Die Vorabkontrolle bei der Videoüberwachung

Nach § 4d Abs. 5 Bundesdatenschutzgesetz (BDSG) unterliegen automatisierte Verarbeitungen, soweit sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, vor Beginn der Verarbeitung einer Prüfung, der sogenannten Vorabkontrolle.

Notwendigkeit einer Vorabkontrolle

Nach der gesetzlichen Regelung ist eine Vorabkontrolle insbesondere dann durchzuführen, wenn

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens

Bei diesen Konstellationen handelt es sich um keine abschließende Aufzählung, d.h. die Annahme „besonderer Risiken“ nach § 4d Abs. 5 Satz 1 BDSG kann sich auch aus anderen Umständen ergeben.
Somit ist jede beabsichtigte Erhebung, Verarbeitung und Nutzung personenbezogener Daten vorweg auf ihre Vorabkontrollbedürftigkeit zu überprüfen.

Im Falle einer Videoüberwachung greift § 4 d Abs. 5 Satz 2 Nr. 2 BDSG, d.h. eine Vorabkontrolle ist durchzuführen, wenn die Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist.
Nach der Darlegung in der BT-Drs. 14/5793 liegen bei einer Videoüberwachung solche besonderen Risiken regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden.
Ebenso kann die verwendete Technik (etwa bei schwenkbaren Kameras mit hoher Auflösung der gewonnenen Bilder) zu einem solchen besonderen Risiko führen.

Eine Vorabkontrollpflicht kann jedoch entfallen, wenn einer der in § 4d Abs. 5 Satz 2 BDSG genannten Ausnahmetatbestände vorliegt, nämlich:

- im Fall einer gesetzlichen Verpflichtung zur Datenverarbeitung (hier zur Videoüberwachung)
- bei Einwilligung des Betroffenen oder
- wenn die Videoüberwachung für die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist.

Die Möglichkeit eines Wegfalls aufgrund einer Einwilligung kommt in der Praxis bei einer Videoüberwachung zumeist nicht zum Tragen, da die gesetzlichen Voraussetzungen für eine wirksame Einwilligung der Betroffenen im Sinne des § 4a BDSG aufgrund der räumlichen und geschäftsspezifischen Gegebenheiten nicht erfüllt werden können.
Auch eine arbeitgeberseitig eingeholte Einwilligung der Beschäftigten in die Überwachung ist irrelevant, da es im Beschäftigungsverhältnis an der Freiwilligkeitsvoraussetzung des § 4a Abs. 1 BDSG mangelt.

Zuständigkeit

Sofern also im Ergebnis die Erforderlichkeit einer Vorabkontrolle nach § 4d Abs. 5 BDSG zu bejahen ist, liegt die Zuständigkeit für deren Durchführung gemäß Abs. 6 beim betrieblichen Datenschutzbeauftragten.

Dies bedeutet gem. § 4f Abs. 1 S. 6 BDSG, dass in diesem Fall die für die Videoüberwachung verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten zu bestellen hat und zwar unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen.

Durchführung

Ziel einer Vorabkontrolle ist die Prüfung der formellen und materiellen Rechtmäßigkeit des Verfahrens in seiner Gesamtheit, um zu gewährleisten, dass die gesetzlichen Vorschriften zum Schutz der Betroffenen und ihr Recht auf informationelle Selbstbestimmung beachtet wurden.

Dies entspricht der gesetzlichen Aufgabe des betrieblichen Datenschutzbeauftragten aus § 4g Abs. 1 BDSG. Er ist daher auch bereits in die Prüfung, ob eine Vorabkontrolle erforderlich ist, mit einzubeziehen.

Der betriebliche Datenschutzbeauftragte hat vor Einführung einer Videoüberwachung zu prüfen, ob

- die Videoüberwachung auf Grundlage der entsprechenden Rechtsgrundlage erfolgt, d.h.
  Prüfung der materiellen Rechtmäßigkeit, hier insbes. §§ 6b, 28, 32 BDSG
- angemessene technisch-organisatorische Maßnahmen geplant wurden
  § 9 BDSG und Anlage hierzu
- gesetzliche Form-, Verfahrens- und Informationsregelungen eingehalten wurden, d.h.
  Prüfung der formellen Rechtmäßigkeit, z.B. Hinweispflicht nach § 6b Abs. 2 BDSG
- der Grundsatz der Datenvermeidung und Datensparsamkeit beachtet wurde
  § 3a BDSG
- Beachtung der Kompetenzen der Mitarbeitervertretung
  Mitbestimmungsrecht des Betriebsrats aus § 87 Abs. 1 Nr. 6 BetrVG

Dabei nimmt der betriebliche Datenschutzbeauftragte gem. § 4d Abs. 6 Satz 2 BDSG die Vorabkontrolle nach Empfang und auf Grundlage der sog. Verfahrensdokumentation (§ 4g Abs. 2 Satz 1 BDSG) vor.
Die hierin enthaltenen Angaben zur Zweckbestimmung, den betroffenen Personen und der diesbezüglichen Daten, möglicher Datenempfänger, den geplanten Speicherfristen sowie den darin vorgesehenen technisch-organisatorischen Maßnahmen kommen dabei besondere Bedeutung zu.

Hinsichtlich der Maßnahmen zur Gewährleistung der Sicherheit der Videobilddaten erfolgt die Bewertung unter Berücksichtigung der

- Gefahren für Vertraulichkeit, Integrität und Verfügbarkeit der Daten
- möglichen Folgen bei missbräuchlicher Verwendung
- eingesetzten Technik und ihrer spezifischen Risiken.

Ablauf und Methodik einer Vorabkontrolle sehen vor, dass in einer ersten Analysestufe die geplanten neuen Technologien und die Verfahrensabläufe skizziert sowie die Anwendungsdaten beschrieben werden. In der zweiten Stufe werden Schwachstellen und mögliche Bedrohungen festgestellt und bewertet, um so möglichst genaue Aussagen über die Gefahren und die daraus resultierenden Risiken zu gewinnen. Hieraus werden dann die geeigneten Sicherungsmaßnahmen abgeleitet. Eine Vorabkontrolle sollte daher – entsprechend der Orientierungshilfe der LfD („Vorabkontrolle leicht gemacht") – wie folgt gegliedert werden:

1. Systembeschreibung,
2. Rechtsgrundlage der Datenverarbeitung, d.h. der Videoüberwachung,
3. Gefahrenanalyse,
4. Risikoanalyse,
5. Datensicherungskonzept,
6. Beherrschung der Gefahren

Systembeschreibung

Hier sind Ist-Zustand und Planung darzustellen. Es kann auf die bewährten Verfahren der Systemanalyse zurückgegriffen werden. Die technisch-organisatorische Darstellung erfolgt unter Bezug auf das verfolgte Ziel.

Rechtsgrundlage der Datenverarbeitung

Die Zulässigkeit der Verarbeitung personenbezogener Daten mit Festlegung des konkret vorliegenden Zwecks der Datenverarbeitung ist zu prüfen und die gesetzliche Regelung darzustellen.

An dieser Stelle ist differenziert darzulegen, nach welcher Befugnisnorm des BDSG die Videoüberwachung in welchen Bereichen jeweils zulässig erfolgen soll.
Die Rechtsgrundlage ist jeweils konkret zu benennen und ggf. zu begründen.
Bei der Videoüberwachung gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG. Mangels Einwilligungsmöglichkeit bedarf es stets einer Erlaubnisnorm. Dies sind:
§ 6b regelt die Videoüberwachung in öffentlich zugänglichen Räumen
§ 28 bei der Überwachung von Räumen, die nicht öffentlich zugänglich sind
§ 32 Rechtsgrundlage für die Überwachung von Mitarbeitern

Die Zulässigkeitsprüfung muss hinsichtlich jeder Verarbeitungsphase erfolgen, also Erhebung, Speicherung, Übermittlung, sonstige Nutzung.

Personenbezogene Daten dürfen stets nur im erforderlichen Umfang verarbeitet werden. Die Rechte der Betroffenen (Auskunft, Berichtigung, Löschung usw.) müssen gewahrt bleiben.

Kommt die Vorabkontrolle bei diesem Prüfschritt zu dem Ergebnis, dass die Videoüberwachung nicht auf eine datenschutzrechtliche Erlaubnisnorm oder wirksame Einwilligung gestützt werden kann, so ist der Kontrollvorgang bereits an dieser Stelle abzubrechen und der betrieblichen Datenschutzbeauftragte gehalten, die verantwortliche Stelle auf die Rechtswidrigkeit der geplanten Datenverarbeitung hinzuweisen und auf ein Unterlassen hinzuwirken.

Gefahrenanalyse

Hier werden die bedrohten Objekte nach Objektgruppen gegliedert, erfasst und die Auswirkungen beschrieben. Dabei sollte der Detaillierungsgrad der Schutzbedürftigkeit des Verfahrens angepasst werden. Zusammenfassungen der Anwendungsbereiche zu Gruppen gleicher Struktur bzw. gleichen Schutzbedarfs sind aus Gründen der Übersichtlichkeit und zur Reduzierung des Analyseaufwands möglich. In der Gefahrenanalyse ist von den Grundbedrohungen „Verlust von Vertraulichkeit, Integrität und Verfügbarkeit" auszugehen.

Die möglichen Gefahren sollten hier verbal beschrieben und nach einem Wertmaßstab klassifiziert werden (z.B. Gefährdung ist „niedrig“, „mittel“ oder „hoch“). Für eine möglichst vollständige Erfassung aller Gefahren bieten sich Checklisten an.

Bedrohte Objekte könnten beispielsweise der Festplattenrekorder oder eine mögliche Wartung durch Fremdunternehmen sein. Diese Objekte (oder auch Objektgruppen) sind Grundlage einer in die verschiedenen Grundbedrohungsarten unterteilten Gefahrenanalyse.

Beispiel:
Bedrohtes Objekt: Festplattenrekorder

- Bedrohung „Verlust der Verfügbarkeit“ – mögliche Gefahren, z.B.
    - Gefährdungen durch höhere Gewalt, wie Ausfall durch Feuer-, Wasserschäden
    - Gefährdungen durch organisatorische Mängel
    - Gefährdungen durch menschliches Versagen, wie Fahrlässigkeit/Unkenntnis
        - beim Einspielen von Software mit Computerviren über Datenträger
        - bei der Bedienung und dadurch Verlust von Daten
    - Gefährdungen durch technisches Versagen
    - unsachgemäße sowie vorsätzliche Handlungen (Diebstahl, Manipulation)

Jeweils mit diesbezüglichen Angaben zur Gefährdung.

- Bedrohung „Verlust der Vertraulichkeit oder Integrität“ – mögliche Gefahren, z.B.
    - unbefugte Kenntnisnahme
    - unberechtigte Nutzung
    - unbefugte Weitergabe
    - unbefugte Aneignung von Datenträgern bei Lagerung oder Transport
    - vorsätzliche Handlungen, wie z.B. unerlaubte Bildeinstellungen.

Wiederum mit den Angaben zur Gefährdung.

Die gleiche Darstellung wäre auch für mögliche weitere bedrohte Objekte zu wählen.

<u>Risikoanalyse</u>

Hier ist die Wahrscheinlichkeit für das Eintreten eines Schadens bei den zuvor in der Gefahrenanalyse aufgeführten Gefahren darzustellen.
Das Risiko wird bestimmt durch die Wahrscheinlichkeit eines Schadenseintritts und durch das Ausmaß des Schadens.

Die Wahrscheinlichkeit für den Eintritt eines Schadens ergibt sich aus dem Missbrauchsinteresse, dem Aufwand, der notwendig ist, um einen Schaden herbeizuführen, dem Risiko, bei einem Missbrauch entdeckt zu werden, und der Verarbeitungshäufigkeit. Er kann in einzelnen Branchen oder Unternehmensbereichen sehr unterschiedlich sein.

Beispiel:
Bedrohtes Objekt: Festplattenrekorder

Bedrohung „Verlust der Vertraulichkeit oder Integrität“ durch unbefugte Kenntnisnahme

- Wahrscheinlichkeit für das Eintreten einer unbefugten Kenntnisnahme,
  Risiken können hier bestehen bei
    - Aufstellung des Festplattenrekorders in einem allgemein zugänglichen Bereich
    - Einbruchsmöglichkeit durch ein Fenster
    - Zutritt in den Raum für viele Personen
    - Fehlende Protokollierung
    - Keine schriftlichen Arbeitsanweisungen
    - Fehlender oder unzureichender Passwortschutz

Zudem ist das Ausmaß des Schadens darzulegen, welches sich aus datenschutzrechtlicher Sicht aus der Beeinträchtigung der Betroffenen ergibt.

Zur Einschätzung möglicher Risiken kann das LfD-Schutzstufenkonzept (s. Anlage) herangezogen werden.
Hinsichtlich der Schutzstufen ist bei den mittels Videoüberwachung gewonnenen Bilddaten grundsätzlich von Schutzstufe C aufwärts auszugehen.
So handelt es sich bereits bei den Daten der Kunden und Mitarbeiter um Daten, deren unsachgemäße Handhabung diese in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen könnten („Ansehen"). Im Deliktfall handelt es sich bei den Videobilddaten der potentiellen Straftäter sogar um Daten, deren unsachgemäße Handhabung diese in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnten („Existenz"), weil aus diesen ohne weiteres Straftaten feststellbar sind.
Es besteht daher ein hohes Risiko bezüglich der Vertraulichkeit.

Datensicherungskonzept

Aus der Gefahren- und Risikoanalyse ist für die zuvor benannten bedrohten Objekte dann ein Sicherheitskonzept zu entwickeln. Die zu treffenden technischen und organisatorischen Maßnahmen (s.a. § 9 S. 1 BDSG und Anlage hierzu) sind zu beschreiben und zu bewerten.

Es sind die technischen und organisatorischen Maßnahmen zu treffen, die in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch gewährleisten, wobei technische Maßnahmen organisatorischen Regelungen vorzuziehen sind.
So sind z.B. bei einer Videoüberwachung Begrenzungen von Aufnahmebereichen einer entsprechenden Organisationsanweisung vorzuziehen, wobei wiederum mechanische Begrenzungen von Aufnahmebereichen gegenüber einer softwareseitigen Verpixelung zu bevorzugen sind.

Beispiel:
Bedrohtes Objekt: Festplattenrekorder

Bedrohung „Verlust der Vertraulichkeit oder Integrität" durch unbefugte Kenntnisnahme

- ➔ Maßnahmen hiergegen
  - Unterbringung des Festplattenrekorders im verschlossenen Raum
  - dort besondere Einbruchsicherung der Fenster
  - Zutritt nur für wenige, berechtigte Personen
  - Protokollierung relevanter Aktivitäten (z.B. Zugriffe, Datenexport)
  - Erstellung einer schriftlichen Arbeitsanweisung
  - Rechteverwaltung Passwortschutz

So wird im Beispiel des bedrohten Objektes „Festplattenrekorder" dem dargestellten Verlust der Vertraulichkeit durch unbefugte Kenntnisnahme durch die o.g. Maßnahmen begegnet und dieser damit niedrig gehalten.

Bei einer Videoüberwachung bedarf es an dieser Stelle unbedingt auch einer Darstellung der organisatorischen Maßnahmen im Falle einer Weitergabe der Videobilddaten. So sollte die Weitergabe im Deliktfall an die Strafverfolgungsbehörden nur unter der Voraussetzung eines strafrechtlichen Ermittlungsverfahrens mit von der Polizei zu benennender Vorgangsnummer erfolgen sowie im Rahmen eines richterlichen Beschlusses oder eines staatsanwaltschaftlichen Auskunftsverlangens durch die zugriffsberechtigten Personen. Die Übermittlung sollte schriftlich unter Angabe des Inhalts sowie des Zeitraums der Aufzeichnung dokumentiert werden (mit Übergabeunterschrift).

Beherrschung der Gefahren – Ergebnis

Die Untersuchungsergebnisse sind schriftlich und verständlich zu dokumentieren, damit die Vorabkontrolle sowohl für die verantwortliche Stelle als auch für die kontrollierende Aufsichtsbehörde nachvollziehbar bleibt.
Daher sollte im Bericht insbesondere das Ergebnis der Überprüfung hinsichtlich der Zulässigkeit der automatisierten Verarbeitung sowie der Angemessenheit der technisch-organisatorischen Maßnahmen thematisiert werden.

Dabei sind unterschiedliche Ergebnisse möglich, sowohl ein begründetes Veto des betrieblichen Datenschutzbeauftragten als auch die uneingeschränkte Billigung der beabsichtigten Videoüberwachung.

Sofern datenschutzrechtliche Bedenken oder ein Restrisiko bestehen, sind diese zu dokumentieren, damit diese seitens der verantwortlichen Stelle ausgeräumt bzw. beseitigt werden können. Auch dieses ist anschließend zu dokumentieren.
Der betriebliche Datenschutzbeauftragte kann an dieser Stelle zudem alternative Lösungen vorschlagen.

Bei andauernden Zweifeln an der Rechtmäßigkeit des geprüften Verfahrens hat sich der betriebliche Datenschutzbeauftragte gem. § 4d Abs. 6 S. 3 BDSG an die Landesbeauftrage für den Datenschutz Niedersachsen als zuständige Aufsichtsbehörde zu wenden.

Übrigens: Allein die Durchführung einer Vorabkontrolle führt nicht automatisch zur Rechtmäßigkeit des geprüften Verfahrens!
Sie ist aber ein wesentlicher Baustein zu einem rechtskonformen Datenumgang!

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5, 30159 Hannover
Tel.: 0511 - 120 4500 / Fax: 0511 - 120 4599
eMail: poststelle@lfd.niedersachsen.de

Anlage

Schutzstufenkonzept der LfD Niedersachsen

Personenbezogene Daten sind im Hinblick auf die allgemeinen datenschutzrechtlichen Sicherungsziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie die damit einhergehenden Gebote der Datensparsamkeit, der Transparenz und der Revisionsfähigkeit vor unsachgemäßer Handhabung zu schützen.

Unsachgemäße Handhabung umfasst hierbei nicht nur Missbrauch, sondern darüber hinaus auch unzureichenden Schutz vor menschlichen Fehlhandlungen, organisatorischen Mängeln, technischem Versagen und höherer Gewalt.

Um technische und organisatorische Maßnahmen zur Sicherstellung des Rechts auf informationelle Selbstbestimmung bezüglich ihrer Angemessenheit bewerten zu können, ist es unter anderem erforderlich, das Schadenspotential (d.h. den Grad möglicher Beeinträchtigung schutzwürdiger Belange) näher zu bestimmen.

Hierzu kann das Schutzstufenkonzept der LfD Niedersachsen herangezogen werden.
Es unterscheidet folgende Schutzstufen:

Stufe	Art der personenbezogenen Daten	Beispiel
A	frei zugängliche Daten, für deren Einsichtnahme kein berechtigtes Interesse geltend gemacht werden muss.	Telefonbücher, Adressbücher, Wahlvorschlagsverzeichnisse
B	Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lassen, deren Kenntnisnahme jedoch an ein berechtigtes Interesse der Einsichtnehmenden gebunden ist.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen
C	Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen können („Ansehen”).	Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten
D	Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können („Existenz”).	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen
E	Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen können.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können

Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auch auf unmittelbar verknüpfte Datenbestände auszudehnen. Werden personenbezogene Daten unter einem Auswahlkriterium in eine Datei aufgenommen, das in der Datei nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten.

Eine Schutzstufenklassifizierung allein reicht allerdings nicht aus, um daraus direkt die erforderlichen und angemessenen technischen-organisatorischen Sicherheitsmaßnahmen abzuleiten. Soll dies erreicht werden, ist das Schadenspotential einer Gefährdung im Rahmen einer Gefahren- und Risikoanalyse gemeinsam mit deren Eintrittswahrscheinlichkeit zu bewerten. Erst hieraus lassen sich bestimmte Schutzbedarfskategorien/Risikobereiche entwickeln, für die adäquate Sicherheitsmaßnahmen definiert werden können.