Datenschutzrisiken richtig abschätzen

DATENSCHUTZVORSORGE *Beim Verarbeiten personenbezogener Daten können hohe Risiken für die Rechte und Freiheiten der Betroffenen entstehen. Dann müssen vorher die Folgen abgeschätzt werden. Personalräte sind dabei frühzeitig einzubeziehen.*

VON **EBERHARD KIESCHE**

Ab 25.5.2018 ist es soweit: Die Datenschutz-Grundverordnung (nachfolgend DS-GVO) gilt unmittelbar. Zeitgleich tritt das BDSG n.F. in Kraft, das das Datenschutzrecht auch für den öffentlichen Bereich des Bundes regelt. In den Bundesländern treten die bisherigen Datenschutzgesetze außer Kraft. In einigen Ländern, wie zum Beispiel Sachsen, Hessen und Hamburg liegen Entwürfe für ein neues Datenschutzgesetz vor. Neu ist die Pflicht zur Datenschutzfolgenabschätzung (nachfolgend DSFA) nach Art. 35 DS-GVO. Das wirkt sich auf die Arbeit der Personalräte im Bund und in Ländern aus. Sie sollten die Neuerungen kennen. Jetzt wird aktive Datenschutzvorsorge von Dienststellen und Personalräten verlangt. Die DSFA gemäß Art. 35 DS-GVO ersetzt die Vorabkontrolle in § 4d Abs. 5 BDSG a. F. Mit der Vorabkontrolle ist sie nur bedingt vergleichbar. Von der Vorabkontrolle gewohnte Ausnahmen entfallen. Die DSFA beinhaltet umfangreichere Pflichten. In der DSFA geht es um den gesamten Lebenszyklus einer Datenverarbeitung.

Ziele der DSFA

Ziel der DSFA ist es, Kriterien des Grundrechtsschutzes anzuwenden, die Folgen von geplanten Datenverarbeitungen zu erfassen sowie objektiv im finalen Bericht zu bewerten. Angemessene Schutzmaßnahmen sind zu entwickeln und umzusetzen.[1] Die DSFA soll bei Datenverarbeitungen mit einem voraussichtlich hohen Risiko vorab klären, inwieweit Risiken für Rechte und Freiheiten natürlicher Personen vermieden werden können. Hierfür sind geeignete Maßnahmen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren zu definieren. Sie müssen auf ihre Wirksamkeit getestet werden. Der Dienststellenleiter als Verantwortlicher (Art. 4 Nr. 7 DS-GVO) muss die DSFA dokumentieren, um die Nachweispflicht gemäß Art. 5 Abs. 2 DS-GVO zu erfüllen.[2]

Die DSFA soll klären, inwieweit die geplante Datenverarbeitung mit der DS-GVO insgesamt übereinstimmt. Zu untersuchen ist, inwieweit die Verarbeitung sich auf das Recht auf Privatleben und den Schutz der personenbezogenen Daten (Erwägungsgrund – ErwGr – 4 DS-GVO; Art. 7, 8 GRCh – EU-Grundrechtecharta) auswirkt. Die Grundrechte der

PRAXISTIPP

Unbestimmte Rechtsbegriffe

Art. 35 DS-GVO enthält unbestimmte Rechtsbegriffe. Hierzu gehören unter anderem »umfangreiche und systematische Überwachung« von Personen, »systematische und umfassende« Bewertung persönlicher Aspekte und »umfangreiche Verarbeitung« sensibler Daten. Hier können Personalräte beispielsweise auf Kommentare zur DS-GVO und Stellungnahmen der Aufsichtsbehörden zurückgreifen.[3]

DARUM GEHT ES

1. Bevor personenbezogene Daten verarbeitet werden, sind die dadurch entstehenden Risiken abzuschätzen.

2. Das obliegt der Dienststelle, die den behördlichen Datenschutzbeauftragten einbeziehen muss.

3. Wenn es um die Daten von Beschäftigten geht, ist auch der Personalrat zu beteiligen.

1 Friedewald u.a., White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz, S. 5; Kiesche, CuA 2/2017, 31.

2 Zur Rechenschafts- bzw. Nachweispflicht siehe GDD (Hrsg.), GDD-Praxishilfe DS-GVO IX Accountability.

3 Hierzu Kiesche, CuA 10/2017, 31; Kiesche/Wilke, CuA 12/2017, 34.

WP29-GRUPPE

Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission zu Fragen des Datenschutzes. Die Gruppe wurde aufgrund von Artikel 29 der Richtlinie 95/46/EG (Datenschutzrichtlinie) vom 24.10.1995 eingesetzt. Ihre amtliche Bezeichnung ist: Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten. Ab 25.5.2018 ist die neue Bezeichnung der WP29-Gruppe »Europäischer Datenschutzausschuss« (Art. 68 ff. DS-GVO).

betroffenen Personen sollen geschützt werden. Das erfordert ein Umdenken in den Dienststellen.[4] Unabdingbar für die DSFA ist das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO.

Adressaten der DSFA

Die DSFA ist Ausdruck des risikobasierten Ansatzes in der DS-GVO.[5] Ihr Ziel ist Risikominimierung oder -vermeidung durch ein Frühwarnsystem. Sie ist Aufgabe des Verantwortlichen, hier des Dienststellenleiters. Mit dem Verantwortlichen ist nach Art. 4 Nr. 7 DS-GVO die jeweilige natürliche oder juristische Person gemeint, die über Zweck und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Er kann sich zur Durchführung der DSFA externer Dienstleister und Experten bedienen. Der Verantwortliche hat bei der DSFA gemäß Art. 35 Abs. 2 DS-GVO den Rat des betrieblichen Datenschutzbeauftragten zu suchen. Lässt er sich nicht beraten, ist dies nach Art. 83 Abs. 4 DS-GVO bußgeldbewehrt. Wenn er dem Rat nicht folgt, so hat er dies zu dokumentieren. Der Datenschutzbeauftragte soll nach Art. 35 Abs. 2, Art. 39 Abs. 1 lit. c DS-GVO auf Anfrage helfen und beraten, jedoch nicht die DSFA durchführen. Sie obliegt der jeweiligen Fachabteilung, die die Daten verarbeiten will.

Bei einer Auftragsverarbeitung gemäß Art. 28 ff. DS-GVO ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen bei der DSFA zu unterstützen (Art. 28 Abs. 3 S. 2 lit f. DS-GVO). Er hat ihn zu unterstützen und zum Beispiel bei den technisch-organisatorischen Maßnahmen zu beraten.

Risiken im Beschäftigtendatenschutz

Art. 35 DS-GVO zur DSFA und die Erwägungsgründe (ErwGr 75, 84, 89–93) katalogisieren Risiken, etwa

- Diskriminierung,
- Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung,
- unbefugte Aufhebung der Pseudonymisierung,
- Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen und
- Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von personenbezogenen Daten bzw. der unbefugte Zugang zu ihnen.

Für Personalräte ist diese Aufzählung noch zu allgemein. Bei der Einführung von Verarbeitungen mit personenbezogenen Daten der Beschäftigten sind die im folgenden Infokasten genannten Risiken zu überprüfen und bestimmte Kriterien zu beachten. Die WP29-Gruppe gibt[6] als Faustregel an, dass eine DSFA regelmäßig durchzuführen ist, wenn mindestens zwei der Kriterien erfüllt sind. Das wird im Beschäftigtendatenschutz regelmäßig der Fall sein.

ÜBERBLICK

Risiken und Kriterien

Beim Einführen von Verarbeitungen mit personenbezogenen Daten der Beschäftigten sind die folgenden Risiken und Kriterien zu überprüfen:

- Einsatz von Profiling- oder Scoring-Verfahren
- automatisierte Entscheidungen mit erheblichen Rechtsfolgen (Art. 22 DS-GVO)
- systematische Überwachung, zum Beispiel Videoüberwachung
- Verarbeitung sensibler Daten, zum Beispiel Gesundheitsdaten
- Verarbeitung von Daten in großem Umfang, zum Beispiel Menge der Daten
- Abgleich oder Kombination von Datenbeständen (ErwGr. 91)
- Machtungleichgewicht, schutzwürdige Person (ErwGr. 75)
- grenzüberschreitender Datentransfer außerhalb der EU und des EWR
- Einsatz neuer Technologien oder biometrischer Verfahren (ErwGr. 89, 91)

Zeitpunkt der DSFA

Eine Risikoanalyse für die Datensicherheit ist für jede geplante Datenverarbeitung nach Art. 24, 25 und 32 DS-GVO stets erforderlich. Es muss weiter geprüft werden, ob eine umfassendere DSFA zwingend erforderlich ist. Die Entscheidung des Verantwortlichen muss dokumentiert werden, damit sie von der Aufsichtsbehörde gegebenenfalls überprüft wer-

4 Hansen, DuD 2016, 587.
5 Siehe unter anderem Art. 39 Abs. 2 DS-GVO.
6 Artikel-29-Datenschutzgruppe, WP 248 – »Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679« v. 4.4.2017, S. 7 – 9.

den kann. Es ist vorab zu bewerten, ob die geplante Datenverarbeitung voraussichtlich ein »hohes Risiko« (Art. 35 Abs. 1, 3 DS-GVO) für die betroffenen Beschäftigten mit sich bringt. Der Verantwortliche hat mit seiner Risikobewertung mögliche Datenschutzfolgen zu operationalisieren. Er muss eine Prognose abgeben, die von der Datenschutzaufsichtsbehörde und gegebenenfalls vom Gericht überprüft werden kann. Er hat Faktoren zu bewerten, wie zum Beispiel die Verwendung neuer Technologien, Art der Verarbeitung, Umfang (Volumen), Umstände (Verwendung, Zugriffe), Eintrittswahrscheinlichkeit des Risikos, Zwecke der Verarbeitung und Schwere des möglichen Schadens (ErwGr. 76). Führt er keine DSFA durch, so hat er das zu dokumentieren.

Die Aufsichtsbehörden sollen nach Art. 35 Abs. 4 DS-GVO eine Positiv-Liste (Blacklist) mit Verarbeitungen erstellen, für die eine DSFA zu erstellen ist. Ob sie auch eine Negativ-Liste (Whitelist) nach Art. 35 Abs. 5 mit Datenverarbeitungen anfertigen, die keine DSFA erfordern, bleibt abzuwarten. Ein Beispiel wäre die Lohnbuchhaltung. Verantwortliche sollten sich auf die Positiv-Liste nicht verlassen, wenn die geplante Verarbeitung nicht gelistet ist. Eine solche Positiv-Liste kann nie abschließend sein.

Art. 35 Abs. 1 Satz 2 DS-GVO erlaubt eine DSFA für die Untersuchung von ähnlichen Verarbeitungsvorgängen mit ähnlich hohen Risiken. Das kann der Fall sein, wenn mehrere Verantwortliche gemeinsame Anwendungen oder Verarbeitungsumgebungen einführen wollen (ErwGr 92).

Regelbeispiele für eine DSFA

In Art. 35 Abs. 3 DS-GVO und den Erwägungsgründen werden Anwendungsfälle benannt. Aus Sicht der Beschäftigten sind unter anderem relevant:

- neuartige Verarbeitungen bzw. Anwendungen
- automatisierte Entscheidungen mit rechtswirksamen Folgen und Beeinträchtigungen, so u.a. Persönlichkeitstests, Online-Bewerberverfahren
- innovativer Einsatz neuer Technologien und systematische Überwachung, unter anderem Gesichts- und Spracherkennung, Videoüberwachung am Arbeitsplatz
- Verlagerung der Personaldatenverarbeitung zu einem Cloud-Anbieter
- Körperdatenverarbeitung mit Wearables
- Sensibilität von persönlichen Aspekten (Art. 9, 10 DS-GVO), etwa Gesundheitsdaten, Führungszeugnisse, biometrische Daten und
- interne Ermittlungen und Compliancemaßnahmen.

Datenschutz-Management-System

Mit der DSFA ist ein Datenschutz-Management-System einzuführen und regelmäßig zu überprüfen. Das folgt unter anderem aus Art. 35 Abs. 11 DS-GVO. Danach ist die Datenverarbeitung bzw. die DSFA im Regelbetrieb regelmäßig zu überprüfen, anlasslos jährlich[7] und sonst bei Anlässen. Dies können veränderte Rahmenbedingungen und Risiken, aktualisierte Software, Datenschutzverletzungen (Art. 33, 34 DS-GVO) oder geänderte Verarbeitungstätigkeiten sein. Die DSFA ist somit ein iterativer Prozess (siehe Schaubild Seite 28).

Inhalte einer DSFA

Nach Art. 35 Abs. 7 DS-GVO (ErwGr. 84, 90) sind folgende Bestandteile einer angemessenen DSFA zu berücksichtigen und in einem DSFA-Bericht aufzunehmen:

- Systematische Beschreibung des geplanten Vorhabens (Prüfgegenstand),
- berechtigte Zwecke, Interessen- und Grundrechtsabwägung,
- Schutz- und Gewährleistungsziele[8] und Risikoanalyse,
- Bewertung der Erforderlichkeit, Datenminimierung und Einhaltung der Zweckbindung,
- Nachweis über Einhaltung der DS-GVO insgesamt und
- nachvollziehbare Dokumentation der Schutzmaßnahmen (Art. 32 DS-GVO) und Wirksamkeitsüberprüfungen.

Der Bericht sollte vollständig oder zumindest teilweise veröffentlicht werden. Wenn es dabei um Beschäftigtendaten geht, ist der Bericht dem Personalrat vorzulegen. Das ergibt sich aus § 68 Abs. 2 BPersVG und den vergleichbaren Vorschriften der Landespersonalvertretungsgesetze. Danach ist der Personalrat rechtzeitig und umfassend zur Durchführung

7 GDD (Hrsg.), a.a.O., 9. WP 248, a.a.O., alle drei Jahre, S. 12.
8 Zum Standard-Datenschutzmodell (SDM) der Datenschutzkonferenz v. 9. und 10.11.2016, V.1.0. https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

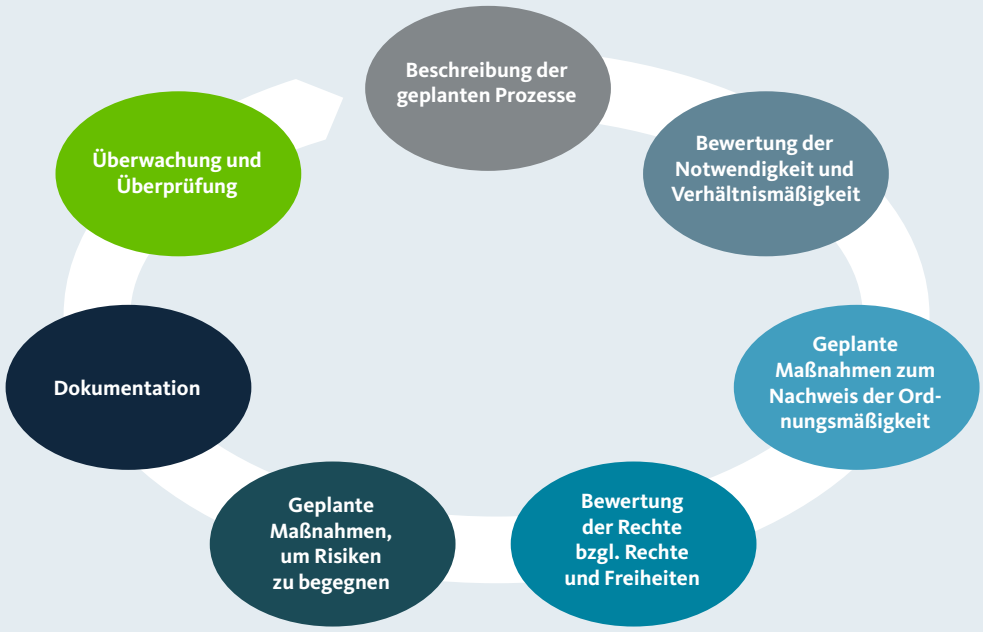
GUT ZU WISSEN

Datenschutzfolgenabschätzung erst ab 25.5.2018

Die DSFA betrifft neue Verarbeitungen ab dem 25.5.2018. Bei Altverfahren besteht eine Empfehlung zur Durchführung einer DSFA wohl dann, wenn es in der Verarbeitung signifikante Änderungen der Rahmenbedingungen gibt, neue Technologien verwendet werden und es bislang keine Vorabkontrolle gegeben hat, wenn Sicherheitslücken sich offenbaren und neue Risiken entstanden sind.

SCHAUBILD

Wiederholender Prozess der Datenschutzfolgenabschätzung



Quelle: WPA 248, Seite 14.

seiner Ausgaben zu unterrichten. Die hierfür erforderlichen Unterlagen sind vorzulegen.

DSFA als kontinuierlicher Prozess

Die DSFA ist als standardisierter Prozess mit Zeitplanung, Dokumentation und Meilensteinen zu organisieren.[9] Die Verantwortlichen können unterschiedliche Methoden einsetzen.[10] Die genutzten Kriterien zur Bewertung der Risiken und Schutzmaßnahmen sollten einheitlich sein.[11] Zu jeder geplanten Datenverarbeitung sollte zumindest in mittleren und größeren Behörden ein Team mit interdisziplinärer Kompetenz eingerichtet werden, geleitet von der zuständigen Fachbereichs- oder Projektleitung.

Beteiligung der Personalräte

Die DS-GVO sieht in Art. 35 Abs. 9 zwar kein neues Mitbestimmungsrecht für Personalräte vor. Aber der Verantwortliche hat gegebenenfalls den Standpunkt der betroffenen Personen bzw. ihrer Vertreter einzuholen. Soweit Beschäftigtendaten betroffen sind, ist dem Verantwortlichen die Anhörung der Personalräte als risikominimierende Maßnahme generell anzuraten (Art. 22 Abs. 3 DS-GVO und ErwGr 71). Die Vorschrift dient unter anderem dazu, Transparenz bei den betroffenen Personen zu schaffen (Art. 5 Abs. 1 lit. a DS-GVO). Beteiligt der Verantwortliche die Personalräte nicht bzw. folgt nicht ihren Vorschlägen, so hat er dies zu dokumentieren.

Der Personalrat sollte vor allen geplanten Verarbeitungen mit Beschäftigtendaten unbedingt bei der DSFA hinzugezogen werden. Das erfordert der Grundrechtsbezug in Art. 88 Abs. 2 DS-GVO. Hiernach müssen in Dienstvereinbarungen angemessene Maßnahmen zum Schutz der Rechte und Freiheiten der Beschäftigten festgelegt werden. Die grundrechtskonforme DSFA dient dazu, solche Schutzmaßnahmen zu definieren. Datenschutz ist Grundrechtsschutz und Qualitätssicherung. Hierbei kann der Personalrat unverzichtbare Unterstützung leisten. ◁

Dr. Eberhard Kiesche,
AoB – Arbeitnehmerorientierte Beratung, Bremen.

9 Mit Ablaufschaubild Bieker/Hansen/Friedewald, RDV 2016, 188 (189).
10 Zum Beispiel das Standard-Datenschutzmodell (SDM) der DSK (a.a.O.); WP 248, a.a.O., Annex 1, S. 20.
11 WP 248, a.a.O., Annex 2, S. 21.