

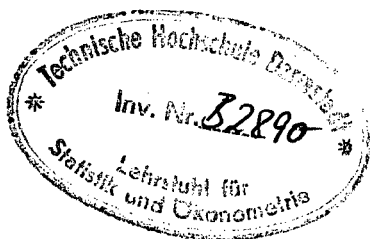
Hentschel/Gliss/Bayer/Dierstein

---

# Datenschutzfibel

unter besonderer Berücksichtigung  
des Personalwesens

---



Juni 1974

Verlag J. P. Bachem in Köln

# Inhalt

1.	<b>Einleitung</b>	9
2.	<b>Begriffsdefinitionen</b>	11
3.	<b>Datenschutz aus der Sicht der Fachabteilung</b>	15
3.1	Einleitung	15
3.2	Der Bürger als Arbeitnehmer	15
3.3	Personaldaten als Entscheidungshilfe	16
3.4	Vertraulichkeit von Personaldaten	18
3.4.1	Bisherige betriebliche Handhabung	18
3.4.2	Zuordnung nach hierarchischen Kriterien	21
3.4.3	Erfordernisse	22
3.5	Anforderungen an die Systemorganisation	24
3.6	Erfassung von Daten	26
3.7	Arbeitgeberfürsorgepflicht und gesetzliche Auskunftspflicht	26
3.8	Bundesdatenschutzgesetz	31
3.8.1	Relevante Paragraphen für die Fachabteilung	31
3.8.2	Problematik für Fachabteilung und DV	35
3.9	Sicherheit der Systeme	35
3.10	Datenschutzbeauftragter und Fachabteilung	36
3.11	Datenschutzbeauftragter	38
3.11.1	Schwerpunkte des Aufgabenbereiches	38
3.11.2	Organisatorische Einordnung	38
3.11.3	Anforderungsprofil	40
	Anhang zu 3.	41
4.	<b>Organisatorische Erfordernisse als flankierende Maßnahmen zur Datensicherung</b>	45
4.1	Organisation als Rahmen für die Kommunikation zwischen Fachabteilung und Datenverarbeitung	45
4.2	Organisation und Systemablauf	47
4.3	Datenschutzbeauftragter und Organisation	49
4.4	Laufende Systeme – zukünftige Systeme; Anforderungskatalog	51
4.4.1	Organisation der technischen Abläufe	52
4.4.1.1	Strukturelle Anforderungen	52
4.4.1.2	Arbeitsfluß, Dateienverwaltung, Programmverwaltung	53
4.4.2	Ablauforganisation	56
4.4.2.1	Daten	56

4.4.2.2	Eingabe .....	57
4.4.2.3	Verarbeitung .....	57
4.4.2.4	Ausgabe .....	58
4.4.3	Organisation der Funktionen – Einordnung der Benutzer in die logische Systemstruktur .....	59
4.4.3.1	Systementwicklungen (Anwendersysteme) .....	59
4.4.3.2	Gruppen für die Wartung der Anwendersysteme .....	59
4.4.3.3	Funktionale Zuständigkeit der Anwender .....	60
4.5	Hinweise, Anhang .....	61
5.	<b>Sicherheitsanalyse von Datenverarbeitungssystemen</b> .....	69
5.1	Sicherheitsaspekte in komplexen Systemen .....	69
5.1.1	Grade der Sicherheit .....	70
5.1.2	Realistisches Sicherheitskonzept .....	70
5.1.3	Eine Methodologie der Sicherheitsanalyse .....	71
5.1.4	Identifikation von schutzbedürftigen Objekten .....	71
5.1.5	Wertung von schutzbedürftigen Objekten .....	71
5.1.6	Identifikation und Wertung der Gefahren .....	72
5.1.7	Schema der Methodologie .....	73
5.1.8	Alternative Methodologien .....	73
5.1.9	Sicherheit: State of the Art .....	74
5.2	Charakterisierung und Klassifizierung von Schwachstellen .....	74
5.2.1	Sicherheitseinrichtungen der Systemkern-Hardware .....	74
5.2.2	Wirksamkeit der Sicherheitseinrichtungen .....	75
5.2.3	Hardware- und Software-Gefahren im Systemkern .....	76
5.2.4	System-Generierung und Software-Anomalien .....	78
5.2.5	Die Zugriffssicherung bei Dateien .....	80
5.2.6	Die Schnittstelle Mensch-System .....	81
5.2.7	Kommunikationslinien und Terminale .....	82
5.2.8	Externe Katastrophen .....	83
5.2.9	Gesetzliche Randgebiete .....	84
5.3	Aufgaben des Datenschutzbeauftragten .....	85
5.3.1	Die besondere Stellung des Datenschutzbeauftragten .....	85
5.3.2	Generierung von Fehler-Hypothesen .....	85
5.3.3	Filter und Bestätigung .....	86
5.3.4	Schwachstellen-Demonstration .....	86
5.3.5	Schwachstellen-Verallgemeinerung .....	87
5.3.6	Einige Erfahrungswerte .....	87
6.	<b>Datenschutz und Datensicherung in Datenverarbeitungssystemen</b> .....	89
6.1	Die Rolle der Wirtschaft bei der Problemlösung .....	90
6.1.1	Aufgaben und Verantwortlichkeiten bei der Lösung des Problems DATENSCHUTZ .....	92

6.1.2	Datenschutz vs. Datensicherung / Rolle des Datenschutzbeauftragten .....	93
6.2	Datenverarbeitung als Risiko für Datenschutz und Datensicherung .....	94
6.2.1	Kennzeichnende Merkmale der elektronischen Datenverarbeitung (EDV) aus der Sicht der Datensicherung .....	95
6.2.2	Konventionelle und neue Gefahren .....	96
6.2.3	„Daten“-Sicherung als übergreifendes Problem .....	97
6.2.4	Speicherung in DV-Systemen als Risiko für den Datenschutz ..	100
6.2.4.1	Verlust des Kontextes .....	101
6.2.4.2	Sensibilisierung durch Korrelation .....	104
6.2.4.3	Reindividualisierung .....	105
6.3	Sicherheit als Grundkonzept für DV-Systeme .....	106
6.3.1	Konstruktionsprinzipien für sichere DV-Systeme .....	107
6.3.2	Eigenschaften der Zugriffsmechanismen .....	112
6.4	Sicherungsmaßnahmen bei Datenbanken und Datenbanksystemen .....	114
6.4.1	Grundprinzipien der Sicherung bei Datenbanksystemen ....	114
6.4.2	Benutzeridentifizierung .....	116
6.4.3	Zugriffssicherung .....	117
6.4.4	Systemreaktionen .....	118
6.4.5	Statistik und Journalführung .....	119
6.4.6	Sicherung durch Kryptographie .....	120
6.5	Nachträgliche Sicherung unsicherer Systeme – Schlußbemerkung .....	120
7.	<b>Schrifttum</b> .....	123