DSGVO-Checkliste für den Kleinbetrieb

Die Grundpflichten, die ohne Datenschutzbeauftragten gelten, in sieben Blöcken zum Abhaken: Verzeichnis, Information, Verträge, Technik, Betroffene, Pannen, Beschäftigte.

1 Verzeichnis und Verantwortung
2 Information der Betroffenen
3 Verträge mit Dienstleistern
4 Technik und Organisation
5 Rechte der Betroffenen
6 Datenpannen
7 Beschäftigte

Die Pflichten der DSGVO gelten für jeden Betrieb, der Kunden-, Personal- oder Lieferantendaten verarbeitet, unabhängig von der Größe und unabhängig davon, ob ein Datenschutzbeauftragter bestellt ist. Diese Liste deckt die Grundpflichten ab, die bei einer Prüfung oder Beschwerde zuerst abgefragt werden. Was Sie nicht abhaken können, ist Ihr Arbeitsprogramm.

1 1. Verzeichnis und Verantwortung

- [ ] **Verzeichnis von Verarbeitungstätigkeiten liegt vor**
  Alle Verarbeitungen mit Zweck, Datenarten, Betroffenen, Empfängern, Löschfristen, Schutzmaßnahmen (Art. 30). Vorlage bei contrust in.

- [ ] **Prüfung Datenschutzbeauftragter dokumentiert**
  Zählung der Personen mit Datenzugriff; Prüfung der Ausnahmen (Folgenabschätzung, sensible Daten). Ergebnis schriftlich, auch wenn keine Pflicht besteht.

- [ ] **Zuständigkeit benannt**
  Wer im Betrieb kümmert sich um Datenschutz, Anfragen und Pannen? Name und Vertretung.

2 2. Information der Betroffenen

- [ ] **Datenschutzerklärung auf der Website**
  passt zu den tatsächlich eingesetzten Diensten (Hosting, Formulare, Karten, Videos, Analyse).

- [ ] **Datenschutzhinweise für Kunden und Lieferanten**
  bei Vertragsschluss, in AGB oder als Anlage (Art. 13).

contrust in – André Walther · Beratender Betriebswirt · Südstr. 8, 08539 Rosenbach (Vogtland) · +49 37431 86 77 35 · info@contrust-in.de · contrust-in.de

- [ ] **Hinweise für Bewerber und Beschäftigte**
  bei Bewerbung und Einstellung; Löschfrist für abgelehnte Bewerbungen festgelegt.

- [ ] **Hinweis bei Videoüberwachung**
  Schild vor dem überwachten Bereich mit Verantwortlichem und Zweck; Speicherdauer kurz.

3 3. Verträge mit Dienstleistern

- [ ] **Liste aller Auftragsverarbeiter**
  Lohnbüro, IT-Betreuung, Cloud, E-Mail, Newsletter, Website-Hosting, Aktenvernichtung, Software-Anbieter.

- [ ] **Vertrag zur Auftragsverarbeitung mit jedem**
  nach Art. 28, unterschrieben oder online akzeptiert und abgelegt.

- [ ] **Drittlandübermittlung geprüft**
  US-Anbieter nur mit Data-Privacy-Framework-Zertifizierung oder Standardvertragsklauseln.

4 4. Technik und Organisation

- [ ] **Zugriffsrechte nach Bedarf**
  Jeder sieht nur, was er für seine Aufgabe braucht; Rechte beim Ausscheiden entzogen.

- [ ] **Zwei-Faktor-Anmeldung**
  für E-Mail, Bank, Cloud, Fernzugang.

- [ ] **Backups nach 3-2-1-Regel**
  eine Kopie offline oder außer Haus; Wiederherstellung getestet.

- [ ] **Updates und Virenschutz**
  automatisch, auf allen Geräten inklusive Smartphones.

- [ ] **Verschlüsselung**
  Laptops und mobile Datenträger verschlüsselt; E-Mail-Versand sensibler Daten geschützt.

- [ ] **Papier**
  Akten verschlossen, Schreibtisch leer, Vernichtung nach DIN 66399.

- [ ] **Maßnahmen dokumentiert**
  als Liste der technischen und organisatorischen Maßnahmen (Art. 32).

5 5. Rechte der Betroffenen

- [ ] **Ablauf für Auskunftsanfragen**
  Wer antwortet, wie wird die Identität geprüft, Frist ein Monat.

- [ ] **Löschkonzept**
  Welche Daten wann gelöscht werden: Bewerbungen, Kundendaten nach Aufbewahrungsfristen, Protokolle, Backups.

- [ ] **Widerspruch und Werbung**
  Werbe-E-Mails nur mit Einwilligung oder an Bestandskunden mit Hinweis auf Widerspruch; Abmeldung in jeder Mail.

6 6. Datenpannen

- [ ] **Meldeweg im Betrieb bekannt**
  Wer erfährt es zuerst, wer entscheidet, wer meldet.

- [ ] **Meldung an die Aufsichtsbehörde binnen 72 Stunden**
  Formular der Behörde bekannt, Zuständigkeit (Sachsen: Sächsische Datenschutz- und Transparenzbeauftragte).

- [ ] **Pannen dokumentiert**
  auch die, die nicht gemeldet werden mussten, mit Begründung.

7 7. Beschäftigte

- [ ] **Verpflichtung auf Vertraulichkeit**
  unterschrieben bei Einstellung.

- [ ] **Schulung**
  mindestens jährlich, mit Teilnehmerliste; Phishing als Schwerpunkt.

- [ ] **Regeln für private Geräte, Homeoffice, Messenger, KI-Werkzeuge**
  schriftlich und bekannt gemacht.

Arbeitshilfe von contrust in – André Walther, Beratender Betriebswirt. Sie gibt den Stand zum genannten Datum wieder und ersetzt keine Rechts-, Steuer- oder Förderberatung. Die Details Ihres Falls klärt das Erstgespräch: contrust-in.de

contrust in – André Walther · Beratender Betriebswirt · Südstr. 8, 08539 Rosenbach (Vogtland) · +49 37431 86 77 35 · info@contrust-in.de · contrust-in.de