

4. Checkliste Zugriffskontrolle

Abkürzungen: erf. = erfüllt, nicht erf. = nicht erfüllt, nicht erfdl. = nicht erforderlich / nicht zutreffend

Vorgabe		erf.	nicht erf.	nicht erfdl.	Bemerkungen
Zugriffskontrolle					
4.1	Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte				
4.1.1	Schriftliches Berechtigungskonzept			x	
4.1.2	Programmtechnisches Berechtigungskonzept	x			ERP / Banking / Adressverwaltung
4.1.3	Rollendefinition	x			
4.1.4	Differenzierte Berechtigungen (Daten)	x			
4.1.5	Differenzierte Berechtigungen für Kenntnisaufnahme, Veränderung, Löschung	x			
4.1.6	Differenzierte Berechtigungen (Anwendungen)	x			
4.1.7	Differenzierte Berechtigungen (Betriebssystem)	x			
4.1.8	Protokollierung				Zugriffsprotokollierung
4.1.8.1	Verfahrensanweisung/Richtlinie			x	
4.1.8.2	Dateizugriffe	x			
4.1.8.3	Programmausführung	x			
4.1.8.4	Shell-Zugriff			x	Zugriff auf Dateisystemebene
4.1.8.5	Richtlinienverstoß	x			
4.1.8.6	Manuelle Protokollauswertung	x			Wie oft, durch wen?
4.1.8.7	Automatische Protokollauswertung			x	Wie oft, durch wen?
4.1.8.8	Aufbewahrung der Protokolle (max.1a)				durchschnittlich 8 Wochen
4.2	Datenträger (DT)				
4.2.1	Benennung eines Verantwortlichen	x			F. Hochdorfer
4.2.2	Mobile DT - Art und Anzahl				beweglich, nicht stationär eingebaut
4.2.2.1	Festplatten			x	
4.2.2.2	USB-Sticks	x			ca. 10
4.2.2.3	SD-Karten	x			4, nur Kameras
4.2.2.4	Disketten			x	
4.2.2.5	Magnetbandkassetten			x	
4.2.2.6	CD	x			keine personenbezogenen Daten
4.2.2.7	DVD	x			keine personenbezogenen Daten
4.2.3	Lagerung nach Dienstschluss			x	
4.2.3.1	Verfahrensanweisung/Richtlinie			x	
4.2.3.2	abschließbare Schränke			x	

Vorgabe		erf.	nicht erf.	nicht erfdl.	Bemerkungen
4.2.4	Auslagerung von Sicherungsdatenträgern	x			externe Sicherung Privatwohnung GF
4.3	Datenträgerverwaltung				keine externen Datenträger mit personenbezogenen Daten
4.3.1	Nachweis über, Eingang, Ausgang sowie Bestand (Verzeichnisse)			x	
4.3.2	Datenträgerinventuren			x	
4.3.3	Festlegungen zur Datenträgerverwendung			x	
4.3.4	Abgrenzung der Bereiche, in denen sich DT befinden dürfen			x	
4.3.5	Festlegung der Personen, die DT befugt sind, DT zu entnehmen			x	
4.3.6	Festlegung der DT-Empfänger			x	
4.3.7	Quittierverfahren			x	
4.3.8	Datenträgerbegleitpapiere			x	
4.3.9	Äußerliche Kennzeichnung der eigenen DT zur Unterscheidung von fremden DT			x	
4.3.10	Trennung der DT verschiedener Auftraggeber			x	
4.3.11	Eigener DT-Pool für jeden Kunden			x	
4.3.12	Verbot des Einsatzes privater DT	x			Richtlinie, Dienstanweisung
4.3.13	Protokollierung der DT-Aussonderung			x	
4.4	Datenträgervernichtung/-entsorgung				
4.4.1	Richtlinien zur Entsorgung/Vernichtung von Fehldrucken und unbrauchbaren bzw. nicht mehr gebrauchten Datenträgern	x			
4.4.2	Datenschutzgerechte Löschung verwendeter DT vor neuer Verwendung bzw. Weitergabe	x			
4.4.3	Sichere Zwischenlagerung	x			abgeschlossener Serverraum
4.4.4	Einsatz von „Reißwolf“/Shredder	x			P-4
4.4.5	Einsatz von Datenträgerlöschgeräten oder - Software			x	
4.4.6	Einsatz von Geräten zum Verbrennen/Zerstören			x	
4.4.7	Kontrolle der ordnungsgemäßen Vernichtung			x	
4.4.8	Einsatz von Entsorgungsunternehmen			x	
4.4.8.1	Zuverlässiges Entsorgungsunternehmen ausgewählt?			x	
4.4.8.2	Vertragliche Regelung vorhanden			x	
4.4.8.3	Entsorgungsbescheinigung, Löschprotokoll			x	
4.5	Regelungen für das Kopieren von DT				
4.5.1	Richtlinie vorhanden			x	
4.5.2	Sperrung der Laufwerke und Anschlüsse (USB, Diskette, CD/DVD ...)			x	
4.5.2.1	Mechanische Verriegelung			x	

Vorgabe		erf.	nicht erf.	nicht erfdl.	Bemerkungen
4.5.2.2	Systemtechnische Einstellung			x	
4.5.2.3	Einsatz spezieller Software			x	
4.5.2.4	Weitere Schnittstellen, die Zugriff ermöglichen, gesperrt			x	
4.5.3	Kopierfunktion grundsätzlich deaktiviert			x	
4.5.4	Einsatz privilegierter Arbeitsplätze			x	
4.5.4.1	Wo?			x	
4.5.4.2	Zu welchem Zweck?			x	
4.5.4.3	Wer hat Zugriff?			x	
4.5.4.4	Netzwerktechnische Anbindung			x	
4.5.4.5	Besondere Sicherheitsmaßnahmen	x			eingeschränkte Benutzerrechte zum Zugriff auf pers. bez. Daten
4.6	Taschenverbot bzw. -kontrollen			x	
4.7	Zugriffsschutz durch Bildschirmschoner	x			GPO
4.7.1	Automatische Sperre	x			GPO
4.7.2	Sperre über Funktionstasten			x	
4.7.3	Ausschließlich passwortgestützte Aufhebung	x			GPO
4.8	Regelungen und Kontrolle von externer Wartung und Fernwartung			x	keine externe Wartung
4.9	Parasitäre Abstrahlung			x	elektromagnetische Abstrahlungen, Schallausbreitungen u.ä.
4.9.1	Messungen durchgeführt			x	
4.9.2	Gegenmaßnahmen eingerichtet			x	

From: <https://datenschutzwiki.w3.de/> - **w3 Datenschutzwiki**

Permanent link: https://datenschutzwiki.w3.de/datenschutz:checkliste_tom_zugriffskontrolle

Last update: **2018/05/16 08:31**

