2/2019
25 – 48

Bodycams
Kurzmeldung
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Datenschutz-Folgenabschätzung

Praxisprojekt: Datenschutz-Folgenabschätzung (Teil 1)

Markus Oman und Siegfried Gruber

Checkliste Videoüberwachung

Hans-Jürgen Pollirer

Provider haben großes Interesse daran, die Daten ihrer Kunden zu schützen

Interview mit Natalie Ségur-Cabanac und Maximilian Schubert, Internet Service Providers Austria

Kontodaten nach der DSGVO

Martin Knoll

Datenschutzrecht im HR-Alltag: Häufige Fragestellungen

Anna Mertinz

Datenschutzbeauftragte: (Un-)Zulässigkeit betrieblicher Nebentätigkeiten

Florian Stangl

Rechtsprechung: DSGVO-Pflichten im Gesundheitsbereich

Viktoria Haidinger

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

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

Datenschutz-Folgenabschätzung gem Art 35 DSGVO (Teil 1)

Notwendiges Übel oder unerlässlicher Schutz für den Betroffenen? In jedem Fall benötigt der Verantwortliche ein handhabbares Vorgehensmodell, welches auch universell einsetzbar ist. In diesem Beitrag wird der Bogen gespannt und – basierend auf den gesetzlichen Normierungen – werden praktische Prüfschritte für die Ermittlung der konkreten Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung aufgezeigt. Im zweiten Teil des Beitrags, der in der nächsten Ausgabe der Dako erscheint, wird ein praktisches Umsetzungsmodell vorgestellt.

Analyse der gesetzlichen Normierungen

Die Verarbeitung personenbezogener Daten betroffener natürlicher Personen stellt einen Eingriff in die Rechte und Freiheiten dieser Personen dar. Je nach Art der verarbeiteten Daten, aber auch durch Art und Umfang der Verarbeitung selbst können sich Risiken für die betroffenen Personen ergeben, sowohl iZm der rechtmäßigen Verarbeitung durch Verantwortliche oder Auftragsverarbeiter, aber auch durch eine allfällige rechtswidrige Verarbeitung durch unbefugte Dritte.

Art 35 Abs 1 DSGVO bestimmt für jene Fälle, in denen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, wann eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist. Ob bzw unter welchen Voraussetzungen ein hohes Risiko vorliegt, ist in der DSGVO nicht legal definiert.

Gem § 21 Abs 2 DSG hatte die österr Datenschutzbehörde im Rahmen von Ver-

ordnungen iSd Art 35 Abs 4 und 5 DSGVO zu bestimmen,

- unter welchen Umständen eine DSFA zwingend erforderlich ist (DSFA-V, auch als **Blacklist** bekannt) bzw
- unter welchen Voraussetzungen keine DSFA durchgeführt werden muss (DSFA-AV, auch als **Whitelist** bekannt).

Dieser Verpflichtung ist die Behörde durch den Erlass von zwei Verordnungen nachgekommen. Zeitgleich mit dem Ingeltungtreten der DSGVO am 25. 5. 2018 wurde im BGBl II 2018/108 die V über Ausnahmen von der DSFA (DSFA-AV) veröffentlicht. Am 9. 11. 2018 folgte die Veröffentlichung der V über Verarbeitungsvorgänge, für die eine DSFA durchzuführen ist (DSFA-V) im BGBl II 2018/278. Somit liegt der entsprechende Rechtsrahmen vor, um überprüfen zu können, ob für eine konkrete Verarbeitung personenbezogener Daten eine DSFA erforderlich ist.

Wann muss eine DSFA durchgeführt werden?[1]

Prüfschritt 1: DSFA-AV (Whitelist)

Keine DSFA ist erforderlich für Datenanwendungen, die schon vor Ingeltungtreten der DSGVO rechtmäßig durchgeführt wurden und die auch nach dem Ingeltungtreten der DSFA-AV den Vorgaben der DSGVO entsprechen, wenn diese

- **1.** gem § 18 DSG 2000 bzw § 50 c DSG 2000 der Vorabkontrolle unterlagen, soweit dafür eine Genehmigung der Datenschutzbehörde vorliegt, oder
- **2.** gem § 17 Abs 2 Z 6 DSG 2000 nicht meldepflichtig waren, da diese Anwendungen einer der in Anl 1 Standard- und Musterverordnung (StMV 2004 BGBl II 2004/312) entsprechen, oder
- **3.** einer der Datenverarbeitungen der Anl DSFA-AV entsprechen (DSFA-A01 bis DSFA-A22), wobei die DSFA-AV im Gegensatz zur StMV 2004 nur die jeweils rechtmäßigen Zwecke einer Verarbeitung beschreibt und keine konkreten Aussagen über die Inhalte der Verarbeitung trifft. Hinsichtlich der Verarbeitung von Bilddaten werden in DSFA-A09 und DSFA-A10 weitere Voraussetzungen genannt, die zur Anwendung der jeweiligen Ausnahme berechtigen.

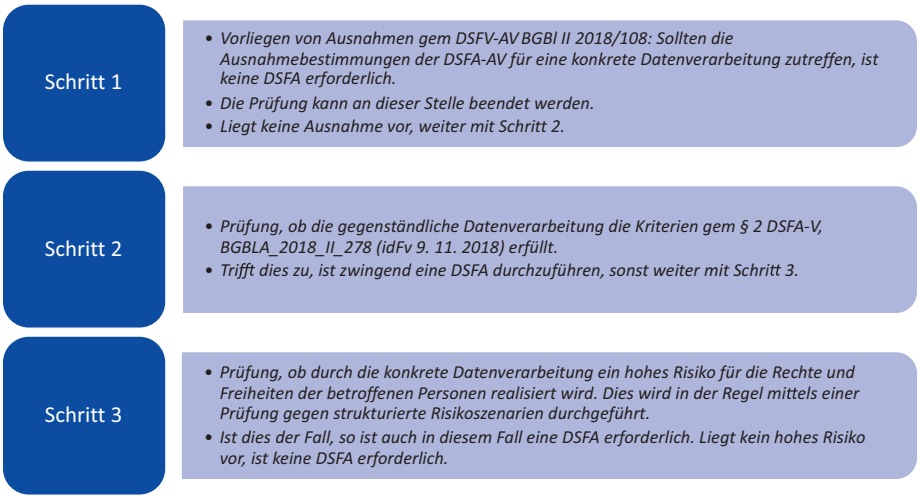

Abbildung: Prüfreihenfolge hinsichtlich konkreter Verarbeitungsvorgänge

Die Ausnahmen 1 und 2 dürfen nur in Anspruch genommen werden, wenn diese Datenverarbeitung seither keiner wesentlichen Veränderung unterzogen wurde.

Prüfschritt 2: DSFA-V (Blacklist)

Die DSFA-V beinhaltet in **§ 2 Abs 2 Kriterien**, die dazu führen, dass eine DSFA zwingend erforderlich ist. Insb handelt es sich hier um Datenverarbeitungen, die eine Bewertung, Beobachtung bzw Überwachung betroffener Personen zum Zweck haben, sowie um Verarbeitungen unter Nutzung neuartiger Technologien oder das Zusammenführen von Daten unterschiedlicher Zwecke und/oder Verantwortlicher, wenn dadurch Entscheidungen getroffen werden, die die betroffenen Personen nicht nur unwesentlich beeinträchtigen, und Verarbeitungen im höchstpersönlichen Lebensbereich der Betroffenen, auch dann, wenn diese auf einer Einwilligung beruhen.

IZm einem **Beschäftigungsverhältnis** ist keine DSFA erforderlich, wenn eine entsprechende Betriebsvereinbarung oder die Zustimmung der Personalvertretung vorliegen. Das ist kritisch zu sehen: Es scheint bedenklich, dass eine kollektive Einwilligung das Erfordernis einer umfassenden Risikobetrachtung entbehrlich machen soll.[2]

§ 2 Abs 3 DSFA-V beinhaltet **weitere Kriterien**, von denen mindestens zwei im Rahmen eines Verarbeitungsvorgangs erfüllt werden müssen, damit eine DSFA erforderlich ist. Zu diesen Kriterien zählen die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten bzw personenbezogener Daten über strafrechtliche Verurteilungen und Strafdaten, Erfassung von Standortdaten iSv § 92 Abs 3 Z 6 TKG 2003, Verarbeitung von personenbezogenen Daten schutzwürdiger betroffener Personen sowie Zusammenführung und Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen.

Prüfschritt 3: hohes Risiko

Weder die DSGVO noch das DSG bzw die darauf basierenden Verordnungen DSFA-AV und DSFA-V definieren die Begriffe „Risiko" bzw „hohes Risiko". In Art 35 Abs 3 DSGVO werden beispielhaft (arg: insbesondere) Kriterien angeführt, bei deren Vorliegen die Durchführung einer DSFA erforderlich sein soll. Diese Kriterien finden sich auch in ErwGr 91 DSGVO.

Um festzustellen, ob eine Datenverarbeitung *„wahrscheinlich ein hohes Risiko mit sich bringt"*, hat die **Art. 29-Arbeitsgruppe** am 4. 4. 2017 ein **Arbeitspapier** verabschiedet, in dem Kriterien angeführt und beispielhaft erläutert werden. Einige dieser Kriterien haben auch Eingang in die DSFA-V gefunden. Diese Kriterien sind jedoch nur beispielhaft und sind daher kein taugliches Mittel, um eine umfassende methodische Bewertung des Risikos, insb des „hohen" Risikos einer Verarbeitungstätigkeit, zu begründen.

Art 32 Abs 1 DSGVO führt hinsichtlich der Sicherheit der Verarbeitung aus, dass Maßnahmen ua unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere eines Risikos ausgewählt werden sollen (sog **„risikobasierter Ansatz"**).

[1] Alle folgenden Angaben basieren auf der Annahme, dass die jeweilige Verarbeitung der personenbezogenen Daten grundsätzlich rechtmäßig erfolgt und sowohl die Grundsätze der Datenverarbeitung (Art 5 DSGVO) sowie alle Betroffenenrechte ausreichend gewahrt werden. [2] Der letzte Abs in § 2 Abs 2 ist unklar, da nicht eindeutig festgelegt ist, ob er sich auf den gesamten § 2 Abs 2 bezieht oder nur auf jene Bereiche, in denen „Profiling" in Form einer Kontrollmaßnahme erfolgt.

Diese Risikobewertung ist Voraussetzung für das Erstellen eines vollständigen Verzeichnisses der Verarbeitungstätigkeiten (Art 30 DSGVO), da dieses gem Art 30 Abs 2 lit d leg cit eine allgemeine Beschreibung der aus dieser Risikobetrachtung abgeleiteten und gem Art 24 Abs 1 leg cit ergriffenen Datensicherheitsmaßnahmen zu enthalten hat. Die entsprechenden Kriterien der Risikobeurteilung hinsichtlich Eintrittswahrscheinlichkeit bzw Auswirkung (Schwere) müssen schon an dieser Stelle vorliegen. Ebenso sollten an dieser Stelle die Schwellenwerte definiert werden, die ein „hohes" Risiko manifestieren.

PRAXISTIPP

Um nun vorab eine Risikobewertung durchführen zu können, müssen einerseits Risiken bzw Risikoszenarien festgelegt und andererseits ein Bewertungssystem verwendet werden, wodurch Risiken (allenfalls subjektiv) bewertet werden können und diese Bewertung für Dritte einfach nachvollziehbar ist.

Risikotypen

Wichtig ist, dass man Risiken definiert, die die tatsächliche Verarbeitungslandschaft widerspiegeln und auch im Optimalfall für alle Bereiche der Organisation anwendbar sind.

ErwGr 75 bietet hier eine demonstrative Auflistung potentieller Risiken, die durch zusätzliche konkrete Risiken von Verarbeitungsvorgängen aus der Sicht der betroffenen Personen ergänzt werden müssen.

Risiken sollen die tatsächliche Verarbeitung in einem Unternehmen widerspiegeln.

Diese Auflistung beinhaltet insb:

- physischen, materiellen oder immateriellen Schaden;
- Diskriminierung;
- Identitätsdiebstahl oder -betrug;
- finanziellen Verlust;
- Rufschädigung;
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten;
- unbefugte Aufhebung der Pseudonymisierung;
- erhebliche wirtschaftliche oder gesellschaftliche Nachteile;
- wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren;
- wenn besondere Kategorien personenbezogene Daten oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden;
- wenn persönliche Aspekte bewertet, analysiert oder prognostiziert werden (Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, Aufenthaltsort oder Ortswechsel);
- Erstellung und Nutzung persönlicher Profile;
- Verarbeitung personenbezogener Daten schutzbedürftiger natürlicher Personen;
- Verarbeitung einer großen Menge personenbezogener Daten bzw Daten von einer große Anzahl betroffener Personen.

Beispiel einer durchgängigen Risikobewertung

Wir haben uns im zweiten Teil dieses Beitrags für die Betrachtung des Risikos einer Videoüberwachung iSe Bildverarbeitung gem § 12 DSG entschieden. Jedoch ist die Vorgehensweise für alle Arten von Risiken eines jeden Verfahrens anwendbar.

Aus Verfahrenssicht könnte eine Risikobetrachtung wie folgt durchgeführt werden:

Grundsätzlich betrachten wir 3 Stufen:

1. Stufe – Prüfung, ob eine Ausnahme gemäß DSFA-AV vorliegt;

2. Stufe – kommen in der Verarbeitung Sachverhalte gem DSFA-V bzw gem Whitepaper 248 der WP 29 zur Anwendung;

3. Stufe – eine individuelle Risikoanalyse (wir wenden hierfür ein Modell mit 22 typischen Risiken an).

Man beginnt daher mit Stufe 1 und soweit eine Genehmigung nach § 18 Abs 2 DSG 2000 vorliegt, ist dies zu beachten.

- Liegt eine Ausnahme gem DSFA-AV vor (dann ist keine DSFA erforderlich) weiters sollte nun eine strukturierte Risikobewertung vorgenommen werden (siehe Details hierzu weiter unten bei Punkt „Bewertung der 22 Risiken"
- Liegen Verarbeitungen vor, die gem DSFA-V bzw Whitepaper der WP 29 ein erhöhtes Risiko beinhalten, dann ist immer eine DSFA erforderlich, außer für spezifische Punkte des Whitepaper 248 der WP 29[3] der Stufe 2, hier kann ein vermutetes Risiko über die Stufe 3 detailliert geprüft werden.
- Liegen generell erhöhte Risiken vor, dann ist eine DSFA erforderlich (es sollten zur Vorbereitung der DSFA auch die Risiken der Stufe 3 geprüft werden).
- Wenn keine DSFA erforderlich ist, dann müssen die in Stufe 3 benannten Datensicherheitsmaßnahmen, zusätzlich zu den bestehenden TOM (Technisch Organisatorische Maßnahmen), ergriffen werden, um den Risiken der Stufe 3 zu begegnen.

Folgende Risiken in Stufe 3 sollten betrachtet werden (diese Liste ist exemplarisch und kann natürlich je nach Notwendigkeit angepasst werden):

- 1. Gefahr für Leib und Leben
- 2. wirtschaftlicher Nachteil
- 3. Diskriminierung der betroffenen Person
- 4. Identitätsdiebstahl
- 5. Identitätsbetrug
- 6. Verlust der Kontrolle über Daten
- 7. Verlust der Vertraulichkeit von Berufsgeheimnissen
- 8. Verlust der Vertraulichkeit von Geschäftsgeheimnissen
- 9. Aufhebung der Pseudonymisierung
- 10. unrechtmäßige Verarbeitung besonderer Kategorien von Daten
- 11. unrechtmäßige Verarbeitung strafrechtlicher Daten
- 12. Erstellung und Nutzung persönlicher Profile
- 13. Analyse und Prognose der Arbeitsleistung
- 14. Analyse und Prognose der wirtschaftlichen Lage
- 15. Analyse und Prognose der Gesundheit
- 16. Analyse und Prognose der persönlichen Vorlieben und Interessen
- 17. Analyse und Prognose der Zuverlässigkeit
- 18. Analyse oder Prognose des Verhaltens

[3] Spezifische Punkte des Whitepaper 248 der WP 29 sind aus unserer Sicht: vertrauliche Daten oder höchstpersönliche Daten; Datenverarbeitung in großem Umfang; Daten zu schutzbedürftigen Betroffenen; innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen; die Verarbeitung hindert an sich *„die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw Durchführung eines Vertrags"*.

- 19. Analyse oder Prognose des Aufenthaltsorts oder Ortswechsels
- 20. Verarbeitung von Daten schutzbedürftiger Personen (zB Kinder)
- 21. Verarbeitung großer Mengen personenbezogener Daten
- 22. Verarbeitung von Daten über eine große Anzahl betroffener Personen

Bewertung dieser 22 Risiken (Beispiel)

In der Praxis haben sich Bewertungssysteme bewährt, nach denen sowohl für die Eintrittswahrscheinlichkeit als auch für die Auswirkungen Kategorien definiert werden und anhand dieser Kategorien eine Risikokennzahl errechnet wird. Hinsichtlich der Kategorien der Auswirkung hat sich die Verwendung subjektiver Bewertungskriterien gegenüber objektiven (in Zahlen ausgedrückten) Werten bewährt.

Beispiele für **Kategorie Eintrittswahrscheinlichkeit**

- 0 = unmöglich
- 1 = < 1 x / Jahr
- 2 = < 10 x / Jahr
- 3 = >= 10 x / Jahr

Beispiele **für Kategorien Auswirkung**

- 0 = keine Auswirkung
- 1 = sehr geringe Auswirkung
- 2 = geringe bis mittlere Auswirkung
- 3 = hohe Auswirkung

Die Bewertung ergibt sich aus einer Kombination der Eintrittswahrscheinlichkeit mit der Auswirkung eines Risikos.

Die **Risikokennzahl** ist das Ergebnis der Multiplikation des Werts der Kategorie für die Eintrittswahrscheinlichkeit multipliziert mit dem Wert der Kategorie für die Auswirkung.

Soweit nach dieser Methode eine Risikokennzahl >= 6 errechnet wird, liegt hohes Risiko vor und es ist eine DSFA durchzuführen.

Wie schon erwähnt behandeln wir im zweiten Teil dieses Beitrags als DSFA-Beispiel eine Bildverarbeitung. Es werden also beim Risiko einer Bildverarbeitung alle Kameras zusammengefasst, die interne Aufnahmen bzw externe Aufnahmen am Gelände zeigen und grundsätzlich nur in einzelnen Bereichen erhöhte Risiken für die Betroffenen erkennen lassen. Die Videoüberwachung ist zur Verwirklichung des Überwachungszwecks (Eigentumsschutz und Schutz vor Gefährdung von Personen) das gelindeste Mittel.

Wir betrachten hier insb die Risiken 6, 20, 21, 22 (es sollten eventuell nach jeweiligem Erfordernis und Situation auch weitere Risiken betrachtet werden).

- Verlust der Kontrolle über Daten: Um das inhärente Risiko aus Auswirkung und Eintrittswahrscheinlichkeit zu minimieren, könnten zB Maßnahmen ergriffen werden wie Zugriffskontrolle, Zutrittskontrolle. Schulungen/Belehrungen
- Verarbeitung großer Datenmengen bzw Daten von vielen Personen (auch Kindern): Um das inhärente Risiko aus Auswirkung und Eintrittswahrscheinlichkeit zu minimieren, könnten zB Maßnahmen ergriffen werden wie Zugriffskontrolle, Zutrittskontrolle, zeitliche Einschränkung der Verarbeitung, insb zeitliche Beschränkung (dzt 72 h), können eine signifikante Verringerung des Risikos erreichen.

Zur Vollständigkeit sei noch erwähnt, dass folgende Maßnahmen (nicht zwingend abschließende Liste) als sinnvoll bei der Reduzierung der angeführten 22 Risiken erscheinen:

- gut ausgearbeitetes Backup-/Recovery-Konzept
- Identitätskontrolle
- Notfallplan
- Protokollierungen
- Rollenkonzept
- Schulung/Belehrungen/Dienstanweisung
- Schutz vor Eingabefehlern
- Schutz vor Malware
- spezielle Berechtigungen
- technische Sicherheitsmaßnahmen der IT
- Verschlüsselung (Data at Rest)
- Verschlüsselung (Data in Motion)
- Vorgehensbeschreibung
- zeitliche Einschränkung der Verarbeitung
- Zugriffskontrolle
- Zutrittskontrolle
- Zuweisung von Schlüsseln iZm Pseudonymisierung

Dako 2019/24

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

Im nächsten Heft der Dako (2019/3) finden Sie die Fortsetzung des Beitrags mit einem praktischen Beispiel zur Bildverarbeitung einer Datenschutz-Folgenabschätzung.