bitbase group

DSGVO-RISIKO-CHECK 2026

März 2026

DSGVO-Risiko-Check 2026

Bußgelder, Schadensersatz & Haftungsfallen – die 30-Minuten-Checkliste für KMU

bbg bitbase group GmbH

Am Heilbrunnen 47
72766 Reutlingen
mail@bitbasegroup.com

Bußgelder, Schadensersatz & Haftungsfallen
– die 30-Minuten-Checkliste für KMU

Für wen? > Geschäftsführung, IT, Datenschutz-/Compliance-Verantwortlichein KMU

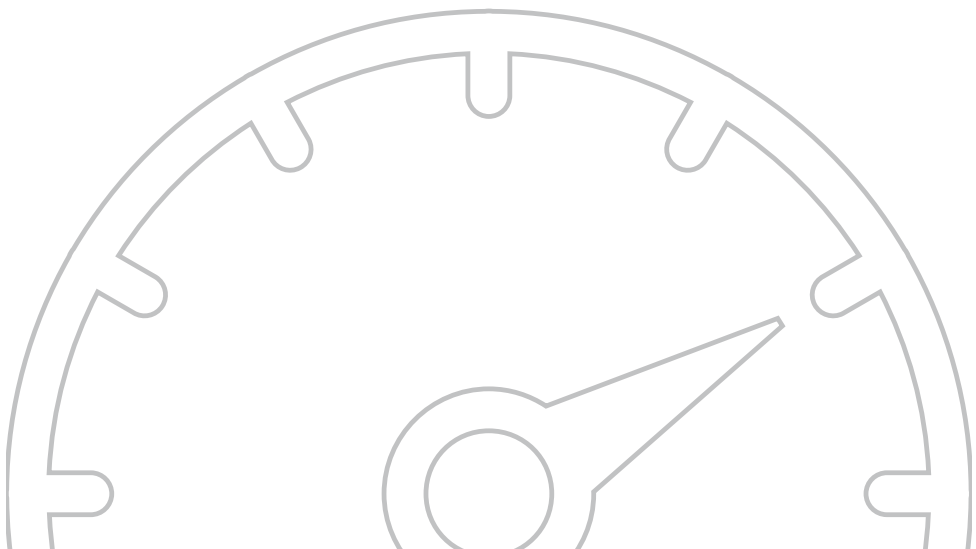
Ziel > In 30 Minuten erkennen, wo die größten DSGVO-Risiken liegen – und welche 10 Maßnahmen am schnellsten Wirkung bringen.

Warum dieses Whitepaper?

Viele KMU haben „irgendwie DSGVO" umgesetzt – aber im Ernstfall zählen nicht gute Absichten, sondern Nachweisbarkeit: klare Zuständigkeiten, funktionierende Prozesse, dokumentierte Maßnahmen. Genau daran setzen Behörden und Betroffene (Schadensersatz) an.

Was Sie am Ende in der Hand haben:

- eine kompakte Checkliste mit Ampellogik
- die 10 größten Bußgeld-/Haftungshebel in KMU



Was in der Praxis **wirklich riskant ist**

Die häufigsten „Teuerstellen“ entstehen nicht durch einen einzelnen Fehler, sondern durch Lücken im System:

01 UNKLARE VERANTWORTLICHKEITEN
(niemand “owned” den Prozess)

02 BETROFFENENRECHTE FUNKTIONIEREN NICHT
(Auskunft/Löschung dauert, ist unvollständig)

03 INCIDENT RESPONSE IST NICHT GEÜBT
(Datenpanne → Chaos → Meldefristen reißen)

04 DIENSTLEISTER/CLOUD SIND NICHT SAUBER ABGESICHERT
(Auskunft/Löschung dauert, ist unvollständig)

05 DATENÜBERMITTLUNGEN/DRITTLAND
werden unterschätzt (Support-Zugriffe, Tools, US-Bezug)

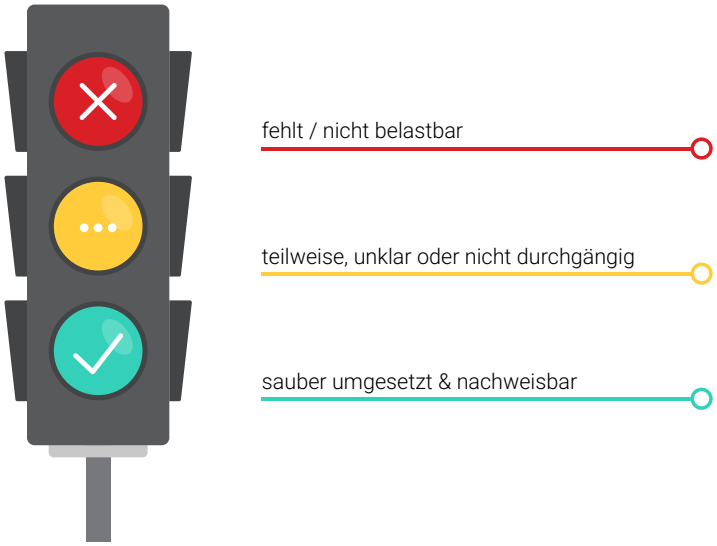
06 LÖSCHKONZEPT IST THEORIE
(Daten bleiben ewig liegen)

07 TRACKING/MARKETING
ist „wild gewachsen“ (Tags, Pixel, Consent)

Merke

„Was Sie nicht schnell erklären und belegen können, gilt im Zweifel als nicht vorhanden.“

Die 30-Minuten **DSGVO-Checkliste**



So funktioniert die Checkliste

Setzen Sie bei jeder Aussage ein Häkchen, wenn die Maßnahme vollständig umgesetzt und nachweisbar ist. Teilweise oder unklare Punkte sollten im Zweifel als nicht erfüllt gelten. Klicken Sie anschließend auf „Ergebnis anzeigen“, um Ihr aktuelles DSGVO-Risiko zu ermitteln. Die Checkliste dient der ersten Orientierung und ersetzt keine rechtliche oder individuelle fachliche Prüfung. Das Ergebnis zeigt, in welchen Bereichen vorrangig Handlungsbedarf besteht und welche Themen zuerst geprüft werden sollten.

A) Governance & Nachweis (5 Punkte)

1. Für jede Verarbeitung ist eine Zuständigkeit eindeutig festgelegt(z. B. HR, Vertrieb, Website, IT) ☐
2. Datenschutz-Aufgaben sind in Rollen/Prozessen verankert (nicht „nebenbei“) ☐
3. Verzeichnis von Verarbeitungstätigkeiten ist aktuell (letzte Pflege < 6 Monate) ☐
4. TOMs (Sicherheitsmaßnahmen) sind dokumentiert und werden überprüft ☐
5. Schulungen finden statt (inkl. Nachweis + Onboarding für neue Mitarbeitende) ☐

B) Betroffenenrechte (5 Punkte)

6. Auskunftsanfragen können innerhalb der Fristen vollständig beantwortet werden ☐
7. Identitätsprüfung ist geregelt (damit keine Daten an die falsche Person gehen) ☐
8. Lösch-/Berichtigungsanfragen sind klar geregelt (inkl. Systemen & Dienstleistern) ☐
9. Es gibt ein Ticket-/Dokumentationssystem für Anfragen (Nachweis!) ☐
10. Standardtexte existieren, aber Fälle werden individuell geprüft ☐

C) Sicherheit & Datenpannen (6 Punkte)

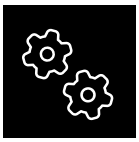
11. Es gibt einen Incident-Response-Prozess (wer tut was wann?)
12. 72-Stunden-Entscheidungslogik ist klar (Meldung ja/nein + Dokumentation)
13. MFA ist für kritische Systeme aktiv (E-Mail, Admin, Cloud, Remote)
14. Berechtigungen folgen „Need-to-know“ (kein „alle haben alles“)
15. Patch-/Update-Prozess ist geregelt und nachweisbar
16. Backups funktionieren (Restore getestet)

D) Dienstleister & Cloud (7 Punkte)

17. Für alle Dienstleister existiert ein AV-Vertrag (inkl. TOM-Anlage)
18. Subdienstleister werden geprüft/überwacht (zumindest transparent dokumentiert)
19. Offboarding ist geregelt (Zugänge weg, Daten zurück/gelöscht, Bestätigung)
20. Cloud-Adminrechte sind stark begrenzt und protokolliert
21. Datenflüsse sind dokumentiert: Wo liegen welche Daten?
22. Drittlandtransfers sind geprüft (z. B. US-Tools, Support-Zugriffe)
23. Verschlüsselung/Schlüsselmanagement ist angemessen umgesetzt

E) Website, Tracking, Marketing (5 Punkte)

24. Consent-Banner ist korrekt konfiguriert (Kategorie, Protokollierung, Widerruf)
25. Tag-/Pixel-Landschaft ist aufgeräumt (keine „Schatten-Tags“)
26. Newsletter/Leads: Double-Opt-In + Nachweis + Löschfristen
27. Datenschutzinformationen sind aktuell und passen zu den realen Tools
28. Rollen & Prozesse für Social Media/Marketing-Daten sind klar



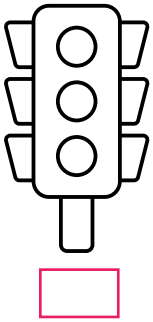
F) HR & interne Prozesse (4 Punkte)

29. Bewerberdaten: Zugriff, Fristen, Löschung funktionieren
30. Mitarbeitendendaten: klare Aufbewahrung/Archivierung, Rollen, Zugriffe
31. BYOD/Remote/Privatgeräte: Regeln + Schutzmaßnahmen
32. Zusammenarbeitstools (Teams/Slack/Drive etc.): Berechtigungen & Freigaben geregelt

0 - 20 > hohes Risiko → (Wesentliche DSGVO-Anforderungen sind nicht erfüllt. Es besteht akuter Handlungsbedarf)

21 - 28 > solide Basis → (DSGVO-Anforderungen sind weitgehend umgesetzt. Fokus auf kontinuierliche Verbesserung und Prüfung)

29 - 32 > gutes Niveau → (DSGVO-Anforderungen sind weitgehend umgesetzt. Fokus auf kontinuierliche Verbesserung und Prüfung)



Ergebnis anzeigen

Die „Top 10“ Maßnahmen mit größter Hebelwirkung

01 VERANTWORTLICHKEITEN PRO PROZESS
schriftlich festlegen (Owner-Liste)

02 BETROFFENENRECHTE-PROZESS
als Ticketflow (SLA + Standardinfos + Eskalation)

03 INCIDENT RESPONSE PLAYBOOK
(1 Seite) + 1 Trockenübung im Quartal

04 MFA ÜBERALL,
Adminrechte reduzieren, Rollen sauber trennen

05 DIENSTLEISTER-INVENTAR
+ AV-Verträge + Subdienstleister-Übersicht

06 DATENFLÜSSE VISUALISIEREN
(Mini-Datenlandkarte: Systeme, Cloud, Tools)

07 LÖSCHKONZEPT PRAGMATISCH:
5 Datenkategorien starten
(HR, Kunden, Leads, Tickets, Logs)

08 CONSENT/TRACKING AUFRÄUMEN
(Tag-Liste, Zwecke, Rechtsgrundlage)

09 PATCH-/VULN-PROZESS
fixieren (Zyklen, Verantwortliche, Nachweise)

10 SCHULUNG & AWARENESS:
Onboarding + jährlicher Refresh
+ Phishing-Mini-Training

Mini-Awareness: NIS2 & KI

NIS2 (Cybersecurity-Regeln):

Für manche Unternehmen (abhängig von Größe/Branche/Rolle in Lieferketten) steigenGovernance- und Nachweisanforderungen. Praktisch relevant: Incident-Prozesse, Schulungen, technische Mindestmaßnahmen.

KI/Automatisierung (EU AI Act):

Wenn Sie KI-Tools für HR, Scoring, Kundenservice oder Automatisierung nutzen, werden Transparenz- und Risikomanagement-Anforderungen zunehmen. Praktisch relevant: Tool-Übersicht, Datenquellen, Zweck, Verantwortlichkeit, Dokumentation.

Markus Vatter
Head of Compliance
bbg bitbase group GmbH

Zum kostenfreies Erstgespräch

bitbase group

DSGVO-RISIKO-CHECK 2026

Weiterführende Links

- Unsere Compliance-Services im Überblick
- Datenschutzberatung nach DSGVO für Unternehmen
- Fachartikel: Verarbeitungsverzeichnis in der Praxis

bbg bitbase group GmbH

Am Heilbrunnen 47
D-72766 Reutlingen

T. +49 (0) 7121 68 08 49-0
F. +49 (0) 7121 68 08 49-99
mail@bitbasegroup.com
www.bitbasegroup.com