

## Up to Data: Videoüberwachung und DSGVO

Jede Videoüberwachung stellt einen Eingriff in die Grundrechte der betroffenen Person – nämlich in das Recht auf informationelle Selbstbestimmung und das Recht am eigenen Bild – dar. Beide Ausprägungen gewährleistet, dass jeder einzelne selbst über die Preisgabe, die Verwendung und die Empfänger seiner personenbezogenen Daten entscheiden kann. Die Videoüberwachung ist aufgrund ihres Eingriffscharakters nur dann zulässig, wenn sie durch eine Rechtsgrundlage gestattet ist und zudem die datenschutzrechtlichen Rahmenbedingungen eingehalten werden.

### I. Arten von Videoaufzeichnungen und Speicherung

Man unterscheidet zwei Arten von Videoaufzeichnungen. Die Art und Weise der Aufzeichnung hat dann Auswirkungen auf die erlaubte Dauer der Speicherung, obwohl die DSGVO hierzu keine klaren Vorgaben trifft. Es gilt daher, dass durch Videoüberwachung aufgezeichnete und gespeicherte Daten

- Videobeobachtung oder Videostreaming:  
 Hier streamen die aufgestellten Kameras beispielsweise den Eingangsbereich eines Unternehmens live auf einen Rechner und ein Mitarbeiter verfolgt diese Live-Beobachtung direkt. Beim Streaming wird dem Verantwortlichen nur eine sehr geringe Speicherdauer ermöglicht. Diese beträgt maximal 24 Stunden. Seinen Grund findet die geringe Speicherfrist in der Tatsache, dass der beobachtende Mitarbeiter bei Auffälligkeiten jeder Zeit eingreifen kann und Straftaten wie Sachbeschädigung, Hausfriedensbruch oder den Einbruchsdiebstahl sofort erkennt und die Polizei verständigen kann. Anders ist dies bei
- der Videoaufzeichnung:  
 Hier erfolgt nämlich eine tatsächliche Überwachung insoweit, als dass die Aufnahmen vorgehalten werden und nur im Falle einer Straftat zu Strafverfolgungszwecken ausgewertet werden. Als Speicherdauer gilt hier ein Richtwert von 72 Stunden. In diesem Zeitraum sollten etwaige Straftaten erkannt worden sein, so dass die Möglichkeit zur Nachverfolgung durch die gespeicherten Aufnahmen besteht. Hiervon kann in Einzelfällen und in begründeten Ausnahmefällen abgewichen werden.

## II. Rechtsgrundlagen & Interessenabwägung

Die DSGVO ist generell als Verbot mit Erlaubnisvorbehalt ausgestaltet. Das heißt, dass grundsätzlich jede Art der Datenverarbeitung erstmal verboten ist, solange keine taugliche Rechtsgrundlage ersichtlich ist. Als Rechtsgrundlage für eine

Videoüberwachung kommt in der Regel Art. 6 Abs. 1 lit. f DSGVO in Betracht. Danach ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Allerdings ist darauf zu achten, dass die Grundrechte der betroffenen Personen nicht gegenüber den Interessen des Verantwortlichen überwiegen.

*ACHTUNG: Zudem ist § 26 BDSG dann zu berücksichtigen, wenn es sich bei den aufgenommenen Bilddaten zugleich um Beschäftigtendaten handelt. Die Videoüberwachung darf nämlich gerade nicht ausschließlich zum Zwecke einer Arbeits- und Leistungskontrolle des Arbeitnehmers vorgenommen werden.*

Trotzdem gilt: Selbst, wenn eine taugliche Rechtsgrundlage vorliegt, ist die Videoüberwachung nicht automatisch zulässig. Vielmehr ist durch eine Interessenabwägung zu ermitteln, ob die Interessen der (aufgezeichneten) betroffenen Personen nicht gegenüber dem Interesse des Verantwortlichen überwiegen können.

Im Rahmen einer solchen Abwägung sollten Sie sich – vor der Installation der Videotechnik – die nachfolgenden Fragen stellen:

- Ist die Videoüberwachung erforderlich? Dies ist dann nicht der Fall, wenn sich der mit ihr verfolgte Zweck mit weniger eingriffsintensiven Maßnahmen erreichen lässt.
- Wäre eine Überwachung an bestimmten Orten oder zu bestimmten Zeiten gleich wirksam?
- Findet die Überwachung in sensiblen Bereichen (Umkleieräumen) statt?
- Findet die Videoüberwachung ununterbrochen statt oder kann ihr der Betroffene auch ausweichen?

Wenn Sie eine dieser Fragen bejahen können, ist die Videoüberwachung nur nach besonderer Einzelfallprüfung und umfassender Guter- und Interessenabwägung erlaubt.

Gern unterstützen wir Sie bei der Abwägung!

### III. Datenschutzfolgenabschätzung (DSFA)

Da die Videoüberwachung – wie bereits erwähnt – eine sehr grundrechtsrelevante Maßnahme darstellt, können gewisse Risiken für die Betroffenen nicht gänzlich ausgeschlossen werden. Eventuell kann deshalb eine DSFA (geregelt in Art. 35 DSGVO) notwendig sein.

Eine DSFA ist nämlich immer dann durchzuführen,

- wenn die Form der Verarbeitung aufgrund der Art und des Umfangs voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat oder
- wenn öffentlich zugängliche Bereiche systematisch überwacht werden.

Für den Betrieb einer sog. „Klingelkamera“, also einer Klingel, die lediglich beim Auslösen der Türklingel aktiviert wird, ist ein DSFA nicht von Nöten.

Gern helfen wir Ihnen bei der Durchführung einer DSFA und stellen Ihnen die erforderlichen Checklisten zur Verfügung.

### IV. Hinweisbeschilderung

Bei einer zulässigen Videoüberwachung sind – für jeden Betroffenen ersichtlich – Hinweisschilder anzubringen. An diese Hinweisschilder sind bestimmte Anforderungen zu stellen. So müssen diese auf folgende Aspekte hinweisen:

- Auf die Videoüberwachung als solche und den damit verfolgten Zweck
- Auf die verantwortliche Stelle
- Auf die Speicherdauer
- Auf die Rechte der Betroffenen

Ein Beispiel für eine ordnungsgemäße Beschilderung haben wir dem Newsletter beigefügt (Piktogramm).

**ACHTUNG:** Sie müssen auch dann auf eine Videoüberwachung hinweisen, wenn Sie beispielsweise im Eingangsbereich Ihres Unternehmens lediglich Kamera-Attrappen aufhängen.

### V. Sonstiges

Beachten Sie, dass Sie – sollten Sie Videotechnik in Ihrem Unternehmen verwenden – an den Abschluss eines entsprechenden Auftragsverarbeitungsvertrages (AVV) denken und den Prozess entsprechend in Ihr Verarbeitungsverzeichnis (VVZ) aufnehmen sollten.

Sollten Sie hierzu Fragen haben, können Sie sich gern an uns wenden!

Ihr Team der RKM Data GmbH