsorgane, die Vorsitzenden der örtlichen Räte, die Generaldirektoren der Kombinate, die Leiter der wirtschaftsleitenden Organe, die Direktoren der Betriebe, die Leiter der Einrichtungen sowie die Vorsitzenden der Genossenschaften, die Leitungen bzw. Vorstände der gesellschaftlichen Organisationen (nachfolgend Leiter der Staatsorgane und Betriebe genannt) sind für die Gewährleistung der Datensicherheit verantwortlich. Sie haben dazu entsprechend den spezifischen Anforderungen die erforderlichen Regelungen und Weisungen

---

[1] Z. Z. gelten:
- Anordnung vom 28. Februar 1986 über den Datenübertragungsdienst – Datenübertragungs-Anordnung – (Sonderdruck Nr. 1268 des Gesetzblattes),
- Anordnung vom 28. Februar 1986 über leitungsgebundene Fernmeldeanlagen für den nichtöffentlichen Fernmeldeverkehr und für das Überlassen von Übertragungswegen (Sonderdruck Nr. 1268 des Gesetzblattes).

zu erlassen und deren Durchsetzung im Verantwortungsbereich zu kontrollieren. Bei vorgesehener Verarbeitung von Staatsgeheimnissen sind die spezifischen Regelungen und Weisungen mit der zuständigen Dienststelle des Ministeriums für Staatssicherheit abzustimmen.

(3) Die Datensicherheit ist in die technologischen Regime und die Arbeitsabläufe zu integrieren. Durch die Leiter der Staatsorgane und Betriebe sind die dafür erforderlichen organisatorischen Voraussetzungen zu schaffen sowie die Anwendung geräte- und softwareseitiger Sicherheitsmaßnahmen zu gewährleisten.

(4) Der konsequente Schutz der Staatsgeheimnisse und der anderen geheimzuhaltenden Informationen ist zu gewährleisten. Es sind nur dafür zugelassene Mittel, Methoden und Verfahren anzuwenden. Bewährte Sicherheitsmaßnahmen sind umfassend in den Staatsorganen und Betrieben zu nutzen.

(5) Die Leiter der Staatsorgane und Betriebe können, in Abhängigkeit von der Bedeutung der Maßnahmen der Datensicherheit, ausgewählte Aufgaben sowie Rechte und Pflichten zur Gewährleistung der Datensicherheit auf andere Leiter im Staatsorgan oder Betrieb übertragen. Die Aufgaben sowie Rechte und Pflichten sind in den Regelungen und Weisungen entsprechend Abs. 2 aufzunehmen.

(6) Die Leiter der Staatsorgane und Betriebe haben zu veranlassen, daß die Gewährleistung der Datensicherheit hinsichtlich ihrer Wirksamkeit und Effektivität regelmäßig analysiert wird, bestehende Schwachstellen herausgearbeitet und die sich daraus ergebenden Maßnahmen realisiert werden.

(7) Mit den Maßnahmen zur Gewährleistung der Datensicherheit sind ein straffes Arbeitsregime und die effektive Nutzung der Rechentechnik zu unterstützen sowie die persönlichen Daten der Bürger zu schützen. Es ist durch differenzierte Maßnahmen Verletzungen der Datensicherheit entgegenzuwirken. Bei Notwendigkeit sind Maßnahmen zur Verminderung der unerwünschten Aus- und Einstrahlung durchzuführen.

(8) Die Datensicherheit ist durch einen Komplex von personellen, organisatorischen, sicherheitstechnischen, programm- und gerätetechnischen und baulichen Maßnahmen zu realisieren. Die für die Maßnahmen erforderlichen Aufwendungen sind in Übereinstimmung mit der Analyse der Sicherheitsanforderungen rechtzeitig zu planen.

(9) In der elektronischen Datenverarbeitung und -übertragung einschließlich der Datenerfassung, -speicherung und -ausgabe sind Werktätige einzusetzen, die entsprechend der ihnen übertragenen Verantwortung und Aufgabenstellung die kadermäßigen Voraussetzungen erfüllen. Durch Schulungen, Belehrungen und andere erzieherische Maßnahmen sind sie zur bewußten Einhaltung der Maßnahmen zur Gewährleistung der Datensicherheit zu befähigen.

(10) Durch die Leiter der Staatsorgane und Betriebe sind zur Unterstützung bei der Realisierung ihrer Aufgaben für die Gewährleistung der Datensicherheit die Beauftragten für Datensicherheit, die Beauftragten für den Geheimnisschutz, Sicherheitsaktive und Kontrollgruppen einzubeziehen.

(11) Verletzungen der Datensicherheit sind konsequent aufzudecken. Es sind unverzüglich Maßnahmen einzuleiten, die die Datensicherheit wiederherstellen. Die zuständigen Organe sind nach den festgelegten Meldepflichten zu informieren. Die Verletzungen der Datensicherheit in den Staatsorganen und Betrieben der Volkswirtschaft sind über die Meldepflicht bei außergewöhnlichen Vorkommnissen hinaus dem Leiter der Arbeitsgruppe für Organisation und Inspektion beim Ministerrat mitzuteilen. Das betrifft nicht die Nationale Volksarmee, die Grenztruppen der DDR, die Zivilverteidigung und die anderen Schutz- und Sicherheitsorgane. Es sind Untersuchungen zu veranlassen. Die Ursachen und begünstigenden Bedingungen sind aufzudecken und zu beseitigen. Die für die Verletzung der Datensicherheit verantwortlichen Personen sind festzustellen und die Durchsetzung ihrer Verantwortlichkeit ist entsprechend den Rechtsvorschriften einzuleiten. Die Verletzungen der Datensicherheit sind auszuwerten.

§ 4

Festlegungen zu Sicherheitsstufen

(1) Ergeben sich für die Datensicherheit durch Bewertung und Einschätzung des Umfanges von Schäden und Störungen Sicherheitserfordernisse, die über die generell für die Datensicherheit festgelegten Anforderungen hinausgehen, sind durch die Leiter der Staatsorgane und Betriebe für Objekte der Datenverarbeitung bzw. für Datenträger, Software, Rechen- und Übertragungstechnik Sicherheitsstufen gemäß den Absätzen 2 und 3 festzulegen. Ergibt die Prüfung der Sicherheitsanforderungen, daß die Datensicherheit am zweckmäßigsten durch die Einstufung des Objektes der Datenverarbeitung zu gewährleisten ist, so ist dieses in die Sicherheitsstufe 1 oder 2 einzustufen. Mit der Einstufung sind die in den §§ 10 und 11 festgelegten Maßnahmen als Mindestanforderungen zu realisieren. Die Entscheidung ist aktenkundig zu begründen.

(2) Die Sicherheitsstufe 1 ist festzulegen, wo

- bei der Verarbeitung von Daten und Informationen durch deren Manipulation, Ausforschung, Offenbarung bzw. Kenntnisnahme oder Zerstörung Leben und Gesundheit von Menschen gefährdet und/oder Anlagen oder andere gesellschaftliche Werte geschädigt bzw. gefährdet und damit volkswirtschaftliche und gesellschaftliche Ziel- und Aufgabenstellungen negativ beeinflußt werden können, bzw.
- Daten und Informationen mit dem Geheimhaltungsgrad VVS bearbeitet werden.

(3) Die Sicherheitsstufe 2 ist festzulegen, wo

- bei der Verarbeitung von Daten und Informationen durch deren Manipulation, Ausforschung, Offenbarung bzw. Kenntnisnahme oder Zerstörung Leben und Gesundheit von Menschen, volkswirtschaftliche Anlagen, Maschinen, Geräte und Ausrüstungen oder andere gesellschaftliche Werte erheblich geschädigt bzw. gefährdet und damit volkswirtschaftliche und gesellschaftliche Ziel- und Aufgabenstellungen beeinträchtigt werden können, bzw.
- Daten und Informationen mit dem Geheimhaltungsgrad VVS und GVS regelmäßig bearbeitet werden.

Gewährleistung der Datensicherheit bei der Softwareentwicklung

§ 5

Arbeit mit Pflichtenheften und Erneuerungspässen

(1) Die Zielstellungen zur Gewährleistung der Datensicherheit sind projektbezogen für Basis- und Anwendungssoftware mit dem Pflichtenheft und Erneuerungspaß bzw. dem Entwicklungsauftrag des Generaldirektors und anderer berechtigter Leiter (in der Nationalen Volksarmee, den Grenztruppen der DDR, der Zivilverteidigung und den anderen Schutz- und Sicherheitsorganen gelten die entsprechenden Führungsdokumente) festzulegen. Auf Grund der Spezifik der Aufgaben können diese als Anlage zum Pflichtenheft bzw. Entwicklungsauftrag dokumentiert werden. Die Verteidigung dieser Aufgaben kann vor einem eingeschränkten Personenkreis erfolgen.

(2) Bei den Verteidigungen zu den Entwicklungsergebnissen entsprechend den Vorgaben des Pflichtenheftes und Erneuerungspasses bzw. Entwicklungsauftrages ist die Realisierung der Maßnahmen zur Gewährleistung der Datensicherheit nachzuweisen.

§ 6

Aufgaben bei der Softwareentwicklung

(1) Im Prozeß der Softwareentwicklung sind die Erarbeitung der Basis- und Anwendungssoftware sowie die Erarbeitung bzw. Implementierung von Algorithmen und Programmen zur Gewährleistung der Datensicherheit im Verarbeitungsprozeß der Daten und Informationen entsprechend den im Pflich-

tenheft bzw. im Entwicklungsauftrag getroffenen Festlegungen zur Datensicherheit vorzubereiten und durchzuführen.

(2) Der Auftraggeber ist verantwortlich für die Bestimmung der Staatsgeheimnisse und der anderen geheimzuhaltenden Informationen sowie die Festlegung der anderen besonders zu schützenden Dienstsachen. Der Softwareentwickler kann in diesen Prozeß einbezogen werden.

(3) Der für den Entwicklungsprozeß zuständige Leiter hat die zu nutzenden Komponenten der Basissoftware, die nachzunutzenden Komponenten der Anwendungssoftware, die Projektierungsmethodik, erforderlichenfalls die Programmiersprache und die Vorschriften zur Dokumentation in den Projektierungsstufen sowie die bei der Projektierung anzuwendende Hardware festzulegen. Die in der Basis- und Anwendungssoftware vorhandenen Algorithmen und Programme zur Sicherung von Daten und Informationen sind in Übereinstimmung mit den Anforderungen zur Datensicherheit anzuwenden. Entsprechend den spezifischen Bedingungen sind in den Staatsorganen und Betrieben eigenverantwortlich zusätzliche softwareseitige Maßnahmen zu realisieren. Die Maßnahmen sind entsprechend dem Entwicklungsstand der Rechentechnik und Software weiter zu vervollkommnen.

(4) Für die Kontrolle der Maßnahmen zur Datensicherheit ist zu gewährleisten, daß der Datenverarbeitungsprozeß in erforderlichem Umfang rekonstruierbar ist.

(5) Die Durchführung der Programmtests und die Erprobung der Programmabläufe mit dienstlichen Daten sind zulässig, sofern die Datensicherheit gewährleistet ist und der Auftraggeber zustimmt.

§ 7

Dokumentation der Entwicklungsergebnisse

(1) Die Dokumentationen (Projektdokumentation, Entwicklungsdokumentation, Anwenderdokumentation) der Software sind erforderlichenfalls geheimzuhalten und durch die berechtigten Leiter der Staatsorgane und Betriebe in Geheimhaltungsgrade einzustufen.

(2) Die Sicherheitskomponenten der Software, d. h., Algorithmen bzw. Programme zur Gewährleistung der Datensicherheit im Datenverarbeitungsprozeß, vor allem

- spezielle Sicherheitskomponenten für Betriebssysteme sowie Datenbank- und Informationsrecherchesysteme der Rechentechnik,
- Sicherheitskomponenten der Software für Rechentechnik, die an Schnittstellen der Betriebssysteme sowie Datenbank- und Informationsrecherchesysteme angepaßt werden,
- Kennwortroutinen und Dateien mit Zugriffsinformationen für Dialog- und Terminalarbeit,
- programmierte Kontrollen für die Sicherung von Stammdaten,
- Programme des automatischen Operators und
- programmierte Kontrollen für den Zugriff auf Dateien und Stammdaten sowie für den Aufruf spezieller Verarbeitungsprogramme,

sind auf die möglichen Auswirkungen durch Entwenden, unberechtigten Zugriff, Manipulation oder sonstigen Mißbrauch zu prüfen und erforderlichenfalls geheimzuhalten.

§ 8

Pflege der Software

(1) Die wissenschaftlich-technischen Arbeiten zur Aktualisierung und Änderung von Programmen und Dokumentationen der Basis- und Anwendungssoftware (Pflege der Software) und die Änderung der Dokumentationen sind nur von den dazu berechtigten und beauftragten Personen durchzuführen.

(2) Die durchgeführten Pflegearbeiten der Software sind in den Dokumentationen nachzuweisen.

Gewährleistung der Datensicherheit bei der Vorbereitung des Einsatzes der Rechentechnik

§ 9

Vorbereitung des Einsatzes der Rechentechnik

(1) Bei der Vorbereitung des Einsatzes der Rechentechnik sind die Anforderungen an die Datensicherheit zu analysieren und zur Verhinderung von Störungen aller Art erforderliche Maßnahmen für den Betrieb der Rechentechnik vorzusehen. Der ausreichende Schutz der Daten, Datenträger, Software und Rechentechnik vor Beschädigung, Mißbrauch und Verlust ist in Übereinstimmung mit § 3 Abs. 5 durch die Leiter zu sichern, in deren Verantwortungsbereich die Rechentechnik unmittelbar installiert wird.

(2) Rechentechnik, die für die Bearbeitung von Staatsgeheimnissen vorgesehen ist, ist unter Berücksichtigung der Grenzwertklassen[2] so zu installieren, daß Staatsgeheimnisse durch unerwünschte Ausstrahlung Unbefugten nicht zur Kenntnis gelangen können. Gegebenenfalls ist ein Gutachten durch das Zentralamt für Funkkontroll- und Meßdienst der Deutschen Post zu beantragen. Die Wirksamkeit der Maßnahmen zur Verminderung der unerwünschten Ausstrahlung ist regelmäßig zu überprüfen.

(3) Bei der Investitionsvorbereitung für den Einsatz von Rechentechnik, die für die Bearbeitung von Staatsgeheimnissen vorgesehen wird, ist durch den Investitionsauftraggeber mit dem Hersteller bzw. Aufsteller im Rahmen des Leistungsvertrages die Bereitstellung von Rechentechnik gemäß den Grenzwertklassen zu vereinbaren. Das Zertifikat für die Rechentechnik ist dem Auftraggeber vom Auftragnehmer schriftlich zu übergeben. Ist der Einsatz der Rechentechnik in einem elektromagnetisch geschirmten Raum vorgesehen, ist kein Zertifikat für die Rechentechnik notwendig, wenn die Ausstrahlungssicherheit des Raumes in einem Zertifikat bestätigt wurde. Bei der Investitionsvorbereitung für den Einsatz importierter Rechentechnik sind durch die Nutzer bei vorgesehener Verarbeitung von Staatsgeheimnissen eigenverantwortlich Maßnahmen, die die vorgenannten Bedingungen erfüllen, einzuleiten. Den Maßnahmen sind die durch das Zentralamt für Funkkontroll- und Meßdienst der Deutschen Post entsprechend den durchgeführten Messungen gegebenen Hinweise zugrunde zu legen.

§ 10

Anforderungen aus der Einstufung von Objekten der Datenverarbeitung mit zentraler Rechentechnik

(1) Bei der Festlegung der Sicherheitsstufe 1 sind die Räume

- der Erfassung der Daten und Informationen der Staatsgeheimnisse,
- der Arbeitsvorbereitung der Datenverarbeitungsprozesse,
- der Datenverarbeitungsprozesse und für die Datenübertragung,
- für die Aufbewahrung und Archivierung von Datenträgern sowie
- mit technischen Betriebsmitteln

Sperrbereiche. Die Räume mit den EDV-Anlagen und -Geräten der 1. Peripherie sowie die Räume zur Aufbewahrung und Archivierung der Datenträger sind fensterlos auszuführen. Wird bereits vorhandene Bausubstanz genutzt, in der sich die Fenster dieser Räume nicht zusetzen lassen, sind die Fenster durch Gitter gegen Einstieg und Einwurf zu sichern. Der Einstieg über die Installationsschächte ist durch bautechnische Maßnahmen zu verhindern.

(2) Bei der Festlegung der Sicherheitsstufe 2 ist das Objekt der Datenverarbeitung zum Sperrbereich zu erklären. Räume mit Terminals für die Dialogarbeit außerhalb des Objektes der Datenverarbeitung sind ebenfalls als Sperrbereiche festzulegen, wenn durch organisatorische, technologische u. a. Maßnahmen der Zugriff zu Daten, für die keine Zugriffs-

[2] Z. Z. gilt der Standard TGL – V 40275.

berechtigung besteht, nicht ausgeschlossen werden kann. Die Räume, in denen die Datenträger und Drucklisten, die als Staatsgeheimnisse eingestuft sind, zentral aufbewahrt werden, sind als VS-Räume entsprechend den Rechtsvorschriften zu sichern. Für die Objekte der Datenverarbeitung ist eine eigene, von anderen Nutzern unabhängige Strom- und Wasserzuführung sowie Klimatisierung vorzusehen. Bei bestehenden Einrichtungen der Datenverarbeitung ohne diese Unabhängigkeit sind diese Maßnahmen bei Neuinvestition, Modernisierung und Rekonstruktion durchzuführen. Innerhalb des Sperrbereiches sind folgende Räume untereinander abzugrenzen und zu sichern sowie die Zutrittsberechtigung festzulegen:

1. der Raum, in dem die EDV-Anlage und -Geräte der 1. Peripherie installiert sind,
2. der Raum zur Aufbewahrung der Datenträger,
3. der Raum für die Arbeitsvor- und -nachbereitung,
4. die Räume, in denen Terminals für die Dialogverarbeitung installiert sind,
5. der Raum für die Datenerfassung von Staatsgeheimnissen,
6. die technischen Betriebsräume,
7. die Räume für die Aufstellung von Chiffriertechnik.

(3) Die Kontrollmaßnahmen zur Verhinderung der unerwünschten Ausstrahlung sind mit dem Zentralamt für Funkkontroll- und Meßdienst der Deutschen Post abzustimmen.

§ 11

Anforderungen aus der Einstufung von Objekten der Datenverarbeitung mit dezentraler Rechentechnik

(1) Die Objekte der Datenverarbeitung mit dezentraler Rechentechnik, für die eine Einstufung in Sicherheitsstufen erfolgte, sind generell so zu sichern, daß die Beschädigung, der Mißbrauch und der Verlust der Daten, Datenträger, Software, Rechentechnik und Übertragungstechnik ausgeschlossen wird. Das schließt die Verhinderung des unberechtigten Fernzugriffs zu Daten und Informationen ein.

(2) Bei der Verarbeitung von Daten und Informationen ist grundsätzlich zu sichern, daß unbefugte Personen die Ausgabe der Daten und Informationen (Bildschirm bzw. Druckliste) nicht einsehen können. Bei der Verarbeitung von Staatsgeheimnissen ist die Einsichtnahme unbefugter Personen auszuschließen.

(3) Die Räume und Behältnisse, in denen Datenträger für die dezentrale Rechentechnik aufbewahrt werden, sind entsprechend den Sicherheitserfordernissen der gespeicherten Daten und Informationen zu schützen.

Gewährleistung der Datensicherheit im Prozeß der Verarbeitung von Daten und Informationen mittels Rechentechnik

§ 12

Nutzung der Rechentechnik

(1) Der Betrieb der Rechentechnik hat nur im Zusammenhang mit der Erfüllung der Arbeitsaufgaben bzw. entsprechend den Dienstpflichten zu erfolgen. Die Nutzung der Rechentechnik für private Zwecke ist nicht gestattet. Die Leiter der Staatsorgane und Betriebe können die Nutzung der Rechentechnik für gesellschaftliche Aufgaben genehmigen.

(2) Die Berechtigungen zur Bedienung der Rechentechnik sowie zur Auftragserteilung und -entgegennahme sind schriftlich in betrieblichen Dokumenten, z. B. in Funktionsplänen oder Arbeitsaufträgen, nachzuweisen. Die Werktätigen müssen die entsprechende Qualifikation besitzen.

(3) Beim Betrieb der Rechentechnik sind die dokumentierten Sicherheitskomponenten der Software zur Gewährleistung der Datensicherheit anzuwenden und deren Umgehung auszuschließen.

(4) Bei Verletzungen der Datensicherheit durch Programme, die mit dem Ziel angefertigt oder in Umlauf gebracht sind, um zum Schaden des Nutzers die Funktion der Rechentechnik unkontrolliert zu verlangsamen, einzuschränken oder zu verhindern (Computerviren), sind bis zur Klärung und Behebung der Ursachen die Arbeiten einzustellen und andere Maßnahmen zur Vermeidung von weiteren Schäden einzuleiten. In Staatsorganen und Betrieben sind diese Verletzungen als außergewöhnliche Vorkommnisse meldepflichtig.

(5) Werden Daten, Informationen und Software ständig zugriffsbereit gespeichert, sind hard- und softwareseitige Mittel zur Identifikation des Nutzers bei der Ein- und Ausgabe der Daten und Informationen, bei der Durchführung von Recherchen sowie bei Veränderungen in den Speicherbelegungen anzuwenden. Die Vergabe der Identifikationsschlüssel hat durch dafür beauftragte Personen zu erfolgen und ist nachzuweisen. Fehlen die hard- und softwareseitigen Mittel, sind organisatorische Maßnahmen anzuwenden.

(6) Bei der Arbeit im Rechnerverbund ist durch technische und programmtechnische Maßnahmen zu gewährleisten, daß der Nutzer nur auf die ihm zugewiesenen Rechnerressourcen zugreifen kann.

(7) Die Nutzung der Rechentechnik durch andere Staatsorgane und Betriebe ist im Rahmen abgeschlossener Wirtschaftsverträge zulässig. Durch die Leiter der auftraggebenden Staatsorgane und Betriebe und der auftragnehmenden Staatsorgane und Betriebe ist zu gewährleisten, daß mit dem Wirtschaftsvertrag die erforderlichen Maßnahmen zur Gewährleistung der Datensicherheit vereinbart werden.

(8) Die Nutzung privater Rechentechnik und Datenträger für dienstliche Aufgaben ohne vertragliche Vereinbarung ist nicht zulässig. Für die vertragliche Vereinbarung gelten die entsprechenden Rechtsvorschriften.[3]

§ 13

Kontrolle der Nutzung der Rechentechnik

(1) Die Nutzung der Rechentechnik und die beim Einsatz zentraler Rechentechnik verwendeten Datenträger sind nachzuweisen. Für Protokolle sind vorrangig die automatisierte Führung von Maschinentagebüchern und andere rechnergestützte Nachweise der Arbeiten anzuwenden. Die Kontrolle der Maschinentagebücher und der anderen Nachweise sind aktenkundig zu sichern.

(2) Die Berechtigung zur Übernahme von Ergebnissen des Datenverarbeitungsprozesses ist auszuweisen. Die Behandlung nicht verwendungsfähiger Drucklisten ist festzulegen.

(3) Die Nutzung der zentralen Rechentechnik durch Werktätige anderer Staatsorgane und Betriebe im Rahmen abgeschlossener Wirtschaftsverträge ist zu kontrollieren. Das unbefugte Benutzen von Daten des Auftragnehmers sowie deren unberechtigte Kenntnisnahme und Kopieren sind bei der Nutzung der Rechentechnik zu verhindern.

§ 14

Instandhaltung der Rechentechnik

(1) Durch vorbeugende Maßnahmen sind die Auswirkungen von Ausfällen der Rechentechnik so gering wie möglich zu halten. Es sind Ersatzvarianten für die Nutzung der Rechentechnik vorzubereiten und deren Wirksamkeit zu überprüfen.

(2) Zur schnellen Überwindung der Ausfälle der Rechentechnik sind Maßnahmen zur Wiederherstellung ihres ursprünglichen Zustandes vorbeugend festzulegen.

(3) Die Arbeiten zur Wartung, Diagnose und Instandsetzung der Rechentechnik sind unter Bedingungen durchzuführen, die die Datensicherheit gewährleisten. Die Ausführung dieser Arbeiten sowie die Durchführung technischer Änderungen sind nur den dazu berechtigten Personen gestattet. Die Arbeiten an Rechentechnik, die in Sicherheitsstufen eingestuft wurde, ist zu beaufsichtigen, sofern keine eigenen Instandhaltungskräfte eingesetzt werden. Dabei ist

[3] Z. Z. gilt die Anordnung vom 27. Oktober 1987 zur Durchsetzung von Ordnung und Sicherheit bei der Durchführung von Softwareleistungen in nebenberuflicher Honorartätigkeit (GBl. I Nr. 28 S. 273).

zu sichern, daß nach den Instandsetzungsarbeiten, die mit dem Zertifikat bestätigten Grenzwerte für die Abschirmung eingehalten werden.

(4) Es ist ein Nachweis über die durchgeführten Wartungs-, Diagnose- und Instandsetzungsarbeiten sowie technischen Änderungen zu führen.

Gewährleistung der Datensicherheit beim Umgang mit Datenbeständen und Datenträgern

§ 15

Aufbewahrung

(1) Die Verantwortung für die Datensicherheit bei der Aufbewahrung und Verwaltung von Datenträgern einschließlich deren Archivierung ist durch den Leiter festzulegen, in dessen Verantwortungsbereich der Datenträger nachzuweisen ist. Das schließt die Kontrolle des Personenkreises ein, der die Zugriffsberechtigung zu den Daten hat. Für die Festlegung des Personenkreises, der Zugriff zu den Daten erhalten soll, ist der für die Daten inhaltlich zuständige Leiter verantwortlich.

(2) Bei der Bearbeitung von Daten in Einrichtungen der Datenverarbeitung ist der Leiter der Einrichtung für die Datensicherheit verantwortlich. Er hat die Anforderungen an die Datensicherheit gemäß den vertraglichen Vereinbarungen mit den Auftraggebern zu gewährleisten. Das gilt auch bei paralleler Bearbeitung von Datenträgern durch mehrere Nutzer.

(3) Datenträger mit wichtigen Daten und Programmen sind auf gesonderten Datenträgern zu duplizieren. Diese Datenträger sind getrennt von den ursprünglichen Datenträgern aufzubewahren. Bei Notwendigkeit sind Datenträger mit Daten und Programmen auch außerhalb der Objekte, in denen die Verarbeitung durchgeführt wird, aufzubewahren. Die Verfahrensweise zur Auslagerung, sicheren Verwahrung und Aktualisierung dieser ausgelagerten Datenträger ist durch die zuständigen Leiter der Staatsorgane und Betriebe zu regeln. Damit ist bei Störungen eine schnelle Wiederherstellung der Funktionsfähigkeit des Datenverarbeitungsprozesses zu gewährleisten. Bei der Aufbewahrung von Datenträgern sind die Festlegungen (technische Vorschriften) der Hersteller einzuhalten.

(4) Datenträger sind grundsätzlich in verschlossenen Räumen und möglichst in verschlossenen Behältnissen aufzubewahren. In Übereinstimmung mit den Anforderungen an die Gewährleistung der Datensicherheit sind Festlegungen für den Zugriff zu den Datenträgern zu treffen.

(5) Datenträger, die Staatsgeheimnisse zum Inhalt haben, sind getrennt von den übrigen Datenträgern aufzubewahren. Diese Daten sind nachweisbar physisch zu löschen, wenn sie für die weitere Arbeit nicht mehr benötigt werden.

(6) Nicht zum eigenen Bestand gehörende Datenträger sind getrennt von den eigenen Datenträgern zu lagern. Sie unterliegen während ihres Vorhandenseins den Festlegungen des Auftragnehmers. Dieser hat den Ein- und Ausgang der Datenträger nachzuweisen.

§ 16

Kennzeichnung

(1) Datenträger sind visuell so zu kennzeichnen, daß

- Verwechselungen verhindert werden sowie eine eindeutige Zuordnung zum Nachweismittel und zum Nutzer gegeben sind sowie
- keine Beschädigung oder funktionelle Beeinträchtigung der Datenträger bzw. Geräte verursacht werden.

Die Art der Kennzeichnung ist in den Weisungen der Leiter der Staatsorgane und Betriebe festzulegen.

(2) Je nach Datenträgerart ist eine eindeutige Zuordnung von Datenträgern und Zubehör (Wechselplattenkassette oder andere äußere Hülle) vorzunehmen. Ist die maschinelle Identifikation von Datenträgern realisierbar, so ist diese anzuwenden.

(3) Bei der Kennzeichnung der Datenträger, die Staatsgeheimnisse beinhalten, sind folgende Verfahrensweisen anzuwenden:

- **Magnetische Datenträger**
  Magnetische Datenträger, auf denen Staatsgeheimnisse gespeichert werden, sind Verschlußsachen (VS). Diese sind vor der ersten Einspeicherung der Daten und Informationen mit einer VS-Signatur zu kennzeichnen und initialisiert bereitzustellen. Der festgelegte Geheimhaltungsgrad sowie die festgelegte Kennzeichnung sind so lange unverändert beizubehalten, wie dieser Datenträger im Bestand geführt wird. Für den Datenträger ist der jeweils höchste Geheimhaltungsgrad vorzusehen, in den eine Datei eingestuft wurde. Staatsgeheimnisse, die auf magnetischen Datenträgern gespeichert sind, aufbewahrt, ständig aktualisiert bzw. ergänzt oder von einem magnetischen Datenträger auf einen anderen übernommen werden, sind bei Ausgabe als Druckliste, Zeichnung oder in anderer vergleichbarer Form mit einer eigenständigen VS-Signatur zu kennzeichnen.
- **Lochkarten**
  Bei Lochkarten ist der gesamte Lochkartensatz als eine VS zu behandeln. Jedem zu einer VS gehörenden Lochkartensatz ist eine Volleckenkarte mit der VS-Signatur beizufügen. Statt Blattzahl ist die zur VS gehörende Lochkartenzahl in der Kennzeichnung anzugeben.
- **Lochbänder**
  Lochbänder sind am Bandanfang und -ende zu kennzeichnen. Statt Blattzahl sind in der VS-Signatur „Anfang“ und „Ende“ einzutragen.

Die Druckliste muß eine andere VS-Signatur als der Datenträger erhalten.

(4) Bei paralleler bzw. gemeinsamer Nutzung magnetischer Festplatten sind technische, organisatorische und programmtechnische Maßnahmen zur Gewährleistung der Datensicherheit anzuwenden. Die Behältnisse und Einschübe für die Festplatten mit gespeicherten Staatsgeheimnissen und anderen geheimzuhaltenden Informationen sind durch personelle und technisch-organisatorische Maßnahmen (wie z. B. petschieren oder plombieren) zu sichern.

§ 17

Nachweisführung

(1) Für alle Datenträger ist ein Datenträgernachweis zu führen. Für die Übergabe/Übernahme der Datenträger ist die lückenlose Nachweisführung zu sichern.

(2) Die Nachweisführung über die Datenträger hat durch namentlich für die Verwaltung von Datenträgern festgelegte Mitarbeiter im Verantwortungsbereich zu erfolgen. Die Nachweisunterlagen für die Datenträger sind zeitlich gemäß den Festlegungen der betrieblichen Archivierungsordnung aufzubewahren.

(3) Für den regelmäßigen Nachweis der auf dem Datenträger befindlichen Software und Dateien ist der mit der Arbeit mit diesen Datenträgern beauftragte Mitarbeiter verantwortlich. Der Nachweis ist anhand von schriftlichen Datenträgerinhaltsverzeichnissen oder Programmlaufprotokollen zu erbringen. Jährlich ist eine Inventur der Datenträger durchzuführen. Im Ergebnis der Inventur sind Maßnahmen für die effektive Nutzung der Datenträger festzulegen.

(4) Es sind Festlegungen zur Zugriffsberechtigung und zur Protokollierung erfolgter Zugriffe auf die Datenträger zu treffen.

(5) Nachweisunterlagen für magnetische Datenträger mit Staatsgeheimnissen und anderen geheimzuhaltenden Informationen haben statt inhaltlicher Angaben die genaue Bezeichnung des Datenträgers zu seiner eindeutigen Identifizierung (Datenträgernummer, Datenträgerart, Fabrikationsnummer usw.) zu enthalten.

§ 18

Transport

(1) Der Transport von Datenträgern, einschließlich des grenzüberschreitenden Transports, hat auf der Grundlage der Rechtsvorschriften zu erfolgen.

(2) Für den Transport von Datenträgern innerhalb des Betriebsgeländes sind Festlegungen auf der Grundlage der örtlichen Gegebenheiten sowie unter Beachtung der Sicherheitsanforderungen an die Datenträger vorzubereiten und durchzusetzen. Dabei sind generell Maßnahmen vorzusehen, die die Datenträger vor unberechtigtem Zugriff schützen.

(3) Vor dem Transport von Datenträgern ist anhand von Datenträgerinhaltsverzeichnissen bzw. -analysen zu sichern, daß sich auf den auszuliefernden Datenträgern nur die zur Auslieferung festgelegten Daten und Informationen befinden. Der Datenaustausch ist auf der Grundlage gesetzlicher Festlegungen oder vertraglicher Vereinbarungen zwischen Staatsorganen und Betrieben durchzuführen.

§ 19

Wartung und Vernichtung

(1) Alle Maßnahmen zur Pflege und Wartung sowie Aussonderung bzw. Vernichtung von Datenträgern sind nachzuweisen.

(2) Die Reinigung bzw. Prüfung der Datenträger hat grundsätzlich nur mit für diese Zwecke geeigneten Mitteln zu erfolgen. Dabei entstehende Unterlagen mit Qualitätsaussagen über den Datenträger sind zum Bestandteil der Nachweisführung zu machen. Für die Reinigung von Datenträgern mit Staatsgeheimnissen und anderen geheimzuhaltenden Informationen sind eine entsprechende Auftragserteilung und Nachweisführung zu gewährleisten.

(3) Die Vernichtung von Datenträgern ist nur nach erfolgter Freigabe durch den Nutzer oder auf Weisung des zuständigen Leiters durchzuführen. Datenträger sind nachweisbar zu vernichten bzw. zu verformen. Die Vernichtung von Datenträgern, die Staatsgeheimnisse und andere geheimzuhaltende Informationen enthalten, hat gemäß den Rechtsvorschriften zu erfolgen.

Gewährleistung der Datensicherheit bei der Datenübertragung

§ 20

Grundsatz

Bei der Übertragung von Daten ist durch das Zusammenwirken von fernmelde-, geräte- und programmtechnischen Mitteln sowie durch organisatorische Maßnahmen weitestgehend zu gewährleisten, daß die übermittelten Daten nur der vorgesehene Empfänger unverändert erhält.

§ 21

Datenübertragung in lokalen Rechnernetzen

(1) Bei der Datenübertragung in lokalen Rechnernetzen sind Maßnahmen durchzuführen, die Abweichungen von den Anforderungen an die Gewährleistung der Datensicherheit ausschließen.

(2) Durch organisatorische, technische und programmtechnische Maßnahmen ist zu sichern, daß bei der Datenübertragung in lokalen Rechnernetzen der Austausch von Staatsgeheimnissen mit den Geheimhaltungsgraden VVS und GVS sowie Dienstsachen ausschließlich zwischen berechtigten Personen durchgeführt werden kann und nur berechtigte Personen auf Daten und Informationen zugreifen können. Bei der Datenübertragung von Staatsgeheimnissen mit den Geheimhaltungsgraden VVS und GVS sind geeignete Schutzverfahren anzuwenden. Das Ministerium für Staatssicherheit ist über die entsprechende Verfahrensweise zu informieren.

(3) Die für die Datenübertragung von Staatsgeheimnissen mit den Geheimhaltungsgraden VVS und GVS in lokalen Rechnernetzen vorgesehene Rechentechnik sowie die betriebseigenen Informationskabel sind so zu installieren, daß unerwünschte Ausstrahlungen außerhalb der ständig bewachten oder beobachteten Objekte oder Geländeabschnitte, in denen der unkontrollierte Aufenthalt von Personen und Verkehrsmitteln ausgeschlossen ist (kontrollierte Zone), nicht auswertbar sind.

§ 22

Datenübertragung über Leitungen zur Datenfernübertragung bzw. -verarbeitung

(1) Die Datenübertragung hat in Übereinstimmung mit den geltenden Rechtsvorschriften gemäß § 1 Abs. 3 zu erfolgen.

(2) Bei der Datenfernübertragung bzw. -verarbeitung ist der unberechtigte Zugriff zu den Staatsgeheimnissen mit den Geheimhaltungsgraden VVS und GVS sowie Dienstsachen und deren Zerstörung auszuschließen.

(3) Staatsgeheimnisse mit den Geheimhaltungsgraden VVS und GVS sind bei der Anwendung der elektronischen Datenübertragung durch technische Mittel zu chiffrieren. Bei der Anwendung der elektronischen Datenübertragung für andere geheimzuhaltende Informationen sind bestehende Möglichkeiten der Chiffrierung zu nutzen bzw. andere ausreichende Möglichkeiten des Schutzes in Abstimmung mit dem Ministerium für Staatssicherheit zu verwenden.

(4) Die Standorte der Rechentechnik, die für die Datenübertragung von Staatsgeheimnissen vorgesehen sind, müssen den gültigen Regelungen zur chiffrierten Datenübertragung entsprechen. Die Rechentechnik ist so zu installieren, daß unerwünschte Ausstrahlungen außerhalb der kontrollierten Zone nicht auswertbar sind.

§ 23

Grenzüberschreitende Datenübertragung

(1) Für den internationalen Datenübertragungsdienst gelten die völkerrechtlichen Verträge, die für die DDR in Kraft sind, wenn sie auf der Grundlage dieser Verträge ihre Teilnahme am internationalen Datenübertragungsdienst erklärt hat.

(2) Die Teilnahme am internationalen automatisierten Informationsaustausch der Mitgliedsländer des RGW erfolgt auf der Grundlage der dazu erlassenen Rechtsvorschrift.[4]

(3) Bei vorgesehener grenzüberschreitender Datenübertragung von Staatsgeheimnissen mit den Geheimhaltungsgraden VVS und GVS sowie der anderen geheimzuhaltenden Informationen ist die Genehmigung durch den für den Bereich zuständigen Minister bzw. Leiter anderer zentraler Staatsorgane einzuholen. Die Übermittlung von Staatsgeheimnissen im grenzüberschreitenden Verkehr darf nur über die dazu berechtigte Chiffrierstelle erfolgen.

§ 24

Schlußbestimmungen

(1) Diese Anordnung tritt mit ihrer Veröffentlichung in Kraft.

(2) Bestehende Regelungen der Minister und Leiter anderer zentraler Staatsorgane zur Gewährleistung von Sicherheit, Ordnung und Geheimnisschutz in der Datenverarbeitung und -übertragung sind mit dieser Anordnung in Übereinstimmung zu bringen bzw. aufzuheben.

(3) Gleichzeitig treten die vom Ministerium für Wissenschaft und Technik gesondert zugestellten Regelungen über die Gewährleistung von Sicherheit, Ordnung und Geheimnisschutz in der Datenverarbeitung und -übertragung außer Kraft.

Berlin, den 23. Februar 1989

Der Minister
für Wissenschaft und Technik
I. V: Herrmann
Staatssekretär

[4] Z. Z. gilt die Anordnung vom 18. März 1988 üb... eilnahme am internationalen automatisierten Informationsau... der Mit-