

Whitepaper

Videoüberwachung

Orientierung für Unternehmen, Praxen und Organisationen

Inhalt

Hinweis zur Nutzung	2
1. Warum Videoüberwachung datenschutzrechtlich sensibel ist	2
2. Für wen gelten diese Vorgaben?	2
3. Zulässigkeit der Videoüberwachung (Rechtsgrundlage)	3
3.1 Mögliche Rechtsgrundlagen.....	3
3.2 Berechtigtes Interesse & Interessenabwägung	3
4. Videoüberwachung im Beschäftigungskontext.....	4
5. Typisch unzulässige Überwachungsbereiche	4
6. Pflichten bei zulässiger Videoüberwachung	4
6.1 Transparenz und Informationspflichten	4
6.2 Speicherbegrenzung	5
6.3 Technisch-organisatorische Maßnahmen	5
6.4 Dokumentationspflichten	5
6.5 Auftragsverarbeitung	6
7. Datenschutz-Folgenabschätzung (DSFA).....	6
8. Praxis-Checkliste: Ist meine Videoüberwachung DSGVO-konform?	6
9. Häufige Risiken in der Praxis	7
10. Ihr nächster sinnvoller Schritt	7
11. Über den Autor	8

Hinweis zur Nutzung

Dieses Whitepaper dient als Orientierungs- und Entscheidungshilfe zur datenschutzkonformen Planung und Durchführung von Videoüberwachung nach der Datenschutz-Grundverordnung (DSGVO). Es ersetzt keine individuelle Rechtsberatung, bietet jedoch eine fundierte und praxisnahe Grundlage für verantwortliche Entscheidungen.

Die Inhalte basieren insbesondere auf der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ der Datenschutzaufsichtsbehörden unter Federführung des Landes Baden-Württemberg sowie auf der aktuellen Verwaltungspraxis deutscher Aufsichtsbehörden.

1. Warum Videoüberwachung datenschutzrechtlich sensibel ist

Videoüberwachung greift unmittelbar in das Recht auf informationelle Selbstbestimmung ein. Bereits einfache Kameras erfassen personenbezogene Daten wie Aufenthaltsort, Verhalten, Begleitung oder Tagesabläufe betroffener Personen.

Die Datenschutzaufsichtsbehörden stellen klar: Videoüberwachung ist kein Standardinstrument, sondern nur unter engen Voraussetzungen zulässig. Insbesondere öffentlich zugängliche Bereiche unterliegen hohen Anforderungen, da betroffene Personen der Überwachung häufig nicht ausweichen können.

Zusätzlich sind die Grundprinzipien der DSGVO zu beachten, insbesondere:

- Rechtmäßigkeit, Transparenz und Zweckbindung
- Datenminimierung
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Privacy by Design und Privacy by Default (Art. 25 DSGVO)

2. Für wen gelten diese Vorgaben?

Dieses Whitepaper richtet sich an nicht-öffentliche Stellen, insbesondere:

- Unternehmen aller Rechtsformen
- Arztpraxen und Gesundheitsdienstleister

- Vereine und Verbände
- Gewerbetreibende und Freiberufler

Öffentliche Stellen (z. B. Behörden, Gerichte, Kommunalverwaltungen) unterliegen teilweise spezialgesetzlichen Regelungen und werden hier nicht vertieft behandelt.

3. Zulässigkeit der Videoüberwachung (Rechtsgrundlage)

3.1 Mögliche Rechtsgrundlagen

In der Praxis stützt sich Videoüberwachung meist auf Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse). In Einzelfällen können auch andere Rechtsgrundlagen in Betracht kommen, etwa:

- gesetzliche Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO)
- vertragliche Schutzpflichten (Art. 6 Abs. 1 lit. b DSGVO)

Die konkrete Rechtsgrundlage ist im Einzelfall zu prüfen und nachvollziehbar zu dokumentieren.

3.2 Berechtigtes Interesse & Interessenabwägung

Eine Videoüberwachung auf Grundlage berechtigter Interessen ist nur zulässig, wenn:

- ein legitimes Interesse besteht (z. B. Schutz vor Diebstahl oder Vandalismus),
- die Überwachung erforderlich ist,
- keine überwiegenden Interessen oder Grundrechte der betroffenen Personen entgegenstehen.

Eine pauschale oder anlasslose Überwachung ist regelmäßig unzulässig. Die Interessenabwägung ist vor Inbetriebnahme schriftlich zu dokumentieren und regelmäßig zu überprüfen.

4. Videoüberwachung im Beschäftigungskontext

Die Überwachung von Beschäftigten unterliegt erhöhten Anforderungen. In Deutschland ist insbesondere § 26 BDSG zu beachten.

Grundsätze:

- Keine permanente Leistungs- oder Verhaltenskontrolle
- Strenge Verhältnismäßigkeitsprüfung
- Transparente Information der Beschäftigten
- Beteiligung des Betriebsrats, sofern vorhanden

Besonders sensible Bereiche wie Pausen- und Sozialräume dürfen regelmäßig nicht überwacht werden.

5. Typisch unzulässige Überwachungsbereiche

Videoüberwachung ist regelmäßig unzulässig in:

- Toiletten, Umkleiden, Duschen, Saunen
- Arzt- und Behandlungsräumen
- Pausen- und Sozialräumen
- Bereichen privater Lebensgestaltung
- privaten Nachbargrundstücken
- verdeckter Überwachung

Auch Kameraattrappen können als Eingriff bewertet werden, wenn sie Überwachungsdruck erzeugen.

6. Pflichten bei zulässiger Videoüberwachung

6.1 Transparenz und Informationspflichten

Betroffene Personen müssen gemäß Art. 13 DSGVO vor Betreten des überwachten Bereichs informiert werden. In der Praxis hat sich ein zweistufiges Informationsmodell bewährt:

- Hinweisschild vor Ort mit den wichtigsten Informationen
- Ausführliche Datenschutzerklärung (z. B. per QR-Code oder Webseite)
- Erforderlich sind u. a.:
- Hinweis auf die Videoüberwachung
- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Rechtsgrundlage
- Speicherfrist
- Hinweise auf Betroffenenrechte

6.2 Speicherbegrenzung

Aufzeichnungen dürfen nur so kurz wie möglich gespeichert werden. In vielen Fällen akzeptieren Aufsichtsbehörden Speicherfristen von 24 bis 72 Stunden. Entscheidend ist jedoch immer eine einzelfallbezogene Begründung.

Unzulässig sind pauschale oder routinemäßig längere Speicherungen ohne nachvollziehbare Rechtfertigung.

6.3 Technisch-organisatorische Maßnahmen

Geeignete Maßnahmen umfassen insbesondere:

- Zugriffsbeschränkungen und Rollenmodelle
- Verschlüsselung
- Protokollierung von Zugriffen
- regelmäßige Überprüfung der Systeme

6.4 Dokumentationspflichten

Videoüberwachung ist im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO zu dokumentieren. Dazu gehören insbesondere:

- Zweck und Rechtsgrundlage
- Kategorien betroffener Personen
- Speicherfristen
- technische und organisatorische Maßnahmen

6.5 Auftragsverarbeitung

Werden externe Dienstleister eingesetzt (z. B. Sicherheitsfirmen, IT-Dienstleister, Cloud-Anbieter), ist ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO erforderlich. Zugriffe durch Dritte müssen klar geregelt und dokumentiert sein.

7. Datenschutz-Folgenabschätzung (DSFA)

Eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO ist erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten betroffener Personen besteht, insbesondere bei:

- großflächiger Überwachung öffentlich zugänglicher Bereiche
- systematischer Beobachtung
- Überwachung schutzbedürftiger Personengruppen

Die Blacklists der Aufsichtsbehörden sind zu berücksichtigen. Ergebnisse der DSFA sind nachvollziehbar zu dokumentieren. Bei verbleibend hohen Risiken kann eine Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO erforderlich sein.

8. Praxis-Checkliste: Ist meine Videoüberwachung DSGVO-konform?

- ☐ Zweck der Videoüberwachung klar definiert und dokumentiert
- ☐ Interessenabwägung durchgeführt und dokumentiert
- ☐ Keine Überwachung unzulässiger Bereiche
- ☐ Transparente Hinweisschilder vorhanden
- ☐ Speicherfristen festgelegt und technisch umgesetzt
- ☐ Zugriffsrechte klar geregelt
- ☐ Verarbeitung im Verzeichnis nach Art. 30 DSGVO dokumentiert
- ☐ Auftragsverarbeitungsverträge geprüft

- ☐ Mitarbeitervertretung beteiligt (falls erforderlich)
- ☐ DSFA geprüft bzw. durchgeführt
- ☐ Löschkonzept technisch umgesetzt

Wenn einzelne Punkte nicht eindeutig beantwortet werden können, besteht Handlungsbedarf.

9. Häufige Risiken in der Praxis

Typische Beanstandungen durch Aufsichtsbehörden betreffen:

- fehlende oder fehlerhafte Interessenabwägung
- zu lange Speicherfristen
- unzureichende Transparenz
- fehlende Dokumentation
- unklare Verantwortlichkeiten
- Zweckänderungen ohne Neubewertung

10. Ihr nächster sinnvoller Schritt

Videoüberwachung ist kein „Installieren und vergessen“-Thema. Eine strukturierte datenschutzrechtliche Prüfung hilft dabei:

- Risiken frühzeitig zu erkennen
- Dokumentationspflichten zu erfüllen
- Beanstandungen durch Aufsichtsbehörden zu vermeiden

11. Über den Autor

Foglia Datenschutz & Informationssicherheit unterstützt Unternehmen, Praxen und Organisationen dabei, Datenschutzanforderungen praxisnah und verhältnismäßig umzusetzen – ohne unnötige Bürokratie, aber mit der notwendigen Sorgfalt.

Sensibilisierungsschulungen zur Prävention von Cyberkriminalität (z.B. Phishing, Quishing und Social Engineering) sowie der richtige Umgang mit personenbezogenen Daten gemäß Datenschutzgrundverordnung (DSGVO), runden das Angebot ab.

Mehr Informationen über den Autor finden Sie auf der Homepage

www.foglia-datenschutz-informationssicherheit.de

oder per Kontaktaufnahme

info@foglia-datenschutz-informationssicherheit.de