Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG

Dr. Wilfried Grieger

wgriege@gwdg.de

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)
Am Faßberg
37077 Göttingen

Version 4.1 vom 9. Februar 1996

Vorworte

Vorwort zur Version 1.0

In der vorliegenden Dokumentation wird versucht, alle Möglichkeiten zu beschreiben, die jeder Benutzer, der personenbezogene Daten verarbeitet, in Anspruch nehmen kann, um diese personenbezogenen Daten im Sinne der Datenschutzgesetze zu sichern. Dabei wird angestrebt, jeweils den neuesten Stand der bei der GWDG eingesetzten Technik und Software darzustellen.

Göttingen, den 11. Mai 1988

W. Grieger

Vorwort zur Version 2.0

Zusätzlich zu den Maßnahmen zum Datenschutz werden noch einige Begriffe aus dem Bundesdatenschutzgesetz erläutert. Dabei wurden die im „Anhang. Literatur“ aufgeführten Dokumentationen verwendet.

Vorausgesetzt werden Grundkenntnisse der Betriebssysteme, unter denen personenbezogene Daten verarbeitet werden sollen.

Göttingen, den 9. April 1990

W. Grieger

Vorwort zur Version 3.0

Am 20. Dezember 1990 wurde ein neues Bundesdatenschutzgesetz im Bundesgesetzblatt verkündet, das am 1. Juni 1991 in Kraft trat. Die Novellierung sollte folgende sechs Ziele erreichen:

1. Verbesserung der Verständlichkeit
2. Verstärkung der Zweckbindung der Daten aus dem Volkszählungsurteil heraus
3. Stärkung der Rechte der Betroffenen
4. Einführung von Zulässigkeitsbedingungen automatischer Abrufverfahren
5. Stärkung der Kompetenz der Kontrollinstanzen
6. Einführung von Sonderregelungen für Medien und Forschung

Ob alle Ziele zur allgemeinen Zufriedenheit erreicht wurden, mag dahingestellt sein, auf jeden Fall wurden einige Vorschriften geändert, so daß eine Neufassung des rechtlichen Teils des Kursskripts erforderlich wurde.

Gleichzeitig vollzieht sich zur Zeit in der elektronischen Datenverarbeitung ein grundsätzlicher Strukturwandel. Die Wissenschaftler fordern eine Dezentralisierung der Rechnerleistung. Die Grundleistung soll von sogenannten Arbeitsplatzrechnern in den Instituten erbracht werden. Nur Spitzen- oder Spezialleistung, für die es unwirtschaftlich wäre, sie in jedem Institut bereitzuhalten, soll von einer zentralen Stelle über Netze abrufbar sein. Diese zentrale Leistung wird zukünftig bei der GWDG über ein UNIX-Cluster erreichbar sein, das zum größten Teil aus Workstations, aber auch aus Spezialrechnern bestehen wird. Aus diesem Grund ist

es angebracht, auch Datenschutzmaßnahmen unter dem Betriebssystem UNIX aufzuführen. Sie können in dieser Version noch nicht vollständig sein.

Die Erläuterung der Datenschutzmaßnahmen auf den Großrechnern IBM 3090 und jetzt VAX 9000 und auf dem PC-Netz ist auf den aktuellen Stand gebracht.

Göttingen, den 22. Januar 1993

W. Grieger

Vorwort zur Version 4.0

Der Strukturwandel in der elektronischen Datenverarbeitung ist nun auch bei der GWDG vollzogen worden. Die Großrechner existieren nicht mehr, offene Systeme in Form von UNIX-Rechnern, die über Datenübertragungsnetze miteinander verbunden sind, haben sich durchgesetzt.

Diese Änderungen haben natürlich auch datenschutzrechtliche Konsequenzen. Sie sollen im vorliegenden Kursskript erläutert werden. Zur gleichen Problematik hat der Landesbeauftragte für den Datenschutz Niedersachsen einige Empfehlungen veröffentlicht, die ebenfalls ins Kursskript aufgenommen wurden.

Göttingen, den 3. Februar 1995

W. Grieger

Vorwort zur Version 4.1

Auf der Datenautobahn sind nun auch Informationen über den Datenschutz abrufbar. Eine wichtige Quelle sind die „Datenschutz-Informationen“ der Humboldt-Universität in Berlin, die unter dem URL

```
http://www.rewi.hu-berlin.de/Datenschutz
```

erreichbar sind.

W. Grieger

Inhalt

KAPITEL 1

Datenschutzgesetze

Im vorliegenden Kapitel werden einige Grundbegriffe aus dem Datenschutzrecht erläutert.

Welches Datenschutzgesetz ist anzuwenden?

Die Verarbeitung personenbezogener Daten wird in einer Vielzahl von Gesetzen geregelt. Dazu gehören das Strafgesetzbuch, das Meldegesetz und die Sozialgesetzbücher. Wenn kein anderes Gesetz die Verarbeitung personenbezogener Daten regelt, muß das „Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes“ und dort Artikel 1, nämlich das „Bundesdatenschutzgesetz“, abgekürzt BDSG, zugrunde gelegt werden. Es ist damit zu einem Auffanggesetz geworden.

In BDSG §§ 1 und 2 ist aufgeführt, wer diesem Gesetz unterliegt. Es handelt sich im wesentlichen um die Behörden des Bundes und um natürliche und juristische Personen.

Als Ergänzung zum BDSG haben die meisten Parlamente der Bundesländer Landesdatenschutzgesetze erlassen. Die dortigen Vorschriften gelten jeweils nur für die Behörden des betreffenden Landes.

Jeder, der personenbezogene Daten auf den Rechenanlagen der GWDG verarbeiten möchte, muß sich demnach nach den Vorschriften des BDSG richten, es sei denn, ein anderes Gesetz regelt die Verarbeitung.

Im folgenden sind deshalb einige Vorschriften des BDSG erläutert.

Was sind personenbezogene Daten?

In BDSG § 3 wird definiert, was unter dem Begriff „personenbezogene Daten“ zu verstehen ist: *Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).* Eine Person ist bestimmt, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder wenn sich der Bezug aus dem Inhalt oder dem Zusammenhang unmittelbar herstellen läßt. Eine Person ist bestimmbar, wenn sich der Bezug ohne unverhältnismäßigen Aufwand herstellen läßt. Statistische oder anonymisierte Daten sind in der Regel nicht mehr personenbezogen.

Dürfen personenbezogene Daten verarbeitet werden?

In BDSG § 4 wird die Verarbeitung personenbezogener Daten zunächst einmal grundsätzlich verboten. Sie ist *nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.*

Am einfachsten ist also der Fall zu behandeln, daß eine Einwilligung vorliegt. Sie muß aber schriftlich erfolgt sein.

Die „Datenverarbeitung“ im Sinne des BDSG wird in § 3 in fünf Phasen eingeteilt, und zwar werden sie mit „Speichern“, „Verändern“, „Übermitteln“, „Sperren“ und „Löschen“ bezeichnet. *Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:*

1. *Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,*

2. *Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,*
3. *Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß*
   a. *die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder*
   b. *der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,*
4. *Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,*
5. *Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.*

Hinzu kommt demzufolge das „Nutzen“ von Daten: *Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.*

Erstmalig ist im neuen Bundesdatenschutzgesetz auch das „Erheben“ von Daten geregelt: *Erheben ist das Beschaffen von Daten über den Betroffenen.*

Nach BDSG § 1 ist der Zweck des Gesetzes, *den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch ... nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.*

Der Begriff „Datei“ im Sinne des BDSG unterscheidet sich nun jedoch von dem in der Datenverarbeitung üblichen. Nach § 3 ist eine Datei

1. *eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder*
2. *jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).*

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

Hinweis: Die Sammlung von personenbezogenen Daten in Akten wird zum größten Teil im zweiten Abschnitt „Datenverarbeitung der öffentlichen Stellen“ des Bundesdatenschutzgesetzes geregelt.

Das BDSG ist in fünf Abschnitte eingeteilt.

Im ersten Abschnitt werden allgemeine Bestimmungen erläutert. Dazu gehören Begriffsbestimmungen, die allgemeine Zulässigkeit der Datenverarbeitung und die unabdingbaren Rechte des Betroffenen.

Der zweite Abschnitt behandelt die Datenverarbeitung der öffentlichen Stellen, der dritte Abschnitt die der nicht-öffentlichen Stellen, zu denen auch die natürlichen und juristischen Personen gehoren.

Im vierten Abschnitt sind Sondervorschriften, unter anderem für die Forschung und für die Medien, aufgeführt.

Der fünfte Abschnitt enthält Strafvorschriften.

Für die Bearbeitung von personenbezogenen Daten von Benutzern der Rechenanlagen der GWDG sind demnach der dritte Abschnitt des BDSG und die Sondervorschriften für die Forschung besonders zu beachten.

Wenn keine andere Rechtsvorschrift zugrundegelegt werden muß und eine Einwilligung des Betroffenen nicht vorliegt, wird die Zulässigkeit der Verarbeitung personenbezogener Daten in BDSG §§ 28, 29 und 30 geregelt. Andere Paragraphen des dritten Abschnitts enthalten Vorschriften, die einzuhalten sind, wenn die Verarbeitung personenbezogener Daten erlaubt ist. Zu diesen Vorschriften gehört, daß einem Betroffenen mitgeteilt werden muß, daß über ihn Daten gespeichert werden.

Welches sind die Sondervorschriften für die Forschung?

In BDSG § 40 sind Sondervorschriften für die Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen aufgeführt.

Dazu gehört, daß für *Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten ... nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden* dürfen.

Weiter sind die *personenbezogenen Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist.*

Diejenigen Wissenschaftler, die personenbezogene Daten veröffentlichen wollen, haben nach BDSG § 40 Abs. 4 folgendes zu beachten:

Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. *der Betroffene eingewilligt hat oder*
2. *dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.*

Welche Datenschutzmaßnahmen sind erforderlich?

Um personenbezogene Daten verarbeiten zu dürfen, müssen auch einige technische und organisatorische Maßnahmen erfüllt werden. Diese sind in BDSG § 9 und in einer Anlage dazu aufgeführt. *Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.*

Die Anlage zu BDSG § 9 hat folgenden Wortlaut:

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. *Unbefugten den Zugang zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (**Zugangskontrolle**),*
2. *zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Datenträgerkontrolle**),*
3. *die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (**Speicherkontrolle**),*

4. *zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (**Benutzerkontrolle**),*
5. *zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (**Zugriffskontrolle**),*
6. *zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (**Übermittlungskontrolle**),*
7. *zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**),*
8. *zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),*
9. *zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**),*
10. *die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (**Organisationskontrolle**).*

Der Punkt 1 wird dabei von der GWDG gewährleistet. Jeder Benutzer, der personenbezogene Daten auf den Rechenanlagen der GWDG verarbeitet, ist verpflichtet zu überprüfen, ob und wieweit die anderen Punkte von ihm selber erfüllt werden müssen. In den folgenden Kapiteln ist aufgeführt, welche Datenschutzmaßnahmen die GWDG anbietet, damit die Ausführung der Vorschriften des BDSG gewährleistet werden kann.

KAPITEL 2

Amtliche Hinweise und Empfehlungen

Im vorliegenden Kapitel werden einige Hinweise und Empfehlungen des Landesbeauftragten für den Datenschutz Niedersachsen mit seiner freundlichen Genehmigung abgedruckt.

Klassifizierung schutzwürdiger Belange

Personenbezogene Daten werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Mißbrauch dieser Daten in 5 Schutzstufen untergliedert. Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auch auf die unmittelbar verknüpfbaren Datenbestände auszudehnen. Werden personenbezogene Daten unter einem Auswahlkriterium in eine Datei aufgenommen, das in der Datei nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten. Enthalten Dateien umfassende Angaben zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre.

Es werden folgende Schutzstufen unterschieden:

A: Frei zugängliche Daten, in die Einsicht gewährt wird, ohne daß der Einsichtnehmende ein berechtigtes Interesse geltend machen muß, z. B. Adreßbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.

B: Personenbezogene Daten, deren Mißbrauch zwar keine besondere Beeinträchtigung erwarten läßt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z. B. beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen.

C: Personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann („Ansehen"), z. B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.

D: Personenbezogene Daten, deren Mißbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann („Existenz"), z. B. gesundheitliche Verhältnisse, Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, wirtschaftlliche Verhältnisse.

E: Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z. B. besonders empfindliche Patientendaten, Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

Falls die Sensitivität nicht bekannt ist, ist von der höchsten Sensitivitätsstufe auszugehen. Denkbar ist auch, daß der Schutz empfindlicher Firmendaten ohne Personenbezug die Einstufung bestimmt. Die Sensitivitätskriterien kommen sinngemäß auch zur Anwendung, wenn es sich um Datensicherungsmaßnahmen zu vollständigen Dateiverzeichnissen, Rechnern oder Netzwerken handelt. So muß sich der Systempaßwortschutz oder die Systemprotokollierung nach den sensitivsten Daten richten, die in dem System verarbeitet werden, das mit dem Paßwort zugänglich ist.

Daten der Sensitivitätsstufe E erfordern eine sehr restriktive UNIX-Handhabung; Vernetzungen sind nur in deutlich eingeschränktem Maße akzeptabel. Von einer Verarbeitung dieser Daten unter UNIX ist daher abzusehen.

Hinweise zur Paßwort-Gestaltung und Paßwort-Verwendung

Erforderlichkeit

Jede Datenverarbeiterin und jeder Datenverarbeiter sollte ein besonderes Interesse haben, die „eigenen Daten“ vor den neugierigen Augen unberechtigter Dritter zu schützen. § 9 des Bundesdatenschutzgesetzes (BDSG) und § 7 des neuen Niedersächsischen Datenschutzgesetzes (NDSG) verpflichten öffentliche Stellen sowie Unternehmen des nicht-öffentlichen Bereichs, die personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen gegen die unberechtigte Verarbeitung oder Nutzung von personenbezogenen Daten zu treffen.

Das Paßwortverfahren ist gegenwärtig das am meisten verwendete Verfahren, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern. Jeder Benutzer sollte über eine Benutzerkennung und über ein persönliches Paßwort verfügen, um sich so gegenüber dem IuK-System als Berechtigter ausweisen zu können. Dem nachgewiesen authentischen Benutzer wird der Zugang zum System, zur Anwendung oder zu Teilen der Anwendung entsprechend den vergebenen Rechten eröffnet.

Mit den folgenden Hinweisen sollen Empfehlungen zur Paßwort-Gestaltung und Tips zur Kontrolle einer datenschutzgerechten Verwendung von Paßworten gegeben werden.

1. Empfehlungen für Benutzer

- Paßwort nirgends notieren und niemandem mitteilen!
  (Ausnahme: z. B. versiegelte Hinterlegung des Systemverwalter-Paßwortes für Notfälle. Die Benutzung des versiegelten Umschlags ist zu dokumentieren.)
- Mindestens 6 Zeichen aus Buchstaben, Ziffern und Zeichen gemischt!
- Mindestens 1 Sonderzeichen verwenden!
- Paßwort regelmäßig ändern, aber nicht zu oft!
- Keine Trivialpaßwörter verwenden!

Um sich auch ein kompliziertes Paßwort leicht merken zu können, sollte man aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und Sonderzeichen einstreuen, so z. B.:

„**Ei**le **mi**t **We**ile“ = EimiWe?

2. Hinweise für Systemverwalter und interne Datenschutzbeauftragte

Die Paßwortregeln sind nach der Sensibilität der zu verarbeitenden personenbezogenen Daten abgestuft. Die Datenschutzbeauftragten des Bundes und der Länder untergliedern personenbezogene Daten nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange in fünf Schutzstufen. Bei der Einordnung in eine der Schutzstufen sind nicht einzelne Datenfelder zu bewerten, vielmehr ist die gesamte Datei, die mögliche Verknüpfbarkeit oder auch das Auswahlkriterium der Speicherung, das nicht selbst gespeichert sein muß, zu berücksichtigen. Die folgenden Maßnahmen sind als Mindestempfehlungen zu verstehen. Die Regeln der niedrigeren Stufe gelten selbstverständlich auch für höhere Stufen.

Ab Stufe A (frei zugängliche Daten):

Vor dem Zugriff auf Daten oder Programme des Systems wird die Anmeldung mittels Benutzerkennung (Login-ID) und Paßwort erzwungen (**Paßwortschutz**).

Jeder Benutzer hat bei der Anmeldung ein nur ihm bekanntes Paßwort einzugeben (**persönliches Paßwort**).

Bei der Erstanmeldung muß das Paßwort durch den Benutzer geändert werden (**Paßwortübergabe an Benutzer**). Dies sollte organisatorisch geregelt werden.

Die Paßworteingabe darf nicht auf dem Bildschirm wiedergegeben werden (**Dunkelsteuerung**).

Trivialpaßwörter (z. B. Vornamen, Geburtsdaten, Dienstnummern) dürfen nicht verwendet werden (**keine Trivialpaßwörter**).

Die Paßwörter müssen spätestens nach sechs Monaten geändert werden (**Paßwortalterung**).

Ab Stufe B (geringes Mißbrauchsrisiko):

Paßworte werden verschlüsselt gespeichert (**Verschlüsselung**). Der Verschlüsselungsalgorithmus sollte auch dem Systemverwalter nicht bekannt sein.

Die **Paßwort-Mindestlänge** beträgt sechs Zeichen, besser acht Zeichen.

Für das Paßwort sollten verwendbar sein: Große und kleine Buchstaben, Zahlen, Sonderzeichen (**alphanumerische Zeichen**).

Eine Zeichenmischung ist vorgeschrieben (**Zeichenmischung**).

Die Paßwort-Regeln und Hinweise für Benutzer sind in einer schriftlichen, allen Benutzern bekannten **Dienstanweisung** festgelegt.

Ab Stufe C (Gefährdung des Ansehens):

Das System ist so einzurichten, daß eine Umgehung des Paßwortschutzes auch mit zusätzlichen Mitteln praktisch nicht möglich ist (**Systemabsicherung**). Es ist insbesondere abzusichern, daß kein Systemstart mit Systemdiskette möglich ist.

Die Anzahl der Fehlversuche hintereinander wird begrenzt (max. fünf), danach wird die Benutzerkennung oder das Terminal gesperrt (**Begrenzung der Fehlversuche**).

Nach spätestens sechs Monaten wird ein Paßwortwechsel technisch erzwungen (**Paßwortalterung**). Nach neun Monaten erfolgt eine Benutzersperre.

Bei der Erstanmeldung eines Benutzers muß die Paßwortänderung technisch erzwungen werden (**Paßwortübergabe an Benutzer**).

Ab Stufe D (Gefährdung der Existenz):

Über mindestens fünf Generationen wird automatisch verhindert, daß das alte Paßwort als neues Paßwort verwendet werden kann. Es muß an mindestens drei Stellen unterschiedlich sein (**keine Paßwortwiederholung**).

Bei wiederholter Fehleingabe erfolgt eine **Reaktionsverzögerung** des Rechners.

Trivialpaßwörter (z. B. Vornamen, Geburtsdaten, Dienstnummern) werden technisch ausgeschlossen (**keine Trivialpaßwörter**).

Eine Mischung von Zeichen wird technisch erzwungen (**erzwungene Zeichenmischung**).

Ab Stufe E (Gefährdung für Leben und Freiheit):

Das Systemverwalter-Paßwort besteht aus zwei Teilen, die jeweils unterschiedlichen Personen bekannt sind (**Vier-Augen-Prinzip**).

Hinweis an die GWDG

Auf den Rechenanlagen der GWDG dürfen keine personenbezogenen Daten der Schutzstufen D und E verarbeitet werden.

KAPITEL 3

Datenschutzmaßnahmen auf den Rechenanlagen der GWDG

Bei der Abgabe seines Antrages auf Zuweisung einer Benutzerkennung hat sich der Benutzer verpflichtet, die Vorschriften der Datenschutzgesetze einzuhalten und die angebotenen Datenschutzmaßnahmen einzusetzen. Soweit er Rechenarbeiten unter seiner Benutzerkennung durch andere Personen zuläßt, ist er für die Einhaltung der eingegangenen Verpflichtungen auch durch diese Personen verantwortlich.

Wird eine Benutzerkennung nicht mehr benötigt und sie daraufhin von der Benutzerverwaltung der Rechenanlagen entfernt, so werden auch sämtliche unter dieser Benutzerkennung gespeicherten Daten auf allen Rechenanlagen der GWDG unwiederbringlich gelöscht.

Datenschutzmaßnahmen auf dem UNIX-Cluster

login-Paßwort

Damit ein Benutzer sich auf einem Rechner des UNIX-Clusters anmelden kann, benötigt er zusammen mit seinem Username ein login-Paßwort. Dieses wird ihm vor der erstmaligen Anmeldung von der GWDG zugeteilt. Nach der mit diesem Paßwort erfolgten Anmeldung sollte es als erstes geändert werden. Dazu wird das Kommando

```
passwd
```

verwendet. Nach dem Absetzen fordert das System zur Eingabe des alten Paßworts auf. Nachdem es eingetippt ist, wird das neue Paßwort zweimal abgefragt, damit Tippfehler ausgeschlossen werden.

Zur Wahl des neuen Paßworts sollten die Hinweise des Landesbeauftragten für den Datenschutz Niedersachsen in Kapitel 2 beachtet werden. Die GWDG empfiehlt jedoch folgende Änderungen:

- Wenn Buchstaben im Paßwort verwendet werden, so sollte es sich nur um Kleinbuchstaben handeln, da manche Netze verschlüsselte oder unverschlüsselte Großbuchstaben fehlerhaft übertragen.
- Auf Sonderzeichen sollte verzichtet werden, da unterschiedliche Netze in der Regel Sonderzeichen unterschiedlich kodieren, so daß es beim Empfang nicht mehr als das ursprüngliche erkannt wird.
- Das Paßwort kann höchstens **acht Zeichen** lang sein.
- Da auf UNIX-Rechner häufig über X-Anwendungen zugegriffen wird und dabei Paßwörter unverschlüsselt und damit im Prinzip für alle am gleichen Netz arbeitenden Benutzer lesbar übertragen werden könnten, empfiehlt sich ein Wechsel des Paßworts einmal im Monat.

Durch den verantwortungsvollen Umgang mit dem login-Paßwort können die Punkte 4, 5 und 8 der Anlage zu BDSG § 9 erfüllt werden.

Dateienschutz

Dateien, die personenbezogene Daten enthalten, sollten immer nach folgendem Schema geschützt sein:

```
-rw-------
```

Dies gilt auch für die Directories, in die diese Dateien eingetragen sind:

```
drwx------
```

Dadurch hat nur der Eigentümer das Recht, die so geschützten Dateien zu bearbeiten. Ein Unbefugter kann nicht den Inhalt einer Directory lesen, so daß auch nicht anhand der Dateinamen auf deren Inhalt geschlossen werden kann.

Dieses Schutzschema läßt sich standardmäßig einstellen, wenn in die Datei **`$HOME/.profile`** folgende Zeile aufgenommen wird:

```
umask 077
```

Ab dem nächsten login werden alle neu angelegten Dateien mit dem angegebenen Schutz versehen.

Bereits existierende Dateien können folgendermaßen nach diesem Schema geschützt werden:

```
chmod go-rwx file
```

Soll einem anderen Benutzer eine Datei mit personenbezogenen Daten zugänglich gemacht werden, so sollte der obige Schutz nicht geändert werden, da er dann für eine ganze group (g) oder sogar für die others (o) aufgehoben werden müßte. Als Lösung kann dagegen die Datei *`file`* dem Benutzer *`userid`* über das Mail-System zugeschickt werden.

Damit lassen sich für Dateien die Punkte 3 und 5 der Anlage zu BDSG § 9 erfüllen.

E-Mail

Elektronische Briefe, E-Mails, enthalten unter Umständen auch personenbezogene Daten. Sollen sie über Datenübertragungsnetze verschickt werden, so muß immer davon ausgegangen werden, daß sie von Unbefugten gelesen werden können, der Datenschutz also in keiner Weise gewährleistet ist.

E-Mails, die an Userids auf dem UNIX-Cluster der GWDG gerichtet sind, enthalten dagegen nur Lese- und Schreibrechte für den Empfänger der Mail, so daß das Mail-System hier auch zum Übertragen personenbezogener Daten geeignet ist.

Soll die Datei *`file`* dem Benutzer *`userid`* mit Hilfe des Mail-Programms `elm` zugeschickt werden, so muß folgendes eingegeben werden:

```
elm userid < file
```

Der Benutzer *`userid`* kann danach unter seiner Userid durch Aufruf des Programms

```
elm
```

die Datei *file* empfangen und in eine seiner Directories kopieren.

Archivbenutzung

Das Archiv wird von einem Archiv-Server der GWDG verwaltet. Für jeden Benutzer enthält das Archiv einen eigenen Bereich, dessen Pfadname sich in der Variablen $AHOME befindet und dessen Zugriffsrechte wie im Abschnitt „Dateienschutz“ verändert werden können.

Standardmäßig besitzt nur der Eigentümer der Dateien Lese- und Schreibrechte.

Damit lassen sich für Dateien im Archiv ebenfalls die Punkte 3 und 5 der Anlage zu BDSG § 9 erfüllen.

Temporäre Dateien

Jedem Benutzer ist für temporäre Dateien ein eigener Bereich zugeordnet, dessen Pfadname sich in der Variablen $THOME befindet und dessen Zugriffsrechte wie im Abschnitt „Dateienschutz“ verändert werden können.

Standardmäßig besitzt nur der Eigentümer der Dateien Lese- und Schreibrechte. Es sollte beachtet werden, daß Dateien in der Directory $THOME nach wenigen Tagen wieder vom System automatisch gelöscht werden.

Auch für temporäre Dateien lassen sich die Punkte 3 und 5 der Anlage zu BDSG § 9 erfüllen.

Verschlüsselung von Dateien

Wenn das unbefugte Lesen einzelner Dateien verhindert werden soll, können diese auch verschlüsselt werden. Die GWDG stellt dafür das Programm `des` bereit, das nach dem Data Encryption Standard arbeitet. Der Aufruf lautet:

```
des -E eingabefile verschlüsseltes_file
```

Dabei ist *eingabefile* der Filename der Datei, die verschlüsselt werden soll, und *verschlüsseltes_file* der Filename der verschlüsselten Datei. Danach wird ein Schlüssel angefordert, der aus beliebigen alphanumerischen Zeichen bestehen und höchstens 1.024 Byte lang sein kann. Die Datei *eingabefile* kann danach gelöscht werden.

Die Entschlüsselung der Datei *verschlüsseltes_file* geschieht durch die Eingabe von:

```
des -D verschlüsseltes_file entschlüsseltes_file
```

Für *entschlüsseltes_file* ist der Filename der Datei einzusetzen, die die entschlüsselte Datei enthalten soll. Angefordert wird nun wieder ein Schlüssel; eingegeben werden muß nun **derselbe Schlüssel**, der auch schon für die Verschlüsselung verwendet wurde.

Genaueres zum Programm `des` erfährt man aus der zugehörigen Man-Page, die durch

```
man des
```

aufzurufen ist.

Magnetbandverarbeitung

Eine Magnetbandverarbeitung ist auf den Rechnern des UNIX-Clusters noch nicht möglich.

Verarbeitung personenbezogener Daten im PC-Netz

Da die im Benutzerraum und im Kursraum der GWDG aufgestellten PCs in erster Linie als Terminals und für den Datentransfer vom und zum UNIX-Cluster vorgesehen sind, können auf ihnen auch keine personenbezogenen Daten verarbeitet werden, da sämtliche Schutzmechanismen fehlen.

Sollen personenbezogene Daten von einer Diskette auf den Fileserver des UNIX-Clusters kopiert werden, so muß auf jeden Fall ausgeschlossen werden, daß eine Zwischenspeicherung auf der Festplatte des PCs erfolgt. Dieses ist auch die Standardeinstellung.

Sollen personenbezogene Daten vom Fileserver des UNIX-Clusters auf eine Diskette kopiert werden, so muß ebenfalls die Festplatte umgangen werden. Vor der Übertragung muß eine beschreibbare Diskette in das Laufwerk geschoben werden.

Beim Kommando für den Kopiervorgang muß dieses Laufwerk explizit angegeben werden.

Dadurch, daß die Dateien nicht auf der Festplatte zwischengespeichert werden, sind sie von Fremden später auch nicht mehr lesbar; die Punkte 3 und 5 der Anlage zu BDSG § 9 sind somit erfüllbar.

Allgemeines

Gedruckte Listen

Die auf den Druckern der GWDG ausgegebenen Listen werden, wenn sie nicht unmittelbar nach dem Druck vom Gerät abgeholt werden, in die Listenausgabefächer gelegt. Dort sind sie jedoch frei zugänglich, so daß personenbezogene Daten in der Regel nicht aufgedruckt sein dürfen.

Listen, die auch personenbezogene Daten enthalten, müssen also direkt vom Drukker abgeholt werden.

Gedruckte Listen können mit einem Aktenvernichter, der sich im Benutzerraum befindet und den Anforderungen des Datenschutzes genügt, vernichtet werden.

ANHANG

Literatur

Die folgende Literatur wurde bei der Zusammenstellung des Materials für die vorliegende Dokumentation verwendet:

1. *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes* vom 20. Dezember 1990, Bundesgesetzblatt Teil I, Nr. 73, S. 2954 - 2981, Bonn 1990
2. L. Bergmann, R. Möhrle, A. Herb, *Datenschutzrecht*, Stuttgart, München, Hannover, Berlin, Weimar 1977, Stand: März 1995
3. H.-J. Schaffland, N. Wiltfang, *Bundesdatenschutzgesetz (BDSG)*, Berlin 1977, Stand: Januar 1996
4. S. Simitis, U. Dammann, H. Geiger, O. Mallmann, S. Walz, *Kommentar zum Bundesdatenschutzgesetz*, Baden-Baden 1992

Online stehen die „Datenschutz-Informationen“ der Humboldt-Universität in Berlin im World Wide Web unter dem URL

```
http://www.rewi.hu-berlin.de/Datenschutz
```

zur Verfügung.

Index