

- [österreichisches Unternehmensgesetzbuch \(UGB\)](#),
- [Konsumentenschutzgesetz \(KSchG\)](#),
- [E-Commerce-Gesetz \(ECG\)](#),
- [Telekommunikationsgesetz \(TKG 2021\)](#),
- [EU-DSGVO und österreichisches Datenschutzgesetz \(DSG\)](#).

Typische Datenschutz Struktur:

- Allgemeine Hinweise und Verantwortlicher
- Datenerfassung auf der Website
- Hosting und Server-Logfiles
- Cookies und lokale Speicherung
- Analyse- und Tracking-Tools (z. B. Google Analytics, Plausible etc.)
- Kontaktformular / Kommunikation
- Benutzerkonten oder Login-Bereiche
- Zahlungsdienste (wenn geplant)
- Rechte der betroffenen Personen
- Datensicherheit und Aufbewahrungsdauer
- Änderungen dieser Datenschutzerklärung

Datenschutz – Zusatzinfos & Empfehlungen

(Ergänzende Hinweise zur Verbesserung und laufenden Pflege der Datenschutzerklärung von NEST-Haus GmbH)



Technische & organisatorische Maßnahmen (TOMs)

- **SSL-/TLS-Verschlüsselung:**
Stellt sicher, dass sämtliche Datenübertragungen (Formulare, Logins, Konfigurator) über HTTPS erfolgen.
→ Ergänzt in der Datenschutzerklärung oder Fußzeile: „*Unsere Website verwendet SSL-Verschlüsselung zum Schutz vertraulicher Inhalte.*“
- **Zugriffsmanagement:**
Interne Zugriffe auf personenbezogene Daten (z. B. Kontaktanfragen) sollten nur autorisierten Mitarbeitenden erlaubt sein; idealerweise mit Rollen-/Rechtesystem dokumentiert.

Cookie- und Einwilligungsmanagement

- Nutzt ein [Consent-Tool](#), das den Anforderungen des TKG 2021 (§ 165) und der DSGVO entspricht (z. B. Klaro!, Cookiebot oder eine eigene Lösung).
- Wichtiger Punkt: [Protokollierung der Einwilligung](#) (Datum, Uhrzeit, IP, gewählte Optionen).
- Für jede Kategorie (Notwendig, Statistik, Komfort etc.) sollte eine [deutliche Beschreibung](#) im Banner erscheinen.

Verzeichnis der Verarbeitungstätigkeiten (intern)

Gemäß Art. 30 DSGVO ist ein [internes Verarbeitungsverzeichnis](#) verpflichtend.

Es wird nicht veröffentlicht, dient aber als Nachweis gegenüber der Datenschutzbehörde.
Darin enthalten:

- Zweck der Verarbeitung

- Kategorien von Daten & Betroffenen
- Empfänger (z. B. Hosting-Dienstleister)
- Speicherdauer
- Technische & organisatorische Schutzmaßnahmen

Auftragsverarbeitungsverträge (AVV)

Schließt mit allen externen Dienstleistern, die personenbezogene Daten verarbeiten, einen **AV-Vertrag** ab – insbesondere:

- **Vercel** (Hosting)
- **Upstash Redis** (Session-Verwaltung)
- **Neon PostgreSQL** (Datenbank)

Diese Verträge sind zentraler Nachweis der DSGVO-Konformität. Die Anbieter stellen in der Regel vorgefertigte AV-Vereinbarungen auf ihren Websites bereit.

Datenspeicherung & Löschroutinen

- Definiert interne **Löschfristen**: z. B. Kontaktanfragen nach 3 Jahren, Logfiles nach 30 Tagen.
- Führt, wenn möglich, eine **automatisierte Löschroutine** in der Datenbank oder im CRM ein.
- Dokumentiert, wann Daten tatsächlich gelöscht oder anonymisiert wurden.

Erweiterte Nutzerrechte (praktische Umsetzung)

- Richtet für Datenschutzanfragen eine **eigene E-Mail-Adresse** (z. B. datenschutz@nest-haus.at) ein.
- Entwickelt ein kurzes **internes Verfahren**, wie Anfragen bearbeitet werden (z. B. Frist: 30 Tage laut Art. 12 Abs. 3 DSGVO).
- Achtung: Identitätsprüfung bei sensiblen Auskunfts- oder Löschanfragen ist Pflicht.