BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
wien.arbeiterkammer.at
DVR 0063673
ERREICHBAR MIT DER LINIE D

Bundesministerium für
Finanzen
Johannesgasse 5
1010 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 651**	Datum
BMF-080700/0012-II/12-DK/2018	BAK/KS-GSt/DZ/MS	Mag Daniela Zimmer	DW 12722	DW 2693	29.03.2018

Bundesgesetz, mit dem das Transparenzdatenbankgesetz 2012 geändert wird (Datenschutzanpassung)

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

Zweck der Änderungen

Mit dem vorliegenden Entwurf erfolgen terminologische Anpassungen an die Datenschutz-Grundverordnung (DSGVO). Soweit die DSGVO im Rahmen von Öffnungsklauseln nationalen Regelungsspielraum eröffnet, wird dieser im vorliegenden Entwurf für einige spezifische Datenschutzregeln genutzt.

Zusammenfassende Bewertung

Der Entwurf wird BAK-seits über weite Strecken zur Kenntnis genommen.

Der Regelungsvorschlag in § 36 h des Entwurfes sollte jedoch aus BAK-Sicht unbedingt kritisch hinterfragt und letztlich ersatzlos gestrichen werden:

Das Betroffenenrecht, von erheblichen Datenschutzverletzungen durch den für die Transparenzdatenbank verantwortlichen Finanzminister benachrichtigt zu werden, wird mit der Begründung ausgeschlossen, die Daten seien pseudonymisiert. Dieser pauschale Ausschluss der Benachrichtigungspflicht ist aus BAK-Sicht nicht DSGVO-konform. Eine Verständigung über die Entwendung verschlüsselter Daten kann nur dann unterbleiben, wenn sie nicht auch gleichzeitig entschlüsselt wurden (oder ein hohes Entschlüsselungsrisiko besteht).

Zu den Details dieser Regelung

Den Erläuterungen zufolge sind sämtliche in der Transparenzdatenbank enthaltenen Daten mit einem bereichsspezifischen Personenkennzeichen verschlüsselt und damit pseudonymisiert.
§ 36 h schließt das Betroffenenrecht auf Benachrichtigung von etwaigen Datenschutzverletzungen gegenüber dem Verantwortlichen mit der Begründung aus, die Daten seien pseudonymisiert. Dem datenverantwortlichen Finanzminister sei deshalb eine Identifikation zur Verständigung der betroffenen Personen auch gar nicht möglich.

Dieser Ansicht ist Folgendes entgegenzuhalten:

Auch bei Verwendung verschlüsselter Daten sind natürlich Gefahrenszenarien denkbar, die eine Benachrichtigungspflicht im Sinn des Artikel 34 DSGVO auslösen. So ist bspw nicht auszuschließen, dass die Verschlüsselung selbst erfolgreich angegriffen und das in Artikel 34 DSGVO angesprochene Risiko für die Privatsphäre schlagend wird.

Pseudonymisierte Daten sind (mittelbar) personenbezogene Daten und unterliegen dem vollen Anwendungsbereich der DSGVO. Nach Artikel 34 DSGVO hat der Verantwortliche Betroffene von einem „Data Breach"-Vorfall zu benachrichtigen, wenn die Verletzung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten" für die Betroffenen darstellt. Alle in Abs 3 abschließend geregelten Ausnahmen für die Benachrichtigungspflicht sind für den im Entwurf geregelten Fall der Verwendung von pseudonymisierten Daten daher nur beschränkt einschlägig und daher auch nur bedingt nutzbar zu machen.

Nach Artikel 34 Abs 3 a) kann eine Verständigung entfallen, wenn der Verantwortliche geeignete technische Sicherheitsvorkehrungen (zB Verschlüsselung) für die von einem „Data Breach"-Vorfall betroffenen Daten getroffen hat. Der DSGVO-Kommentar Kühling/Buchner verweist darauf, dass es „unklar ist, welche konkreten Anwendungsfälle durch diesen Befreiungstatbestand adressiert werden". „Der Ausnahmetatbestand sei jedenfalls nur relevant, wenn zuvor eine Verletzung des Datenschutzes bejaht wurde – also die Sicherheitsvorkehrungen die Verletzung gerade nicht verhindern konnten. Das Beispiel Verschlüsselung deutet auf Sachverhalte hin, bei denen Unberechtigte entweder auf ein System zugreifen können oder einen Datenträger entwenden konnten, in denen ausschließlich verschlüsselte Daten gespeichert sind. Im Ergebnis wurden dann zwar Sicherheitsvorkehrungen gebrochen, aber es kommt dennoch zu keiner Verletzung der Sicherheit personenbezogener Daten."

Mit anderen Worten: eine präventive Datenverschlüsselung entbindet den Auftraggeber nur dann von seiner Benachrichtigungspflicht, wenn die Daten „nur“ rechtswidrig entwendet werden. Wurden sie darüber hinaus auch nachweislich entschlüsselt oder besteht ein hohes Risiko, dass sie entschlüsselt werden könnten, so hat der Auftraggeber ohne Zweifel seiner Benachrichtigungspflicht nachzukommen. Da der Auftraggeber wohl in der Regel die erfolgreiche Entschlüsselung bereits rechtswidrig im Umlauf befindlicher verschlüsselter Daten nicht ausschließen wird können, wird er vorsorglich seiner Benachrichtigungspflicht (unter Einbindung der Stammzahlenregisterbehörde, die die Betroffenen identifizieren kann) auch nachkommen müssen.

Vor diesem Hintergrund ist der in § 36 h vorgenommene pauschale Ausschluss der Benachrichtigungspflicht von Betroffenen im Fall von erheblichen Datenschutzverletzungen durch den Finanzminister als Auftraggeber der Transparenzdatenbank überschießend und nicht DSGVO-konform.

In Bezug auf Artikel 34 DSGVO gibt es keine speziellen Öffnungsklauseln für nationale, ergänzende Regelungen. Es gilt das Transformationsverbot, weshalb auch eine Einschränkung der Bestimmung auf den exakten Regelungsgegenstand des Artikel 34 Abs 3 a DSGVO nicht sachgerecht wäre. Daher ist die Bestimmung ersatzlos zu streichen.

Rudi Kaske
Präsident
F.d.R.d.A.

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