Dako
dako.bei.182

Sp.
8,03

Markus Oman/Siegfried Gruber
Geschäftsführender Gesellschafter O.P.P. – Beratungsgruppe/Prokurist O.P.P. – Beratungsgruppe

Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO(Teil 2)

Umsetzung DSFA-Praxisbeispiel Videoüberwachung Der Beitrag befasst sich mit den Rahmenbedingungen und der praktikablen Umsetzung einer Datenschutz-Folgenabschätzung (DSFA) iSd Art 35 DSGVO. Im ersten Teil, erschienen in der letzten Ausgabe der Dako, wurde der Rechtsrahmen einer DSFA erläutert. Im zweiten Teil folgt nun ein Praxisbeispiel einer DSFA in Form einer Videoüberwachung, respektive einer Bildverarbeitung, wie diese nun durch das neue DSG bezeichnet wird.

DSFA am Beispiel einer Videoüberwachung

Beschreibung des Zwecks der Verarbeitung	**Aufzeichnung von Bilddaten (Video) zum Zweck des Eigentumsschutzes im Eingangsbereich des gewerblich genutzten Bürogebäudes Büroweg 1, 1000 Kleinstadt**
Was soll das Ziel der Verarbeitung sein?	Ziel der Verarbeitung ist neben der Abschreckung durch Kamera bzw entsprechendem Hinweisschild, die Möglichkeit eines allfälligen Nachweises strafrechtlich relevanten Verhaltens (Einbruch, Diebstahl, Sachbeschädigung) und der Möglichkeit der Ausforschung allfälliger Täter.
Wer ist Betroffener?	Betroffene Personen sind neben den an dieser Adresse Beschäftigten auch alle Kunden/Klienten der Gewerbeinhaber, sowie allfällige Besucher und Lieferanten. Aufgrund der an diesem Standort ebenfalls befindlichen Akutgeriatrie-Praxis (eigener Verantwortlicher), ist eine Datenverarbeitung besonderer Kategorien personenbezogener Daten nicht auszuschließen (Gesundheitsdaten).
Warum muss die Verarbeitung genauso wie beschrieben, betrieben werden?	Das Bürogebäude befindet sich am Ortsende, in dem wenig Personenverkehr (Passanten) stattfindet. In der Vergangenheit gab es in der unmittelbaren Nachbarschaft Einschleich- und Einbruchsdiebstähle sowie gefährliche Drohungen gegen Personen. Dies Vorfälle passierten zumeist zu üblichen Bürozeiten, insb die Einschleichdiebstähle. Der überwachte Bereich umfasst den Zugang zum Bürotrakt. Der Zugang ist sowohl über eine Treppe vom Büroweg 1 erreichbar, als auch über das Treppenhaus der Tiefgarage. Der Zugang zur Tiefgarage ist ohne Barriere möglich. Die Zugänge zum Bürotrakt sind vom angeschlossenen Bürohaus aus nicht einsehbar. Da die berufliche Tätigkeit der Büronutzer auch mit häufiger Reisetätigkeit verbunden ist, ist der Gesamtkomplex mitunter über längere Zeiträume (mehrere Tage bis Wochen) ungenutzt und somit unbeaufsichtigt.
Warum ist diese Art der Durch- und Ausführung das gelindeste Mittel aus der Sicht des Betroffenen?	Eine persönliche Überwachung des Zugangsbereiches durch den Eigentümer bzw durch eine von ihm beauftragten Person ist aufgrund der räumlichen Situation nicht möglich. Zudem ist eine 7x24 Stunden Überwachung erforderlich, da die potentielle Bedrohung keiner zeitlichen Einschränkung unterliegt. Aufgrund der häufigen Abwesenheit der Nutzer des Bürotrakts und der Praxis (Hausbesuche) ist eine Beweissicherung über einen längeren Zeitraum erforderlich, da ein allfällig strafrechtlich relevantes Verhalten erst nach der Rückkehr erkannt werden kann.
Beschreibung der Anwendung aus technisch-organisatorischer Sicht. Mit welchen technischen Mitteln soll das Ziel erreicht werden? Mit welchen organisatorischen Mitteln soll das Ziel erreicht werden?	Eine einzelne Videokamera ist über dem Eingang des Bürotrakts installiert und erfasst den Bereich des Zugangs, sodass alle Personen, die sich entweder über die Tiefgarage als auch über den Zugang Büroweg 1 dem Bürotrakt nähern, von der Kamera erfasst werden. Die Aufzeichnung der Kamera wird durch einen Bewegungssensor aktiviert. Die Aufzeichnung beginnt mit dem Auslösen des Bewegungssensors und endet 120 Sekunden nach der letzten vom Bewegungssensor erkannten Bewegung. Die Daten der Kamera werden über eine verschlüsselte WLAN-Verbindung an einen zentralen Server übertragen und dort für die Dauer von 72 Stunden gespeichert. Die Möglichkeit der Einsichtnahme in die gespeicherten Video-Daten besteht ausschließlich für berechtigte Benutzer nach Eingabe von Benutzername und Passwort. Derzeit ist nur der Eigentümer als Nutzer angelegt, die Zugangsdaten sind nur diesem bekannt. Die Löschung von Daten die älter als 72 Stunden sind, erfolgt automatisch durch das System aufgrund entsprechender Voreinstellungen. Sollen aufgrund eines Vorfalls Daten für einen längeren Zeitraum gespeichert werden, müssen diese vor Ablauf der 72 Stunden auf einen externen Speicherplatz kopiert werden. Auch diese Transaktion ist nur dem Eigentümer möglich.

Risikobeschreibung Risiko 1

Erkanntes Risikoszenario beschreiben (möglichst detailliert).	**Identifikation von Personen, die in keinem Zusammenhang mit dem Schutzzweck der Bildverarbeitung stehen (Patienten, Besucher etc).**
Weshalb wird angenommen, dass dieses Risiko besteht?	Die Kamera erfasst jede Bewegung und zeichnet automatisch Bilddaten auf, ohne Rücksichtnahme auf die Identität der Person und des Zwecks des Besuchs.
Unter welchen Umständen wird dieses Risiko schlagend?	Bei jeder Einsichtnahme in die aufgezeichneten Bilddaten mit und ohne konkreten Anlassfall oder durch unberechtigte Personen.
Welche Auswirkungen könnte das Risiko auf die Betroffenen haben?	Personen (insb Patienten der Praxis) können identifiziert werden. Es besteht das Risiko, dass die Tatsache offenbart wird, dass geriatrische Behandlung in Anspruch genommen wird, und damit verbunden die Gefahr einer Offenlegung bzw einer damit verbundenen Diskriminierung.
Risikomanagement durch IT & Kommunikations-Technik.	Die Speicherung der Bilddaten erfolgt auf einem Server, der Zugriff auf die Bilddaten ist nur nach Eingabe des korrekten Benutzernamens und dem Passwort möglich.

Beschreibung der Wirksamkeit der Kontrollen im Bereich IKT.	Da der technische Zugang ausschließlich durch den Eigentümer erfolgen kann, ist eine unbefugte Kenntnisnahme der verarbeiteten Daten technisch ausgeschlossen.
Risikomanagement durch angepasste und abgesicherte Organisation des Verantwortlichen.	Die Verwaltung von Benutzerkennzeichen, die Zugriff auf die Videodaten erlauben, erfolgt ausschließlich durch den Eigentümer. Die Benutzerdaten werden nicht schriftlich aufgezeichnet bzw aufbewahrt. Alle Zugriffe auf das System werden protokolliert und im Falle des Verdachts einer unberechtigten Nutzung ausgewertet. Die Mitarbeiter des Verantwortlichen werden über die Folgen einer unrechtmäßigen Nutzung bzw deren Versuch aufgeklärt.
Beschreibung der Wirksamkeit der Kontrollen im Bereich der Organisation des Verantwortlichen (zB durch ein erweitertes IKS iSd § 22 GmbHG).	Die beschriebene Maßnahme verhindert eine unberechtigte Kenntnisnahme, bzw ermöglicht die Kenntnis davon.
Risikomanagement durch Analyse des Umfelds des Verantwortlichen und Vergleich des Umfelds mit ähnlichen Verantwortlichen.	Es wurde ein Vergleich der Datensicherheitsmaßnahmen mit einem ähnlichen Objekt (Fa ABC-Compliance MC-straße 1500, 4999 Großdorf) durchgeführt. Das Risiko einer Verarbeitung von Gesundheitsdaten an diesem Standort besteht nicht. Die sonstigen Risiken und die ergriffenen Datensicherheitsmaßnahmen sind identisch.
Beschreibung der Wirksamkeit der Kontrollen im Bereich der Umfeldbewertung (zB Marktanalysen, neue Technologien, neue Judikatur).	Die eingesetzte Technologie und eine allenfalls damit verbundene weitergehende Verarbeitung personenbezogener Daten wird einer laufenden Betrachtung unterzogen. Allenfalls mögliche weitere Verarbeitungsarten führen zur Notwendigkeit einer Überarbeitung dieser DSFA.

Risikobeschreibung – Risiko 2[1]

Erkanntes Risikoszenario beschreiben (möglichst detailliert).	**Die Bilddaten werden direkt an der Kamera abgegriffen.**
Weshalb wird angenommen, dass dieses Risiko besteht?	Die Kamera überträgt die Daten mittels WLAN. Es besteht die theoretische Möglichkeit, sich in diesen Datenstrom einzuklinken und diese Daten unerkannt abzugreifen und unberechtigterweise zu speichern.
Unter welchen Umständen wird dieses Risiko schlagend?	Wenn der Datenstrom zwischen der Kamera und dem Server abgegriffen wird.
Welche Auswirkungen könnte das Risiko auf die Betroffenen haben?	Personen (insb Patienten der Praxis) können identifiziert werden. Es besteht das Risiko, dass die Tatsache offenbart wird, dass geriatrische Behandlung in Anspruch genommen wird, und damit verbunden die Gefahr einer Offenlegung bzw einer damit verbundenen Diskriminierung.
Risikomanagement durch IT & Kommunikations-Technik.	Der Datenstrom zwischen der Kamera und dem WLAN-Router erfolgt WPS-verschlüsselt unter Verwendung eines komplexen WLAN Passworts. Eine Änderung des Passworts auf der Kamera ist nur durch Verwendung einer physischen Kabelverbindung zum dahinter liegenden Netzwerk möglich. Der nächste physische Zugangspunkt zum Netzwerk befindet sich im Gebäudeinneren.
Beschreibung der Wirksamkeit der Kontrollen im Bereich IKT.	Durch die Verwendung der oben beschriebenen Maßnahmen ist eine missbräuchliche Verwendung der Netzwerkverbindung nahezu unmöglich. Zudem müsste sich der potentielle Angreifer in physischer Nähe der Kamera befinden (maximal 20 Meter). In diesen Fällen befände er sich entweder auf dem Grundstück des Bürogebäudes oder auf einer Straße ohne Parkmöglichkeit.
Risikomanagement durch angepasste und abgesicherte Organisation des Verantwortlichen.	keine
Beschreibung der Wirksamkeit der Kontrollen im Bereich der Organisation des Verantwortlichen (zB durch ein erweitertes IKS iSd § 22 GmbHG).	keine
Risikomanagement durch Analyse des Umfelds des Verantwortlichen und Vergleich des Umfelds mit ähnlichen Verantwortlichen	Es wurde ein Vergleich der Datensicherheitsmaßnahmen mit einem ähnlichen Objekt (Fa ABC-Compliance MC-straße 1500, 4999 Großdorf) durchgeführt. Das Risiko einer Verarbeitung von Gesundheitsdaten an diesem Standort besteht nicht. Die sonstigen Risiken und die ergriffenen Datensicherheitsmaßnahmen sind identisch.
Beschreibung der Wirksamkeit der Kontrollen im Bereich der Umfeldbewertung (zB Marktanalysen, neue Technologien, neue Judikatur)	Die eingesetzte Technologie und eine allenfalls damit verbundene weitergehende Verarbeitung personenbezogener Daten wird einer laufenden Betrachtung unterzogen. Allenfalls mögliche weitere Verarbeitungsarten führen zur Notwendigkeit einer Überarbeitung dieser DSFA.

[1] Diese Risiken sind exemplarisch angeführt, natürlich gibt es je nach Gegebenheit viele weitere Risiken – Querdenken ist bei einer DSFA immer notwendig!

Einschätzung bzw Beurteilung des Gesamt-Restrisikos und Ableitung einer eventuellen Notwendigkeit einer Konsultation der DSB

Geringes Restrisiko	nicht zutreffend
Akzeptables Restrisiko	Aufgrund der Möglichkeit der Verarbeitung besonderer Kategorien von personenbezogenen Daten iVm mit einer potenziellen missbräuchlichen Verarbeitung durch Dritte besteht aus der Sicht betroffener Personen ein grundsätzliches, aber geringes und daher akzeptables Restrisiko. Eine missbräuchliche Verarbeitung könnte allenfalls nur iZm hoher krimineller Energie und technischen Aufwand erfolgen, der hier nicht zu erwarten ist. Durch erweiterte technische Möglichkeiten besteht daher nur eine sehr geringe latente Gefahr, dass Daten abgegriffen bzw kopiert werden. Die Entwicklung der technischen Möglichkeiten ist laufend zu beobachten und bei Veränderungen sind zusätzliche bzw andere Datensicherheitsmaßnahmen zu ergreifen.
Hohes Restrisiko	nicht zutreffend
Restrisiko ist nicht bestimmbar	nicht zurtreffend

Schlusswort

Bei einer DSFA ist es wichtig, sehr genau und mit passenden und umfangreichen Worten den Zweck, die Verarbeitungen (Art, Form und technische Umsetzung) und die Risiken zu beschreiben. Dann sind insb die Risiken nach der Vorgehensidee der Risikobeschreibung und der Risikobegegnung zu bewerten und nach einer vollständigen fachlichen Überzeugung festzustellen, ob ein hohes Risiko für den Betroffenen besteht. In diesem Fall oder auch wenn das Risiko nicht eindeutig feststellbar ist, muss der Verantwortliche die DSB konsultieren und mit dieser im Verfahren das Thema abhandeln.

Ist das Risiko gering und schränkt daher den Betroffenen in seinen Rechten und Freiheiten nicht ein, kann die Verarbeitung durchgeführt werden. Es sollte jedoch in regelmäßigen Abständen überprüft werden (zumindest jährlich und bei größeren technischen bzw organisatorischen Änderungen), ob die Sachverhalte und Umstände, welche zu den Einschätzungen geführt haben, noch anwendbar sind.

Dako 2019/#

Zum Thema

Über die Autoren

Mag. jur. Siegfried Gruber ist Prokurist bei der O.P.P. – Beratungsgruppe.
Mag. Ing. Markus Oman, CSE, ist geschäftsführender Gesellschafter der O.P.P. – Beratungsgruppe.
Kontakt: Tel: +43 (0)699 125 180 89, E-Mail: datenschutz@opp-beratung.com
Internet: www.opp-beratung.com

Hinweis

Der erste Teil diese Beitrags behandelt den Rechtsrahmen für eine DSFA und ist in der vorherigen Ausgabe der Dako erschienen; *Oman/Gruber*, Datenschutz-Folgenabschätzung gem Art 35 DSGVO (Teil 1), Dako 2019/24.