Sicherheit & Standards

Kompakte Übersicht für Procurement/IT/Compliance – bewusst ohne interne Konfigurationsdetails (keine Ports, Pfade, Regelwerke oder Backup-Zeitpläne).

---

1) Standort & Prinzipien

- Datenstandort: Kernsysteme in Deutschland/EU; Verarbeitung innerhalb Europas.
- Datenminimierung: so viel wie nötig, so wenig wie möglich.
- Zweckbindung: projekt- und nachweisbezogen statt „Sammeln auf Vorrat“.
- Nachvollziehbarkeit: Owner, Versionen, Freigaben und Übergaben statt „letzte Datei per Mail“.
- Trennung: Website-Betrieb/Tracking getrennt von Projekt- und Nachweisdaten.

2) Transport & Zugriff

- Transportverschlüsselung: Zugriff/Übertragung über TLS/HTTPS (keine Klartext-Übertragung).
- Zugriffskontrolle: rollenbasiert („Need-to-know“) und aufgabenbezogen.
- Administrative Zugänge: zusätzliche Absicherung ist Standard (z. B. MFA/2FA für kritische Admin-Oberflächen).

3) Backups & Wiederherstellung

- Backups werden regelmäßig erstellt und getrennt aufbewahrt (mehr als eine Kopie).
- Wichtig ist ein definierter Wiederherstellungspfad (Restore), damit „Backup“ nicht nur ein Ordner ist.
- Restore-Tests können je nach Kritikalität als Betriebsroutine vereinbart werden (kurzes Protokoll: Datum/Umfang/Ergebnis).

4) Umgang mit Sicherheitsvorfällen (Incident Response)

- Klarer Ablauf: Einordnung → Eindämmung → Kommunikation → dokumentierte Maßnahmen.
- Für Kundenprojekte können Ansprechpartner, Kommunikationsweg und notwendige Artefakte vorab festgelegt werden.

5) Transparenz & Unterlagen (projektbezogen)

- AVV/DPA inkl. TOMs (wenn ITTCON im Projekt Auftragsverarbeiter ist).
- Datenkategorien, Zwecke, Rollen/Verantwortlichkeiten, Retention/Löschung.
- Sub-Prozessoren/Datenflüsse (Website vs. Projektdaten sauber getrennt).
- Technische Nachweise (z. B. TLS-Check, 2FA-Policy, Backup-/Restore-Protokolle) liegen intern als Proof-Pack vor und werden bei Bedarf kontrolliert bereitgestellt.

Links

https://ittcon.eu/wissen/sicherheit
https://ittcon.eu/datenschutz
https://ittcon.eu/kontakt