

Datensicherheit – Checkliste

Physische Sicherheit	Erfüllt?
Datenträger nicht frei zugänglich?	
Gehäuse oder Klemmen als Mitnahmesicherung für Computer?	
Bildschirme nicht einsehbar von Externen?	
Passwortgeschützter Bildschirmschoner eingestellt?	
Netzwerksicherheit	
Sensible Daten nur auf internen Servern?	
Firewalls auf dem neusten Stand?	
Anti Virus Software installiert (und regelmäßig geupdatet)?	
Informations- und Computersicherheit	
Authentifikation für Datenzugang vorhanden?	
Durch (mindestens eins)	
• Etwas das man weiß (z. B. Passwort) • Etwas das man hat (z. B. Smart Card, Schlüssel) • Etwas über einen selbst (z. B. Fingerabdruck, Face ID, Stimmerkennung)	
Ggf. Benutzerkonten mit verschiedenen Rechten?	
Datenschutz	
Daten sind zweckgebunden erhoben?	
Informierte Einwilligung vorhanden?	
Daten sind anonymisiert oder pseudonymisiert?	
Maßnahmen bei Datenschutzverletzungen sind bekannt?	

Das Material ist im Rahmen des Projekts „DIM.RUHR: Datenkompetenzzentrum für die interprofessionelle Nutzung von Gesundheitsdaten in der Metropole Ruhr“ (Förderkennzeichen: 16DKZ2008[A-F]) entstanden. Dementsprechend spiegelt das Material in Version 1.0 den Stand von 2025 wider.

„**Daten managen - 4.2 Datensicherheit: Checkliste**“ von Anne Mainz und Sven Meister.

Dieses Werk und dessen Inhalt sind – sofern nicht anders angegeben – lizenziert unter CC BY 4.0. Ausgenommen aus der Lizenz sind die verwendeten Logos.

Der Lizenzvertrag ist hier abrufbar:

<https://creativecommons.org/licenses/by/4.0/>

