

Orientierungshilfe
für
Erforderliche Maßnahmen der
technischen und organisatorischen Sicherheit

Die nachfolgende Übersicht stellt die grundlegend notwendigen Maßnahmen dar, die zur Erreichung der technischen und organisatorischen Sicherheit bei der Be- und Verarbeitung personenbezogener Daten ergriffen werden müssen.

Aufgrund der Eigenart der jeweils zu be- und verarbeitenden personenbezogenen Daten oder aufgrund besonderer gesetzlicher Bestimmungen und Vorschriften können weitere Maßnahmen erforderlich sein.

Sofern eine einzelne Maßnahme auf mehrere Art und Weisen und mit unterschiedlich intensiver Schutzwirkung realisiert werden kann, so ist jeweils die Form der Realisierung zu wählen, die der spezifischen Umgebung, der spezifischen Schutzwürdigkeit der zu be- und verarbeitenden Daten und dem spezifischen Bedrohungspotenzial angemessen Rechnung trägt.

Ist eine Maßnahme in der nachfolgenden Tabelle in der Form "(X)" markiert, so ist diese nur für den Fall zu ergreifen, dass besonders schutzwürdige personenbezogene Daten be- und verarbeitet werden.

Für einzelne Maßnahmen oder Maßnahmenbündel liegen spezielle und detaillierte Orientierungshilfen vor, die bei Bedarf angefordert werden können.

Der Bayerische Landesbeauftragte für den Datenschutz

- 2 -

Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Infrastrukturelle Maßnahmen

Einbruchsschutz (Fenster, Türen)	X	X	X			
Vermeidung wasserführender Leitungen	X	X	X			
verdeckte Kabelführung	X	X	X		X	
Notausschalter	X	X				
verschlossene Behälter, Schränke, Räume	X	X	X	X	X	
Einbruchmeldeanlage	X	X	X			
Feuchtigkeitsmeldeanlage	X	X	X			
Brandmeldeanlage	X	X	X			
gesicherte Klimatisierung	X	X				
gesicherte Stromversorgung	X	X	X			
Überspannungsschutz	X	X	X			
angepasste Stromkreisaufteilung	X	X	X			
schadensminimierende Netztopologie			X		X	
unterbrechungsfreie Stromversorgung	X	X	X			
Brandabschottung der Versorgungstrassen	X	X	X		X	
Vermeidung von Brandbrücken	X	X	X		X	
geeignete Feuerlöschgeräte	X	X	X			
möglichst geringe Brandlast (Papier, usw.)	X	X	X			
separates Datensicherungsarchiv	X	X		X	X	
gesicherte Übergangsstelle(n)						X

Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Zugangssicherheitsmaßnahmen

abgeschotteter Bereich	X	X	X			
verschlossene Räume	X	X	X	X		
Zutrittskontrollen (Ausweisleser, ...)	X	X	X			
festgelegte Zugangsberechtigungen	X	X	X			
revisionsfähige Schlüsselverwaltung	X	X	X			

	Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
--	---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Zugriffssicherheitsmaßnahmen

begrenzte System-Managerfunktion	X	X				X	
Deaktivierung nicht benutzter Anschlüsse			X				
eindeutige Benutzeridentifizierung	X	X		X	X	X	X
starke Benutzerauthentifizierung	X	X		X	X	X	X
bedarfsgerechte Rechtezuweisung	X	X		X	X	X	X
Nutzung von Boot-/Setup-Passwort		X		X	X		
Datenverschlüsselung (Festplatte)	(X)	(X)		(X)	X		
passwortgeschützte Bildschirm-Dunkelschaltung				X	X		
Sperrung von Diskettenlaufwerken				X	(X)		
separate Zugriffssicherheitssoftware	X	X		X	X		
Begrenzung der erfolglosen Anmeldeversuche	X	X		X	X	X	X
geordnete Systemverwaltung	X	X		X	X	X	X
zwangsläufige (Benutzer-Menüführung)	X	X		X	X	X	
Sperrung der Betriebssystemebene				X	X	X	X
Vom Benutzer vergebene Passwörter	X	X		X	X	X	X
Verschluss der Sicherungsträger	X	X		X	X		
sicherheitsspezifische Netztopologie						X	X
Trennung von eingehenden und ausgehenden Verbindungen							X
Festlegung berechtigter Kommunikationspartner (Rufnummern)							X

Der Bayerische Landesbeauftragte für den Datenschutz

- 5 -

	Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
--	---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Organisatorische Maßnahmen

Funktionstrennung	X	X				X	
Sicherheitsrichtlinien	X	X	X	X	X	X	X
Programmierrichtlinien (Menütechnik, Benutzerführung, ...)	X	X		X	X	X	X
PC-Verpflichtungserklärung (Mitarbeiter)				X	X	X	X
klare Verantwortungsregelungen	X	X	X	X	X	X	X
Verfahrensverzeichnis	X	X		X	X		X
formalisierte Berechtigungsvergabe, Berechtigungsänderung und -widerruf	X	X		X	X	X	X
Freigabeverfahren für Software	X	X		X	X	X	
Trennung von Test und Produktion	X	X					
Geregelte Datenträgerverwaltung (inkl. Aufbewahrungsrichtlinien)	X	X		X	X		
Geregelte Eingangskontrolle von Datenträgern und Dokumenten	X	X		X	X	X	X
Virenvorsorge	X	X		X	X	X	X
Richtlinien für Passwortaufbau	X	X		X	X	X	X
Richtlinien für Passwortgebrauch	X	X		X	X	X	X
Verbot privater Hardware	X	X		X	X	X	X
Verbot privater Software	X	X		X	X	X	X
Überwachung von Fremdpersonal	X	X	X	X	X	X	X
unangemeldete und unregelmäßige Kontrollen	X	X	X	X	X	X	
Bedienungs- und Benutzeranweisungen	X	X		X	X	X	X
Benutzerservice und -betreuung	X	X		X	X	X	X

Der Bayerische Landesbeauftragte für den Datenschutz

- 6 -

Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Beweissicherungsmaßnahmen

sicherheitsrelevante Protokollierung	X	X		X	X	X	X
Protokollaufbewahrung (z. B. 1 Jahr)	X	X		X	X	X	X
revisionsfähige Schlüsselverwaltung	X	X	X	X	X	X	X
revisionsfähige Benutzerverwaltung	X	X		X	X	X	X
Programmentwicklungsdokumentation	X	X		X	X	X	
Programmablaufdokumentation	X	X				X	
Dokumentation der Abruf- und Übermittlungsprogramme						X	X
Dokumentation der Empfänger						X	X

	Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
--	---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Notfallvorsorgemaßnahmen

Übersicht Verfügbarkeitsanforderungen	X	X	X			X	
Datensicherungskonzept	X	X		X	X		
Störfallplan	X	X	X	X		X	X
Notfallhandbuch	X	X	X	X	X	X	X
Notfallübungen	X	X	X			X	X
Wiederanlaufplan	X	X	X			X	X
Wiederanlauftest	X	X	X			X	X
Ersatzbeschaffungsplan	X	X	X			X	X

Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Übertragungssicherheitsmaßnahmen

Verschlüsselungskomponenten					(X)	X
Nutzung von Standardangeboten (z.B. Rückruffunktionen, Virtuelles Netz)						X
Einrichten geschlossener Benutzergruppen						X
Vertragliche Pflichtenfestlegung						X
Deaktivierung unbenutzter Anschlussstellen	X	X	X	X	X	

	Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
--	---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Personelle Sicherheitsmaßnahmen

schriftliches Anforderungsprofil	X	X				X	X
gründliche Einweisung	X	X	X	X	X	X	X
regelmäßige fachliche Weiterbildung	X	X	X	X	X	X	
regelmäßige Belehrung und Schulung in einschlägigen Gesetzen und Vorschriften	X	X		X	X	X	
Vertretungsregelung	X	X	X	X	X	X	X
schriftl. Festlegung Fremdpersonal	X	X	X	X	X	X	X

	Rechenzentrum	Abteilungsrechner, Server	Netzknoten, Verteiler	Endgerät	tragbare PC	lokale Vernetzung	Anschluss an öffentliche Netze
--	---------------	---------------------------	-----------------------	----------	-------------	-------------------	--------------------------------

Sonstige Sicherheitsmaßnahmen

Entsorgungsregelung Festplatten	X	X		X	X		
Entsorgungsregelung sonstiger maschinell lesbarer Datenträger	X	X		X	X		
Entsorgungsregelung Druckerzeugnisse	X	X		X	X	X	X
Kontrolle der Sicherheitsorganisation	X	X	X	X	X	X	X
Verträge mit Fremdfirmen	X	X	X				X
Netzwerkdokumentation (Kabelplan, usw.)						X	X
einheitliche Beschaffungsstrategie	X	X	X	X	X		