

Anlage 2

Sicherheitsprotokoll für Berlin
§ 5 II BlnDSG

1. **NUR BEFUGTE KÖNNEN PERSONENBEZOGENE DATEN ZUR KENNTNIS NEHMEN (VERTRAULICHKEIT)**

Das Rechenzentrum ist nur für ausgewählte Mitarbeiter/innen zugänglich: Es gibt ein elektronisch gesichertes Zugangssystem mit Protokollierung.

2. **PERSONENBEZOGENE DATEN BLEIBEN WÄHREND DER VERARBEITUNG UNVERSEHRT, VOLLSTÄNDIG UND AKTUELL (INTEGRITÄT)**

Zugriffe, welche nur für berechtigte Nutzer/innen möglich sind, werden in verschiedenen Systemdateien protokolliert.

3. **PERSONENBEZOGENE DATEN KÖNNEN ZEITGERECHT ZUR VERFÜGUNG STEHEN UND ORDNUNGSGEMÄß VERARBEITET WERDEN (VERFÜGBARKEIT)**

Die Server stehen in einem gesicherten Rechenzentrum mit Feuermelder und Sprinkler. Es erfolgt kein Zugriff ohne Berechtigung, es gibt regelmäßige Backups. Alle Übertragungen finden über verschlüsselte und gesicherte Protokolle statt. Ein physikalischer Transport von Datenträgern ist nicht geplant.

4. **JEDERZEIT KÖNNEN PERSONENBEZOGENE DATEN IHREM URSPRUNG ZUGEORDNET WERDEN (AUTHENTIZITÄT)**

Angelegte Daten und Dateien werden mit Referenz auf den Ersteller gespeichert. Sämtliche Zugriffe auf personenbezogene Daten werden gemäß Punkt 2 protokolliert.

5. **ES KANN FESTGESTELLT WERDEN, WER WANN WELCHE PERSONENBEZOGENEN DATEN IN WELCHER WEISE VERARBEITET HAT (REVISIONSFÄHIGKEIT)**

Jede/r Benutzer/in hat einen individuellen Account mit (Vorname, Nachname) und mit einem selbst gewählten Passwort. Sämtliche Zugriffe auf personenbezogene Daten werden gemäß den Punkten 2 und 3 protokolliert.

6. **DIE VERFAHRENSWEISEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN SIND VOLLSTÄNDIG, AKTUELL UND IN EINER WEISE DOKUMENTIERT, DASS SIE IN ZUMUTBARER ZEIT NACHVOLLZOGEN WERDEN KÖNNEN (TRANSPARENZ)**

Daten werden ausschließlich lokal im System gehalten, dort ist per „privacy by design“-Konzept und implementierungsspezifischer Restriktionen keine, über den Verarbeitungsauftrag hinausgehende Verarbeitung, möglich.