DIGITALE SOUVERÄNITÄT

Volle Kontrolle über Ihre Daten!

KONTAKT

Vertriebsteam
+49 721 35280-0 ▪ info@technidata.de

Ein Service der TechniData IT Gruppe

Als IT-Dienstleister mit Fokus auf IT-Infrastruktur, Rechenzentrumsbetrieb (zertifiziert nach aktuellen Sicherheits- und Datenschutzstandards), Managed Services und IT-Security unterstützen wir Sie dabei, Ihre digitale Souveränität zu stärken – zuverlässig, rechtskonform und technologisch auf dem neuesten Stand.

IT-SICHERHEIT UND DATENSCHUTZ

IT-Sicherheit und Datenschutz ganzheitlich denken:

- Datenlage und IT-Infrastruktur analysieren
- Datenhaltung absichern
- Auftragsverarbeitung rechtssicher gestalten
- IT-Sicherheitsniveau verbessern
- Mitarbeitende sensibilisieren
- Dokumentation & Nachweise bereitstellen
- IT-Partner mit Verantwortung wählen

WORAUF SOLLTEN SIE ACHTEN?

Digitale Souveränität bedeutet mehr als nur Datenspeicherung – es geht um den aktiven Schutz Ihrer digitalen Identität, Systeme und Geschäftsprozesse. Wer sensible Daten extern verarbeitet oder speichert, muss genau hinschauen: Nur wer die Kontrolle über seine IT behält, bleibt unabhängig, sicher und rechtskonform. Achten Sie deswegen darauf, dass Ihre Daten möglichst in Deutschland oder mindestens im rechtssicheren EU-Raum gespeichert bzw. verarbeitet werden – das sichert nicht nur DSGVO-Konformität, sondern schützt Sie auch vor dem ungewollten Zugriff durch Drittstaaten.

CHECKLISTE

Datenlage und IT-Infrastruktur analysieren

- Wo liegen Ihre Daten? (physisch & digital)
- Wer hat Zugriff? (intern & extern)
- Welche Dienste und Anbieter nutzen Sie – und unter welchem Rechtsregime?

Datenhaltung absichern

- DSGVO konforme Datenspeicherung möglichst in deutschen Rechenzentren sicherstellen
- Auf DSGVO-konforme Anbieter achten (Vermeidung von CLOUD-Act-Risiken)
- Backup- & Wiederherstellungsprozesse prüfen und dokumentieren

Auftragsverarbeitung rechtssicher gestalten

- Bestehende Dienstleisterverträge überprüfen (z. B. Hosting, Cloud, IT-Services)
- AV-Verträge abschließen oder aktualisieren
- Klarheit über Verantwortlichkeiten & Kontrollrechte

IT-Sicherheitsniveau verbessern

- Sicherheitskonzepte auf Basis von Standards (z. B. ISO 27001, BSI-Grundschutz)
- Einführung von Zero-Trust-Prinzipien
- Netzwerksegmentierung, Patchmanagement, Monitoring etablieren

Mitarbeitende sensibilisieren

- Datenschutz- und Security-Schulungen durchführen
- Awareness-Kampagnen gegen Social Engineering & Phishing
- Zuständigkeiten und Meldewege bei Vorfällen festlegen

Dokumentation & Nachweise bereitstellen

- Datenschutz-Folgenabschätzungen (DSFA), TOMs, Verfahrensverzeichnisse
- Audit-Trails, Prüfberichte und Schwachstellenanalysen archivieren
- Nachweise für Aufsichtsbehörden und Kunden auf Abruf verfügbar halten

IT-Partner mit Verantwortung wählen

- Möglichst Anbieter mit eigenen, zertifizierten Rechenzentren in Deutschland wählen
- Vertragliche Klarheit über Datenhoheit, Zugriffsschutz und Service-Level
- Langfristige Zusammenarbeit mit Partnern, die DSGVO, Sicherheit und Betrieb vereinen

Weitere Informationen erhalten Sie hier:

TechniData IT AG Emmy-Noether-Str. 9 ▪ 76131 Karlsruhe
info@technidata.de ▪ www.technidata.de