BUNDESARBEITSKAMMER

PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65-0

http://wien.arbeiterkammer.at

Österreichische Datenschutzbehörde
Wickenburggasse 8
1080 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
DSB-D056.000/000GSt/DZ/Ho 4-DSB/2018	BAK/KS-	Daniela Zimmer	DW12722	DW12693	02.08.2018

Verordnung der Datenschutzbehörde – Datenschutz-Folgenabschätzung (DSFA-V)

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfs und nimmt dazu wie folgt Stellung:

Zweck

Mit dem vorliegenden Entwurf kommt die Datenschutzbehörde den Vorgaben des Art 35 Abs 4 Datenschutz-Grundverordnung (DSGVO) nach. Demnach hat sie eine Liste zu veröffentlichen, aus der jene Arten von Datenverarbeitungen hervorgehen, für die Verantwortliche eine Datenschutz-Folgenabschätzung (DSFA) zum Nachweis der Einhaltung datenschutzrechtlicher Anforderungen vorzunehmen haben. Die DSFA hat eine Beschreibung geplanter Datenverarbeitungen, ihrer Notwendigkeit und Verhältnismäßigkeit, die Risiken, ihre Bewältigung und den Nachweis, dass die DSGVO damit eingehalten wird, zu enthalten. Aufzunehmen sind jene Aktivitäten, von denen ein hohes Risiko für die Rechte und Freiheiten der Betroffenen (aufgrund der Art, des Umfangs, der Umstände bzw Zwecke) ausgeht. Wird ein Verarbeitungsvorgang in der Verordnung nicht erwähnt, befreit dies den Verantwortlichen nicht in jedem Fall von seiner Pflicht, eine DSFA durchzuführen. Er muss dann aus eigenem bewerten, ob eine DSFA geboten ist.

DVR NR. 1048384

Zusammenfassende Bewertung

- **Detailliertere Liste:** Bleiben Verarbeitungen in der Liste unerwähnt, stellt dies zwar keinen Blankoscheck einer zwangsläufigen Entbindung von der DSFA dar. Dennoch dürften Verarbeiter diesen Umstand für sich als günstiges Indiz deuten, keine DSFA vornehmen zu müssen. Vielfach werden sie daher nicht von sich aus die Initiative zu einer DSFA setzen. Vor diesem Hintergrund sollte die Liste möglichst umfassend und lückenlos typische risikogeneigte Anwendungen anführen.

- **Ergänzung um konkrete Anwendungsbeispiele:** Die Bestimmungen des Entwurfs weisen einen sehr hohen Abstraktionsgrad auf. Die Zuordnung von Datenverarbeitungen zu solchen die DSFA-pflichtig sind (oder nicht), wird in der Praxis äußerst schwierig sein. Als Anregung sei auf einige der deutschen Aufsichtsbehörden (zB Landesbeauftragter für Datenschutz Baden-Württemberg) verwiesen. Diese bieten Rechtsanwendern äußerst praktische Hilfestellungen in Form von Tabellen mit anschaulichen, konkreten Anwendungsbeispielen.

- **Der Fokus auf die Risikokategorie „umfangreiche" Datenverarbeitungen fehlt:** Die Art 29-Datenschutzgruppe nennt in Bezug auf Big Data folgende Faktoren, die auf eine besondere Risikoneigung hindeuten: Zahl der Betroffenen, Bandbreite der Datenelemente, Datenmenge, Dauer der Verarbeitung, geografisches Ausmaß. Dieses Risikoprofil fehlt im Entwurf aus nicht nachvollziehbaren Gründen gänzlich. Es sollte im Entwurf ebenso verankert werden.

- **Betriebsvereinbarung oder Zustimmung der Personalvertretung unter Berücksichtigung der inhaltlichen Vorgaben des Art 88 Abs 2 DSGVO:** Nicht jede derartige Vereinbarung führt eo ipso zu einem Entfall der DSFA im Beschäftigungskontext, sondern es muss vielmehr eine entsprechende unionsrechtliche „Qualifizierung" vorliegen, sprich es müssen insb geeignete und besondere Maßnahmen zur Wahrung der berechtigten Interessen der Beschäftigten vereinbart werden.

- **Die zweite Liste mit wenig strikten Anforderungen ist praxisfern und damit datenschutzunfreundlich:** Nach den Vorstellungen der DSB müssen zwei von vier sehr spezifischen Situationen für eine DSFA-Pflicht vorliegen (§ 2 Abs 3). Die Trennung der Risikobereiche in zwei verschiedene Listen mit unterschiedlich strengen Anforderungen ist nicht sachgerecht und sollte aufgegeben werden. Bei nur vier Auswahlkriterien wären in der Praxis zwei „Treffer" selten.

- **Pflicht zur DSFA beim Abgleich von Datensätzen zu wenig streng:** Die Einschränkungen (zB auf Verarbeitungen, die über die nach „Verkehrssitten" zu erwartende Verarbeitungen hinausgehen) sind vage, kaum bewertbar und sollten zur Anhebung des Datenschutzniveaus unbedingt gestrichen werden.

Zum Hintergrund

Art 35 Abs 3 DSGVO nennt exemplarische Fälle, in denen eine DSFA durchzuführen ist:

1. Systematische, umfassende Bewertung persönlicher Aspekt von Personen auf Basis automatisierter Verarbeitung bzw Profilings als Grundlage für Entscheidungen, die Rechtswirkung entfalten oder Personen in ähnlicher Weise erheblich beeinträchtigen;
2. umfangreiche Verarbeitung sensibler Daten oder von Daten über Straftaten;
3. systematische, weiträumige Überwachung öffentlich zugänglicher Bereiche.

Die Aufsichtsbehörden können bei der Ausarbeitung ihrer Liste auf die Leitlinien der Artikel 29-Datenschutzgruppe (WP248) zurückgreifen. Diese hat 2017 ein Arbeitspapier (WP248) veröffentlicht, das Klassen an Verarbeitungsvorgängen bestimmt, von denen voraussichtlich ein hohes Risiko für die Betroffenen ausgeht. Neun Kriterien wurden herausgearbeitet: Bewerten oder Einstufen von Personen, automatisierte Entscheidungsfindung mit Rechtswirkung, systematische Überwachung, vertrauliche oder höchstpersönliche Daten (va sensible bzw strafrechtliche Daten), Daten in großem Umfang, Abgleichen oder Zusammenführen von Datensätzen, Daten über schutzbedürftige Betroffene, neue technologische Lösungen und Verarbeitungen, die Betroffene an der Rechtsausübung, Nutzung eines Dienstes oder Durchführung eines Vertrages hindern. Erfüllt ein Verarbeitungsvorgang zwei dieser Kriterien, muss der Verantwortliche nach den Vorstellungen der Art 29-Datenschutzgruppe zum Schluss kommen, dass eine DSFA verpflichtend ist. Manchmal wird der Datenverantwortliche von der Notwendigkeit einer DSFA nach dem Arbeitspapier auch schon dann ausgehen müssen, wenn nur ein Kriterium erfüllt ist.

Zu den Details des Entwurfes

- **Zu § 2 Abs 1 (Verarbeitungsvorgänge für die eine Datenschutz-Folgenabschätzung durchzuführen ist):**

Die BAK begrüßt den Hinweis im Besonderen Teil der Erläuterungen, dass die Nicht-Anführung einer Verarbeitungstätigkeit in der vorliegenden Verordnung (VO) nicht unbedingt bedeutet, dass keine DSFA durchzuführen wäre, sondern die Vorabprüfung gem Art 35 Abs 1 DS-GVO immer geboten ist.

Nach Ansicht der BAK wäre es für den Rechtsunterworfenen, sprich hauptsächlich den Verantwortlichen, aber noch um vieles transparenter, wenn dieser wichtige Hinweis direkt im Verordnungstext aufzufinden wäre, was hiermit angeregt wird.

- **Liste in § 2 Abs 2 (Pflicht zur DSFA bei einem erfüllten Kriterium) wird begrüßt:**

Ausdrücklich begrüßt wird, dass bei Vorliegen eines der Kriterien des § 2 Abs 2 jedenfalls eine DSFA durchzuführen ist. Damit erhöht sich die Rechtssicherheit in einem Bereich, der ohnehin von schwierigen Abwägungen geprägt ist. Das gewählte System schafft mehr Klarheit für den Rechtsanwender als der Vorschlag der Art 29-Gruppe. Letzterer basiert auf der Idee, dass bei gleichzeitigem Vorliegen von zumindest zwei der angeführten Kriterien eine DSFA regelmäßig durchzuführen ist, bei lediglich einem Kriterium kann sie – abhängig von den Umständen des Einzelfalls – ebenfalls erforderlich sein.

- **Der Entwurf lässt die Risikokategorie „umfangreiche" Datenverarbeitungen außer Acht:**

Der Entwurf orientiert sich über weite Strecken an den Leitlinien der Art 29-Datenschutzgruppe. Vor diesem Hintergrund ist nicht nachvollziehbar, weshalb die Kategorie „Datenverarbeitung in großem Umfang" gar nicht aufgegriffen wurde. Dieses Merkmal hat die Arbeitsgruppe als Indiz für besonders risikogeneigte Anwendungen eingestuft. Auch Artikel 35 Abs 3 DSGVO hebt diesen Aspekt mehrfach hervor („umfangreiche Verarbeitung besonderer Kategorien von Daten", „umfangreiche Überwachung öffentlich zugänglicher Orte"). Der Hinweis in den Erläuterungen, dass bei Verarbeitungen nach Art 26 DSGVO (also Verarbeitungen mit mehreren Verantwortlichen) große Datenmengen verarbeitet werden, reicht jedenfalls nicht aus, um dem Risiko, das von einer Verarbeitung vielfältigster Datenarten ausgeht, gerecht zu werden.

Vor diesem Hintergrund ist es erforderlich, den Begriff „umfangreiche Datenverarbeitungen" in die Verordnung aufzunehmen und DSFA-pflichtige Anwendungsfelder für diesen Risikobereich näher zu determinieren.

- **Zur Ausnahme bei Vorliegen eines Instrumentes der kollektiven Mitbestimmung in § 2 Abs 2 letzter Satz**

Eine DSFA ist nach dem Entwurf vom Verantwortlichen im Zusammenhang mit Beschäftigungsverhältnissen dann nicht jedenfalls durchzuführen, wenn zwar eines der genannten Kriterien erfüllt ist, aber eine Betriebsvereinbarung oder eine Zustimmung der Personalvertretung vorliegt.

Die BAK schätzt diese Anerkennung der Möglichkeit des prophylaktischen Persönlichkeitsschutzes von Beschäftigten durch Instrumente der kollektiven Mitbestimmung. In diesem Sinne sollte aber genau diese Zweckrichtung des prophylaktischen Persönlichkeitsschutzes als Begründung des – möglichen – Entfalls einer DSFA normativ betont werden; am empfehlenswertesten erscheint der BAK aus Gründen der Rechtssicherheit diesbezüglich folgende – sich inhärent aus der DSGVO im Beschäftigungskontext ergebende – Formulierung: **„Betriebsvereinbarung oder Zustimmung der Personalvertretung unter Berücksichtigung der inhaltlichen Vorgaben des Art 88 Abs 2 DSGVO"**.

Damit wird klargestellt, dass nicht jede derartige Vereinbarung eo ipso zu einem Entfall der DSFA im Beschäftigungskontext führt, sondern vielmehr eine entsprechende unionsrechtliche „Qualifizierung" vorliegen muss, sprich insb geeignete und besondere Maßnahmen zur Wahrung der berechtigten Interessen der Beschäftigten vereinbart werden müssen.

- **Pflicht zur DSFA bei Zusammenführung und/oder Abgleich von Datensätzen nur, wenn die Verarbeitung über die nach „Verkehrssitten" zu erwartende Verarbeitungen hinausgeht**

Die Erläuterungen führen zu Abs 2 Z 6 Folgendes aus: Entscheidend sei, dass Daten aus mehreren Verarbeitungen „verschnitten" werden, und die Verarbeitung über die von Betroffenen üblicherweise, dh nach der Verkehrsauffassung oder den Verkehrssitten bzw nach der Lebenserfahrung im Regelfall – ohne das Vorliegen außergewöhnlicher Umstände – zu erwartenden Verarbeitungen hinausgeht.

Die Anwendung der Norm im Einzelfall erfordert die Beurteilung von nicht weniger als sieben unbestimmten Begriffen. Sie lässt damit kein verlässliches Urteil darüber zu, wann nun im Falle eines Datenabgleichs eine DSFA vorzunehmen ist und wann nicht. Vor allem die Einschränkung auf Verarbeitungen „die über die von einem Betroffenen üblicherweise zu erwartenden Verarbeitungen hinausgehen" dürfte kaum je einer seriösen Beurteilung zugänglich sein und sollte jedenfalls ersatzlos gestrichen werden.

- **Anforderungen des § 2 Abs 3 nicht praxisnah und damit datenschutzunfreundlich:**

Die in Abs 3 gewählte Systematik bietet aus Grundrechtssicht weniger Schutz, als es die Art 29-Gruppe empfiehlt. Die Liste des Abs 3 erfasst nur 4 Kategorien von denen zumindest zwei vorliegen müssen, um eine Pflicht zur DSFA auszulösen. Dass von diesen vier genannten Situationen (sensible Daten, strafrechtliche Daten, Standortdaten, besonders schutzbedürftige Betroffene) gleich zwei gegeben sind, dürfte angesichts der geringeren Auswahlmöglichkeiten an überdies sehr spezifischen Situationen sehr selten zutreffen. Die Zuordnungen der von der Art 29-Gruppe erarbeiteten Risikobereiche in die striktere Regelung des Abs 2 bzw weniger strikte des Abs 3 ist nicht nachvollziehbar. Warum bspw ein Datenabgleich von wenig heiklen Datenarten jedenfalls eine DSFA bedingt und damit strenger beurteilt wird als die Verarbeitung von „nur" sensiblen Daten (bei denen noch strafrechtsrelevante oder Standortdaten oder besonders Schutzbedürftige zusätzlich erfasst sein müssen, um eine DSFA-Pflicht auszulösen), ist sachlich nicht begründbar.

Die Trennung der Risikobereiche in zwei verschiedene Listen mit unterschiedlich strengen Anforderungen sollte deshalb unbedingt aufgegeben werden. Es sollte bei allen Kriterien nach den Regeln von Abs 2 vorgegangen werden. Alternativ wäre zumindest in Abs 3 anzuordnen, dass eine DSFA durchzuführen ist, wenn neben einem Kriterium nach Abs 3 zumindest ein weiteres aus der Liste des Abs 2 oder 3 erfüllt ist.

- **Zu den Kriterien gemäß § 2 Abs 3:**

In Anlehnung an die Beispiele für die Notwendigkeit einer DSFA in den Leitlinien zur DSFA im WP 248 rev 01 vom 04.10.2017 regt die BAK an, hier eine „Systematische Überwachung" von Betroffenen als weiteres Kriterium aufzunehmen, sprich „Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben". Dadurch würden (in Zusammenschau mit der Z 4 des Entwurfes) sowohl eine systematische Überwachung am Arbeitsplatz als auch ein Profiling von Bewerbern bzw Beschäftigten an Hand öffentlich zugänglicher Daten aus sozialen Netzwerken jedenfalls einer DSFA unterworfen.

- **Anregungen aus der deutschen Umsetzung von Art 35 DSGVO**

Um dem Rechtsanwender angesichts des hohen Abstraktionsgrad der Kriterien für die DSFA eine praktische Hilfestellung zu bieten, arbeiten einige der deutschen Aufsichtsbehörden mit sehr anschaulichen Anwendungsbeispielen. Zur Illustration darf auf die Liste des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Würtemberg verwiesen werden, der für den nicht-öffentlichen Bereich eine Tabelle anbietet, aus der DSFA-pflichtige Verarbeitungstätigkeiten, typische Einsatzfelder und Beispiele sehr übersichtlich hervorgehen.

Für den Rechtsanwender wäre es überaus hilfreich, wenn in den Erläuterungen ebenfalls mit Hilfe einer Tabelle typische, häufige DSFA-pflichtige Verarbeitungsvorgänge möglichst konkret und gut nachvollziehbar veranschaulicht würden. Dazu zählen nach der Vorstellung der deutschen Aufsichtsbehörden bspw Scorings durch Auskunfteien, Banken oder Versicherungen, Fraud-Prevention-Systeme, Inkassodienstleistungen, Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden, soziale Netzwerke, Bewertungsportale, Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten, Einsatz von RFID/NFC durch Apps oder Karten, Offline-Tracking von Kundenbewegungen in Warenhäusern, Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes, Fahrzeugdatenverarbeitung, Einsatz von Dienstleistern mit Sitz außerhalb der EU durch medizinische Leistungserbringer, Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten, Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind, Video-/Telefongespräch-Auswertung mittels Algorithmen, Geolokalisierung, die für die Diensterbringung nicht erforderlich ist usw.

Im Dienste der von uns vertretenen Mitglieder hoffen wir, dass unsere Anliegen aufgegriffen werden und stehen für weitere Auskünfte jederzeit gerne zur Verfügung.

Renate Anderl
Präsidentin
F.d.R.d.A.

Melitta Aschauer-Nagl
iV des Direktors
F.d.R.d.A.