	Erstellt	**Geprüft und Freigegeben**
am:		
von:		
Unterschrift:		

Aufbewahrungsdauer von relevanten DV-Unterlagen

Überlegungen aus datenschutzrechtlicher Sicht

In der Konferenz der Obersten Aufsichtsbehörden für den Datenschutz so-wie in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist schon mehrfach die Frage der Aufbewahrungsfrist von Konsolprotokollen erörtert worden, ohne dass es bisher in dieser Frage zu einer abschließenden Meinungsbildung gekommen ist. Ähnliches gilt für die Aufbewahrungsdauer der Nachweise im Zusammenhang mit der Eingabekontrolle (Ziffer / der Anlage zu § 6 Absatz 1 Bundesdatenschutzgesetz bzw. der entsprechenden Bestimmung in den Landesdatenschutzgesetzen), für die Aufzeichnung des berechtigten Interesses an einer Datenübermittlung § 32 Abs. 2 BDSG) sowie weiteren DV-Unterlagen, die datenschutzrecht-lich relevant sein können.

1. Die Datenschutzgesetze des Bundes und der Länder geben für die Festlegung von Aufbewahrungsfristen direkt nicht her. Auch die Kommentare sind hier nicht eindeutig. Um in der Sache weiterzukommen und der DV-Praxis konkrete Hinweise zu geben, soll nachfolgend versucht werden, die Frage der Aufbewahrungsfrist von DV-Unterlagen zu strukturieren und einer Antwort näher zu bringen. Der Diskussionsbeitrag knüpft dabei an die bisherigen Diskussionen sowie die Veröffentlichung „Aufbewahrungsfrist für Nachweise im Sinne des § 6 BDSG" im DATENSCHUTZBERATER Nr. 3 vom 15. März 1983 an.

2. **Datenschutzprüfungen**, die sich auf die Zulässigkeit und Rechtmäßigkeit der Datenverarbeitung, die ordnungsgemäße Anwendung der DV-Programme sowie die Verfolgung und Ahndung von Ordnungswidrigkeiten und Straftaten nach den Datenschutzbestimmungen beziehen, können ohne prüfungsfähige Unterlagen nicht wirksam durchgeführt werden. Es ist deshalb erforderlich sich zunächst einen Überblick über die verschiedenen DV-Unterlagen, ihren Verwendungszweck im Rechenzentrum sowie die datenschutzrechtlichen Erfordernisse zu verschaffen.

2.1 Folgende **DV-Unterlagen und Materialien** lassen sich unterscheiden.

a. Unterlagen und Materialien zur Einrichtung, Ausstattung und **inneren Organisation des Rechenzentrums**

- Betriebsgrundstück, Gebäude, Räume, Inventar
- Ver- und Entsorgungseinrichtungen, Sicherheits- und Alarmeinrichtungen, Betriebstechnik, Transport- und Kommunikationsmittel

- Betriebssoftware einschließlich sonstiger systemnaher bzw. allgemein einsetzbarer Software (Beschaffungsunterlagen, Beschreibungen etc.
- Aufbau- und Ablauforganisation, Geschäftsverteilung, Arbeitsanweisungen, Zutrittsregelungen etc.

b. **Dokumentationsunterlagen der DV-Verfahren**

- Aktenmaterial zur Vorgeschichte. Erstentwicklung und Pflege der DV-Verfahren sowie damit zusammenhängender Hard- und Fremdsoftwarebeschaffungen.
- Verfahren- und Programmdokumentationen einschließlich Abschlussfestergebnisse und Freigabe der Abnahmeerklärungen sowie Anweisungen für die Arbeitsvorbereitung, die Arbeitsnachbereitung und das Operating.
- Benutzerunterlagen einschließlich Datenerhebungsbogen, Anweisungen für die Datenerfassung und Hinweisen zur Fehlerkorrektur.
- Übersicht über die Art der gespeicherten Daten sowie eventuelle Unterlagen zur Veröffentlichung und Anmeldung der Dateien nach den Datenschutzgesetzen des Bundes und der Länder (z. B. §§ 12, 15, 19, 29 BDSB, §§ 8, 14, 21 BrDSG)

c. Unterlagen und Materialien zur **Anwendung** und **Benutzung** von DV-Verfahren (verfahrensbezogene Unterlagen und Materialien)

- Auftragsunterlagen, Weisungen des Auftragsgebers, Berechtigungsprüfungen etc.
- Unterlagen zur Benutzung/Anwendung der DV-Verfahren wie z. B. Termin- und Arbeitspläne, Auftragszettel, JCL-Listen, Dateienein- und ausgang etc.
- Aufzeichnung des berechtigten Interesses für eine Datenübermittlung gemäß § 32 Abs. 2 BDSG

d. Unterlagen und Materialien zur **Systembenutzung (**systembezogene Unterlagen und Materialien)

- System-LOG-Informationen Konsolprotokoll (enthalten keine personenbezogenen Daten)
- SMF-Informationen, Job-Account-Daten
- Schichtpläne, Besucherbuch, Störungsbuch, Wartungsbuch, IMS-Log-Buch etc.
- IMS-Log-Bänder oder dergleichen (enthalten im Datenteil unter Umständen personenbezogene Daten die mit einem eventuellen Sperrungs-bzw. Löschungsanspruch versehen sind)

e. **Ergebnisse der Anwendung** und Nutzung von DV-Verfahren (eigentliche Verarbeitungsergebnisse)

- Erhebungsunterlagen, Erfassungsprotokolle, Eingabeprotokolle etc.
- Druckausgaben, Mikroverfilmungen, grafische oder bildliche Aufbereitungen etc.

- Auf elektronischen Datenträgern gespeicherte Datenbestände, Texte, Schlüsselverzeichnisse, Tabellenwerte etc.

2.2 Der Verwendungszweck dieser Unterlagen ist unterschiedlich. Datenschutzgesichtspunkte spielen bei der Erzeugung und Aufbewahrung insbesondere der verfahrens- bzw. systembezogenen Unterlagen eine untergeordnete Rolle. Im eigentlichen Rechenzentrumsbetrieb dominieren Gesichtspunkte des Arbeitseinflüssen und der Datensicherung. Und nur insoweit werden datenschutzrechtliche Gesichtspunkte berücksichtigt. Die Art der verwendeten Datenträger ist vielfähig, wobei auch hierbei datenschutzrechtliche Erfordernisse nicht im Vordergrund der Überlegungen stehen.

2.3 **Datenschutzrechtliche Erfordernisse ergeben sich vor allem aus folgenden Bestimmungen des BDSG oder des BrDSG (im Bremen):**

a) Zulässigkeit und Rechtmäßigkeit der Datenverarbeitung gemäß §§ 3, 9, 10, 11 BDSG bzw. §§ 3, 10, 11, 13 BrDSG.

b) Auskunfts- und Einsichtsrecht des Datenschutzbeauftragten in Unterlagen und Akten, namentlich in die zu führenden Übersichten, in die gespeicherten Daten, die DVF-Programme und Programmunterlagen gemäß § 19 Abs. 3 BDSG bzw. § 20 Abs. 3 Br DSG.

c) Auskunfts- und Einsichtsrecht der Datenschutzaufsichtsbehörde (in Bremen: Landesbeauftragter für den Datenschutz) in Geschäftsunterlagen, namentlich in die nach § 29 Satz 3 Nr. 1 BDSG vom betrieblichen Datenschutzbeauftragten zu führenden Übersichten, in die gespeicherten personenbezogenen Daten und die DV-Programme gemäß § 30 Abs. 2 und 3 BDSG und § 40 BDSG.

d) Nachträgliche Kontrolle der Dateneingabe (Eingabekontrolle) gemäß Anlage zu § 6 Abs. 1 S 1 BDSG bzw. BrDSG. Bei der Festlegung der Aufbewahrungsfrist für derartige Unterlagen sind die Betroffenenrechte, insbesondere der Löschungs- und Sperrungsanspruch mit zu berücksichtigen.

e) Überwachung der ordnungsgemäßen Anwendung der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, gemäß § 29 Satz 3 Nr. 2 BDSG bzw. § 8 Satz 2 Nr. BrDSG

f) Aufzeichnung des berechtigten Interesses für eine Datenübermittlung gemäß § 32 Abs. 2 BDSG.

g) Ordnungswidrige Tatbestände gemäß § 42 BDSG und ihre Verjährungsfristen.

h) Unbefugte Datenverarbeitung als Straftat nach § 41 BDSG bzw. § 30 BrDSG oder aufgrund bereichsspezifischer Sonderregelungen wie z. B. Bruch des Statistikgeheimnisses, des damit zusammenhängender Verjährungsfristen nach dem STGB.

3. Für die **Aufbewahrungsfrist der verschiedenen DV-Unterlagen** sind neben den datenschutzrechtlichen Erfordernissen noch weitere Gesichtspunkte wie z. B. andere Rechtsvorschriften, privatrechtliche Vereinbarungen, betriebliche oder verwaltungsinterne Regelungen etc. von Bedeutung. Sofern sich aus anderen Rechtsvorschriften wie z. B. em öffentlichen Haushalts- und Kassenrecht, dem Steuer- und Abgabenrecht, dem Handelsgesetzbuch, dem Vertragsrecht, aus innerbetrieblichen Regelungen oder dgl. Keine anderen (Längeren) Fristen ergeben, sollten für die verschiedenen DV-Unterlagen wenigstens die folgenden Aufbewahrungsfristen vorgesehen werden:

Aufbewahrungsfristen von DV-Unterlagen

DV-Unterlage	Aufbewahrungspflicht
➢ **Unterlagen und Materialen zur Einrichtung, Ausstattung und inneren Organisation des Rechenzentrums** • Betriebsgrundstück, Gebäude, Räume, Inventar • Ver- und Entsorgungseinrichtungen, Sicherheits- und Alarmeinrichtungen, Betriebstechnik, Transport- und Kommunikationsmittel • Hardware-Einrichtungen (Konfigurationsübersichten, Miet- oder Kaufverträge etc.) • Betriebssoftware einschließlich sonstiger systemnaher bzw. allgemein einsetzbarer Software (Beschaffungsunterlagen, Beschreibungen etc.) • Aufbau- und Ablauforganisation, Geschäftsverteilung, Arbeitsanweisungen, Zutrittsregelungen etc.	Entsprechend der jeweiligen Akten bzw. Archivordnung unter Berücksichtigung haushaltsrechtlicher, steuerrechtlicher, handelsrechtlicher, vertraglicher etc. Aufbewahrungsbestimmungen
➢ **Dokumentenunterlagen** • Aktenmaterial zur Vorgeschichte, Erstentwicklung und Pflege der DV-Verfahren sowie damit zusammenhängender Hard- und Fremdsoftwarebeschaffungen • Verfahren- und Programmdokumentation einschließlich Abschlusstestergebnisse und Freigabe- bzw. Abnahmeerklärungen wobei Anweisungen für die Arbeitsvorbereitung die Arbeitsnachbereitung und das Operating • Benutzerunterlagen einschließlich Datenerhebungsbogen, Anweisungen für die Datenerfassung und Hinweisen für die Fehlerkorrektur • Übersicht über die Art der gespeicherten Daten sowie eventuelle Unterlagen zur Veröffentlich und Anmeldung der Dateien nach den Datenschutzgesetzen des Bundes und der Länder (z. B. §§ 12, 15, 19 Abs. 4, 29 BDSG, §§ 8, 14, 21 BrDSG	Mindestens so lange wie die Verarbeitungsergebnisse beim Benutzer/Auftraggeber aufzubewahren sind, ansonsten entsprechend der jeweiligen Akten- oder Archivordnung
➢ **Unterlagen und Materialien zur Anwendung von DV-Verfahren**	Nach Vorgaben des Benutzers Auftrags-

(verfahrensbezogene Unterlagen) • Auftragsunterlagen, Weisungen des Auftraggebers, Berechtigungsprüfungen etc. • Unterlagen zur Benutzung/Anwendung der DV-Verfahren wie z. B. Termin- und Arbeitspläne Auftragszettel, JCL-Listen, Daten-ein- und Ausgang etc. • Aufzeichnung des berechtigten Interesses für eine Datenübermittlung gemäß § 32 Abs. 2 BDSG	gebers, mindestens doch 3 Jahre
➢ **Unterlagen und Materialien zur Systembenutzung** • System-Log-Informations/Konsolprotokolle (enthalten keine personenbezogenen Daten) • SMF-Information/Job-Account-Daten • Schichtpläne, Besucherbuch, Störungsbuch, Wartungsbuch, IMS-Log-Buch etc. • IMS-Log-Bänder oder dergleichen DB-Protokollierung (enthalten im Datenteil unter Umständen personenbezogene Daten, die mit einem eventuellen Sperrungs- oder Löschungsanspruch versehen sind)	Mindestens 3 Jahre 1 Monat
➢ **Ergebnisse der Anwendung und Nutzung von DV-Verfahren (eigentliche Verarbeitungsergebnisse)** • Erhebungsunterlagen, Erfassungsprotokolle, Eingabeprotokolle etc. • Druckausgaben, Mikroverfilmungen, grafische oder bildliche Aufbereitungen etc. auf elektronisch-lesbaren Datenträgern gespeicherte Datenbestände, Texte, Schlüsselverzeichnisse. Tabellenwerte, etc.	Vorgabe des Benutzer/ Auftraggebers

4. Für die viel diskutierte Frage der Aufbewahrungsfrist von Konsolprotokollen (System-Log-Informationen) kann folgende Überlegung als Anhalt zur Fristbestimmung dienen:

System-Log-Informatioen können u´zusammen mit anderen Informationen wie z. B. Job-Account-Daten, Arbeits- und Terminplänen, Schichtplänen etc. bei nachträglichen Daten-

schutzkontrollen verwendet werden. Da im vorhinein der Anlass einer nachträglichen Kontrolle nicht feststeht, müsste eigentlich der schlimmstmögliche Fall ins Auge gefasst werden, der sich nach den datenschutzrechtlichen Strafvorschriften § 30 Abs. 2 BrDSG, § 41 Abs. 2 BDSG) ergibt. Nach § 78 Abs. 3 Nr. 4 StGB verjähren derartige Straftaten nach 5 Jahren. System-Log-Informationen wären danach also auf welchem Datenträger auch immer – mindestens 5 Jahre aufzubewahren.

Im Hinblick darauf, dass System-Log-Informationen für nachträgliche Datenschutzkontrollen allein nicht ausreichen und der erschwerte Tatbestand des § 30 Abs. 2 BrDSG bzw. § 41 Abs. 2 BDSG eher die Ausnahme darstellen wird, kann eine kürzere Aufbewahrungsfrist erwogen werden. Straftaten nach § 30 Abs. 1 BrDSG oder § 41 Abs. 1 BDSG verjähren gemäß § 78 Abs. 3 Nr. 5 StGB bereits nach 3 Jahren. Sofern sich aus anderen Rechtsvorschriften wie z. B. dem öffentlichen Haushalts- und Kassenrecht, dem Steuer- und Abgabenrecht, dem Handelsgesetzbuch oder Vertragsrecht keine anderen (längeren) Fristen ergeben, sollten System-LG-Infomationen wenigstens 3 Jahre verfügbar bleiben. Auf welchem Datenträger (Papier oder Magnetband) die Informationen gespeichert, d. h. aufbewahrt werden, bleibt den jeweiligen räumlichen organisatorischen und systemtechnischen Gegebenheiten überlassen.

Wichtig dabei ist jedoch, dass die Informationen lückenlos und vollständig sind, d. h. alle erzeugten System-Log-Information umfassen, nicht nachträglich verändert werden und mindestens 3 Jahre auswertbar bleiben.

In diesem Zusammenhang wird häufig argumentiert, dass die tägliche Prüfung der Konsolprotokolle eine längere Aufbewahrungsfrist ersetzen könne. Abgesehen davon, dass eine vollständige und umfassende Prüfung der Konsolprotokolle im täglichen Rechenzentrumsbetrieb nicht zu realisieren sein wird, erscheint dieser Gedanke auch deshalb nicht zwingend, weil es sich bei dieser Prüfung um einen isolierten Vorgang handelt, unter dem primären Gesichtspunkt der Betriebssicherheit im Sinne der datenschutzrechtlichen Strafvorschriften zum Gegenstand haben, sondern z. B. auch die ordnungsgemäße Anwendung von DV-Programmen oder die sorgfältige Auswahl eines DV-Dienstleistungsunternehmens. Eine wesentlich kürzere Aufbewahrungsfrist der Konsolprotokolle (Systemmeldungen angereicherte Job-Account-Daten). Dies ist heute jedoch (noch) nicht der Fall.

5. Die Aufbewahrungsdauer der anderen unter c) und b) genannten DV-Unterlagen könnte aufgrund ähnlicher Überlegungen ebenfalls auf drei Jahre festgelegt werden. Lediglich für die Aufbewahrungsfrist von IMS-Log-Informationen/LMS-Log-Bänder) könnte folgendes gelten:

Was die Aufbewahrungsdauer dieser Bänder anbetrifft, so enthalten die Datenschutzgesetze auch hierzu keine speziellen Regelungen. Sie ist daher von Fall zu Fall festzuglegen. Neben dem Sicherungsinteresse des Datenverarbeiters ist von Bedeutung:

5.1 Nach der Anlage zu § 6 Abs. 2 BDSG oder BrDSG ist u.a. zu gewährleisten, dass nachträglich **überprüft und festgestellt** werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind **(Eingabekontrolle).** Eine Protokollierung der einzelnen Eingabe wird vom Gesetz für den Regelfall nicht gefordert. Es reicht vielmehr aus, wenn die näheren Umstände einer Eingabe aufgrund von Unterlagen jederzeit rekonstruierbar sind, z. B. aufgrund der Verfahrensdokumentation, von System – und Konsolprotokollen, von Änderungsprotokollen und sonstigen Unterlagen beim zuständigen Bearbeiter etc. Aus diesen Unterlagen insgesamt müssen der Zeitpunkt der Dateneingabe, ihr Inhalt sowie die Identität desjenigen, der die Daten eingegeben hat, hervorgehen.

5.2 Mit der nachträglichen Überprüfung und Feststellung kollidiert unter Umständen der datenschutzrechtliche **Löschungsanspruch** einen Betroffenen. Dieser Anspruch verpflichtet die

speichernde Stelle. Maßnahmen zu treffen, die eine künftige Informationsgewinnung aus gespeicherten und jetzt zu löschenden Daten unmöglich machen. Die Kenntnisnahme des Informationsgehaltes eines Datums durch den Einsatz der Datenverarbeitung mus also der speichernden Stelle unmöglich gemacht werden. Es genügt nicht, dass die speichernde Stelle durch Nutzungsverbote oder Zugangsbeschränkungen die Daten der Kenntnisnahme durch ihre Mitarbeiter entzieht. Eine Löschung liegt ebenfalls nicht vor, wenn die Daten an anderer Stelle oder auf einem anderen Datenträger erneut oder weiterhin gespeichert werden. Das bedeutet, dass nur die Daten im jeweiligen aktuellen Datenbestand, sondern auch in allen angelegten Kopien, Logbändern oder der gleichen zu löschen sind.

Aufgrund dieser Überlegungen und nach Abwägung des angesprochenen Interessenkonflikts bestehen aus der Sicht des Datenschutzes grundsätzlich keine Bedenken gegen eine Praxis, IMS Logbänder 30 Tage aufzubewahren. Hierbei ist davon auszugehen, dass:

a) Die Eingabekontrolle aufgrund anderer Unterlagen des Rechenzentrum und/Oder des Anwender/Auftraggebers grundsätzlich möglich ist. Die Aufbewahrungsdauer dieser Unterlagen richtet sich nach den allgemeinen Vorschriften der Datenschutzgesetze oder speziellen weitergehenden Vorschriften, wie z. B. haushaltsrechtlichen, steuerrechtlichen, handelsrechtlichen oder vertraglichen Bestimmungen.
b) Die Logbänder ausschließ0lich für Sicherungszwecke und nur durch berechtigtes Personal benutzt werden.
c) Die Logbänder nach Ablauf der 30-tägigen Sperrfrist unverzüglich gelöscht, d. h. neu überschreiben oder physisch gelöst werden und
d) Bei der Aufbewahrung (Archivierung) der Logbänder die erforderlichen technischen und organisatorischen Sicherungsmaßnahmen getroffen sind.
e) Die Aufbewahrungsdauer dieser Unterlagen und Materialien richtet sich nach den Erfordernissen der speichernden Stellen (Benutzer oder Auftraggeber der RZ).

6. Abschließend sei darauf hingewiesen, dass die Festlegung der Aufbewahrungsdauer nicht isoliert für eine einzelne Unterlage bzw. einen einzelnen Nachweis erfolgen sollte, sondern stets im Zusammenschau aller relevanten DV-Unterlagen unter Berücksichtigung des jeweiligen Verwendungszwecks sowie der speziellen datenschutzrechtlichen Erfordernisse. Außerdem sollte berücksichtigt werden, dass die Entwicklung im Bereich der Informationstechnologie mit den ständig „verbesserten" oder neuen Modellen, Typen, Programm-Versionen oder Diensten dazu zwingt, die einmal getroffenen Festlegungen laufend zu überprüfen und ggf. anzupassen.