bitbase group

VIDEOÜBERWACHUNG DATENSCHUTZKONFORM UMSETZEN

Februar 2026

Videoüberwachung datenschutzkonform umsetzen

Anforderungen verstehen. Risiken vermeiden.

bbg bitbase group GmbH

Am Heilbrunnen 47
72766 Reutlingen
mail@bitbasegroup.com

Whitepaper & 30-Minuten-Checkliste für Zulässigkeit, Schilder, Speicherfristen, Zugriff, DSFA & Dienstleister

Für wen? > Geschäftsführung, IT, Facility, HR, Datenschutzkoordination/DSB in KMU (branchenoffen)

Ziel > In 30 Minuten erkennen, ob eine geplante oder bestehende Videoüberwachung zulässig ist – und welche 10 Maßnahmen am schnellsten Risiko reduzieren.

Warum Videoüberwachung ein „Haftungshebel" ist

Videoüberwachung ist schnell installiert – aber rechtlich und organisatorisch oft komplex. Der Grund: Sie greift tief in Persönlichkeitsrechte ein. Behörden und Gerichte schauen deshalb besonders genau hin, ob die Überwachung wirklich erforderlich ist, ob sie möglichst datensparsam umgesetzt wird und ob Betroffene transparent informiert werden.

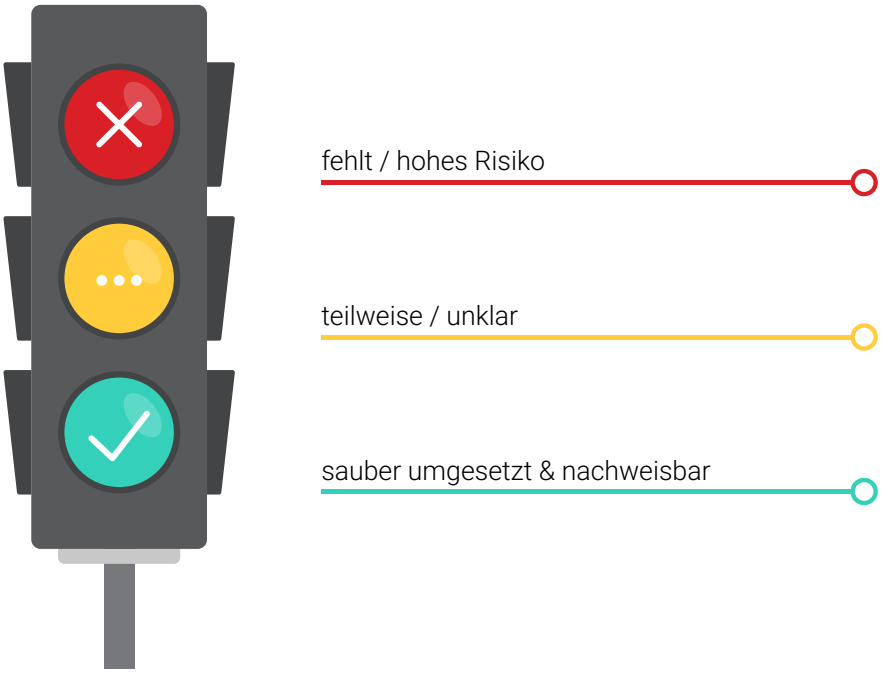
Typische Risikotreiber in KMU:

- Zweck ist zu allgemein („Sicherheit/Abschreckung") oder vermischt (Sicherheit + Leistungskontrolle)
- Kritische Bereiche werden miterfasst (Arbeitsplätze, öffentliche Flächen, Nachbargrundstücke)
- Zu lange Speicherung oder „Vorratsspeicherung"
- Fehlende oder unzureichende Beschilderung/Information
- Cloud-/Dienstleister-Lösungen ohne saubere Verträge und Transferprüfung
- „Smarte" Videoanalyse-Funktionen sind aktiv (Bewegungsanalyse, Tracking, Heatmaps)

„Wenn Zweck und Erforderlichkeit nicht glasklar sind,
ist Videoüberwachung im Zweifel unzulässig."

Praxisfolge: Erst Zulässigkeit sauber herleiten (Zweck, mildere Mittel, Abwägung) – dann Technik, Schilder, Speicherfristen.

Die 30-Minuten-**Ampelprüfung**



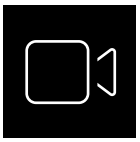
So funktioniert die Checkliste

Setzen Sie bei jeder Aussage ein Häkchen, wenn diese in Ihrem Unternehmen umgesetzt und nachweisbar ist. Klicken Sie anschließend auf „Ergebnis ansehen“, um Ihr aktuelles Risiko zu ermitteln.

A) Grundsatzprüfung: Dürfen wir überhaupt überwachen?

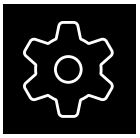
- ☐ 1. Zweck je Kamera ist eindeutig definiert
  (z. B. Diebstahlschutz, Zutrittskontrolle, Personenschutz)
- ☐ 2. Keine Zweckvermischung (insbesondere keine Leistungs-/Verhaltenskontrolle)
- ☐ 3. Rechtsgrundlage ist passend festgelegt und begründet
  (z. B. berechtigtes Interesse / Beschäftigtenkontext sauber geprüft)
- ☐ 4. Interessenabwägung ist dokumentiert: Warum erforderlich? Welche Risiken für Betroffene?
- ☐ 5. Mildere Mittel wurden geprüft
  (Zutrittskontrolle, Alarmanlage, Beleuchtung, organisatorische Maßnahmen)

Stopp-Regel: Wenn Punkte 1–5 nicht mindestens überwiegend sind: erst Grundlagen klären, bevor weiter investiert wird.



B) Bereiche & Kamerawinkel: Was wird genau erfasst?

6. Es werden keine öffentlichen Verkehrsflächen (Straße/Gehweg) erfasst ☐
7. Nachbargrundstücke/Wohnbereiche werden nicht erfasst (oder zuverlässig maskiert) ☐
8. Kameraausrichtung ist auf das notwendige Minimum reduziert ☐
(Privatzonen-Maskierung/Blenden aktiv)
9. Arbeitsplätze/Beschäftigtenbereiche werden nicht überwacht ☐
– oder es gibt einen außergewöhnlich tragfähigen Grund + klare Regelung
10. Bei sensiblen Bereichen (z. B. Umkleiden, Sanitär, Pausenräume) ☐
findet keine Überwachung statt



C) Technik & Datenminimierung (häufig „stille“ Risiken)

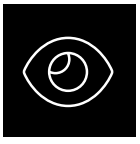
11. Audioaufzeichnung ist deaktiviert ☐
12. Zoom/Schwenk/Auto-Tracking sind deaktiviert oder strikt begrenzt ☐
13. Live-Ansicht und Aufzeichnung sind getrennt bewertet (Aufzeichnung nur, wenn erforderlich) ☐
14. Bildqualität/Zoom ist nicht höher als nötig (keine „Übererfassung“) ☐
15. Zugriff auf Kameras/Recorder ist technisch abgesichert (starke Passwörter, MFA wo möglich) ☐

Awareness KI/Videoanalyse:

16. Es ist geprüft, ob smarte Analysefunktionen aktiv sind ☐
(Zählung, Heatmaps, Objekt-/Personenerkennung, Tracking)
17. Falls ja: separate Prüfung (höheres Risiko, meist DSFA-nahe) ☐

D) Speicherung & Löschung

18. Standard-Speicherfrist ist kurz (z. B. 48–72 Stunden) ☐
19. Längere Speicherung ist konkret begründet (z. B. Wochenende, konkrete Vorfalllage) ☐
20. Vorfall-Sicherung ist geregelt: Nur relevante Sequenzen werden gesichert, ☐
Rest wird fristgerecht gelöscht
21. Löschung passiert automatisiert und nachvollziehbar ☐



E) Transparenz: Schilder & Informationen

22. Hinweisschild ist vor Betreten des überwachten Bereichs gut sichtbar ☐
23. Das Schild enthält die wichtigsten Kerninfos ☐
(Kontakt der verantwortlichen Stelle, Zweck, Kontakt)
24. Erweiterte Informationen sind leicht zugänglich (Aushang/QR-Code/Website) ☐
25. Es gibt eine klare Anlaufstelle für Betroffenenanfragen ☐

F) Zugriff & Auswertung: Wer darf was – und wann?

26. Zugriff ist auf wenige, namentlich benannte Personen beschränkt ☐
27. Zugriffe/Auswertungen werden protokolliert ☐
28. Es gibt Regeln für Herausgabe (z. B. Polizei/Versicherung) inkl. Dokumentation ☐
29. Vier-Augen-Prinzip oder Freigabeprozess ist vorgesehen ☐
30. Exporte/Weiterleitungen sind technisch und organisatorisch kontrolliert ☐

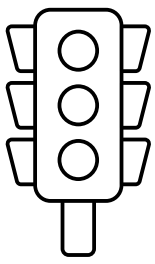
G) Dienstleister & Cloud (relevant bei vielen Kamerasystemen)

31. Externe Dienstleister/Cloud-Komponenten sind identifiziert ☐
32. Es gibt einen passenden Vertrag (inkl. Sicherheits-/Technikmaßnahmen) ☐
33. Subdienstleister/Support-Zugriffe sind transparent ☐
34. Drittlandbezüge sind geprüft (z. B. US-Cloud/Support) und dokumentiert ☐
35. Offboarding ist geregelt: Zugänge weg, Datenrückgabe/-löschung bestätigt ☐

H) DSFA & Dokumentation: Die „Behörden-Mappe“

36. Es ist geprüft, ob eine Datenschutz-Folgenabschätzung erforderlich ist ☐
37. Wenn erforderlich: DSFA ist durchgeführt, Risiken & Maßnahmen sind festgehalten ☐
38. Videoüberwachung ist im Verzeichnis der Verarbeitungstätigkeiten dokumentiert ☐
39. Interessenabwägung, technische Maßnahmen, Speicherfristen, Zugriffsregeln sind zentral abgelegt ☐
40. Regelmäßiger Review ist geplant (z. B. jährlich): Brauchen wir das noch in diesem Umfang? ☐

0 - 7	gutes Fundament, Feinschliff und Nachweise nachziehen
8 - 14	mittleres Risiko, priorisierte Maßnahmen in 60 Tagen umsetzen
ab 15	gutes Niveau → Feinschliff (Transfers, Testing, kontinuierliche Pflege)



☐

Ergebnis anzeigen

Top 10 Quick Wins

01 ZWECK JE KAMERA
auf einen Satz reduzieren und dokumentieren

02 INTERESSENABWÄGUNG
als 1–2 Seiten erstellen (inkl. Alternativen)

03 KAMERAWINKEL PRÜFEN,
Privatzonen-Maskierung aktivieren

04 AUDIO DEAKTIVIEREN,
Tracking/Zoom minimieren

05 SPEICHERDAUER
kurz einstellen (48–72h)
+ Vorfall-Sicherung definieren

06 BESCHILDERUNG
+ QR-Code-Infoseite sauber machen

07 ZUGRIFFSKONZEPT:
wenige Personen, Logging, Freigabeprozess

08 DIENSTLEISTERLISTE
aufräumen + Verträge/Sicherheitsmaßnahmen bündeln

09 DRITTLAND-/CLOUD-BEZÜGE
prüfen und dokumentieren

10 „BEHÖRDEN-MAPPE“ ANLEGEN:
Verzeichnis, Abwägung, DSFA (falls nötig),
Technik, Schilder, Prozesse

Kostenfreies Erstgespräch (20–30 Minuten)

Wir gehen Ihre Checkliste gemeinsam durch und identifizieren die 3 größten Risikohebel – inklusive konkreter Quick Wins.

Sie erhalten danach (kostenfrei):

- eine kurze Prioritätenliste (Top 5 Maßnahmen)
- eine Empfehlung, ob ein Kurz-Audit / DSFA sinnvoll ist (und in welchem Umfang)

Terminvereinbarung: Buchen Sie Ihr Erstgespräch über die Website der bitbase group oder schreiben Sie eine kurze Nachricht mit Ihrem Wunschtermin.

Markus Vatter
Head of Compliance
bbg bitbase group GmbH

Zum kostenfreien Erstgespräch

bitbase group

VIDEOÜBERWACHUNG DATENSCHUTZKONFORM UMSETZEN

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