An die
Datenschutzbörde

Wickenburggasse 8
1080 Wien

Wien, 31. Juli 2018

Betreff: Zeichen: DSB-D056.000/0004-DSB/2018
Entwurf der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung durchzuführen ist (DSFA-V)

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Dieses Dokument ist mit einer qualifizierten elektronischen Signatur versehen.

Anlage:
Stellungnahme elektronisch übermittelt
(dsb@dsb.gv.at)

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

1. Einleitung

Grundsätzlich ist jede Verordnung zu begrüßen, die die Vorgaben der DSGVO näher bestimmt und damit einen Beitrag zur Förderung der Rechtssicherheit im Datenschutz leistet.

Es ist für alle Verantwortlichen von zentraler Bedeutung zu wissen, wann verpflichtend eine Datenschutzfolgenabschätzung (DSFA) durchzuführen ist. Eine derartige Folgenabschätzung muss, wenn sie seriös gemacht wird mit 5-20 Personentagen und entsprechenden Kosten je Verarbeitung kalkuliert werden.

Kein Verantwortlicher wird diese Kosten überflüssigerweise tragen wollen, andererseits aber auch nicht leichtfertig eine Folgenabschätzung unterlassen, mit weitreichenden Schadenersatz- und Straffolgen.

Leider erfüllt der vorgelegte Verordnungsentwurf nur bedingt die Aufgabe Rechtssicherheit zu schaffen. Im Gegensatz zu den geradezu vorbildlichen Bestimmungen der früheren Standard- und Musterverordnung, gibt der vorliegende Entwurf über weite Strecken bloß die Bestimmungen der DSGVO wieder. Selbst in den Erläuterungen wird nicht entscheidend über die Empfehlungen der (früheren) Artikel 29 Datenschutzgruppe, jetzt "European Data Protection Board" hinaus gegangen.

Statt wie in der bisherigen Standard- und Musterverordnung konkrete Einsatzszenarien bis hin zu Datenarten, Betroffenenkreise und Übermittlungsempfänger zu beschreiben, bleiben die Vorgaben abstrakt und allgemein.

Diese führt etwa dazu, dass eine Datenschutzfolgenabschätzung unterschiedslos bei allen Verarbeitungen durchzuführen ist, bei denen mehrere Verantwortliche beteiligt sind. Unabhängig davon ob zwei Internetkonzerne mehrere hundert Millionen Userdaten abgleichen oder zwei selbständige Sozialforscher eine gemeinsame Umfrage mit 800 Teilnehmern organisieren.

Es wird daher dringend angeregt zumindest in einem verbindlichen Anhang Größenordnungen bei der Zahl der betroffenen Perrsonen, bei den verwendeten Datenarten und den angewandten Verarbeitungstechniken aufzulisten die jedenfalls zu einer Datenschutzfolgenabschätzung führen.

Eine derartige Liste hätte auch den Vorteil, dass Verantwortliche - um eine umfassende Folgenabschätzung zu vermeiden - auch auf einzelne, nicht absolut erforderliche "riskante" Verarbeitungsformen verzichten. Ein von der DSGVO jedenfalls gewünschter Lenkungseffekt.

Es ist der ARGE DATEN selbstverständlich bewusst, dass auf Grund der technologischen Entwicklung einzelne Verarbeitungen in Zukunft als "riskant" hinzu kommen werden, während wiederum andere Verarbeitungen nicht jenes Risikopotential haben, als ursprünglich angenommen.

Deshalb wurde vom Gesetzgeber auch das Instrument der Verordnung gewählt, dass eine rasche Anpasssung an neue technische Gegebenheiten erlaubt. Diese Vorgangsweise hat

sich unter anderem im Signaturbereich, aber auch in anderen Bereichen wie dem Umweltschutz oder der Ernährung bewährt.

2. § 2 Abs. 2 Z 1 + 2 Bewertung persönlicher Aspekte

Die Bestimmungen der Ziffern 1 und 2 zielen offenkundig auf die "Profiling"- und automatisierte Entscheidungsfingungs-Regelung der DSGVO ab, enthalten jedoch, ebenso wie die DSGVO, zahlreiche unbestimmte Formulierungen. Selbst die Erläuterungen zum Entwurf sind nicht wesentlicher bestimmter.

So sollen "*Verarbeitungen, die eine Bewertung oder Einstufung natürlicher Personen ... umfassen ... und negative rechtliche, physische oder finanzielle Auswirkungen haben können*" zu einer Folgenabschätzung führen.

Streng genommen trifft das auf jede Bewerberliste mit Reihung der Einladung zum Vorstellungsgespräch, jede Warteliste oder sonstige Liste zu, bei der Personen nicht bloß alphabethisch gereiht werden. Selbst eine alphabethische Reihung *könnte negative rechtliche, physische oder finanzielle Auswirkungen haben*.

Durch die Verwendung des Konjunktiv bei gleichzeitiger Vermeidung eine Darstellung jener Verarbeitungsszenarien, an die der Verordnungsautor gedacht hat, wird diese Bestimmung zur Allerweltsregel, in der alle oder niemand darunter fallen.

Auch die zweite Formulierung "*Verarbeitungen von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von natürlichen Personen dienen und von Dritten dazu genutzt werden können, automatisierte Entscheidungsfindungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten*", lässt sich auf jede beliebige öffentlich zugänglich Liste anwenden.

So existieren Verarbeitungen und Dienste die aus der Art und Zahl der sozialen Kontakte in einem Social Media Account, aus der Zahl von Postings, aus der Verwendung von Wörtern, ... Kreditwürdigkeit, sozialen Status, Bedeutung, wirtschaftliche Vernetzung, politischen Einfluss usw ableiten.

Die in diesem Entwurf gewählte Formulierung würde jedoch nicht nur jene verpflichten eine Datenschutzfolgenabschätzung zu machen, die derartige Interpretationen vornehmen, sondern schon alle die derartige Informationen bereit stellen bzw. veröffentlichen.

Nimmt man die Formulierung des Verordnungsentwurfs wörtlich, würde sogar das Firmenbuch mit seinen Angaben zu Gesellschaftsverhältnissen, Geschäftsführern und Handelsbevollmächtigten unter die Gruppe der "riskanten" Verarbeitungen fallen. Auch aus der Verknüpfung dieser Daten lässt sich etwa wirtschaftlicher Einfluss oder Vermögen der eingetragenen Personen ableiten. Es wäre damit eine verpflichtende Folgenabschätzung erforderlich.

3. Ausnahmen bei Bestehen einer Betriebsvereinbarung

Von einer Datenschutzfolgenabschätzung generell ausgenommen werden Verarbeitungen im Beschäftigungsverhältnis, zu denen eine Betriebsvereinbarung existiert.

Diese Ausnahme ist zu weitreichend und verkennt das Instrument der Betriebsvereinbarung. In der langjährigen Beratungspraxis der ARGE DATEN war durchgehend festzustellen, dass gerade das Vorliegen oder Nicht-Vorliegen der Genehmigung einer Datenverarbeitung durch die Datenschutzbehörde den Abschluss oder die Verweigerung einer Betriebsvereinbarung erleichterte.

Betriebsräte sind in der Regel arbeitsrechtlich gut informiert, nicht jedoch Experten in der Bewertung riskanter Datenverarbeitungen. Mit der generellen Ausnahme BV-pflichtiger Verarbeitungen von der Folgenabschätzung nimmt man den Betriebsräten eine einfache Möglichkeit sich über die Risken einer Verarbeitung zu informieren.

De facto stellt diese Ausnahme einen Freibrief dar, beliebige Maßnahmen zur Mitarbeiterüberwachung ohne Risikoabschätzung einzuführen.

4. Verarbeitungen von Standortdaten

In § 2 Abs. 3 Z 3 werden "Standortdaten" als eines von vier Kriterien genannt, die bei Vorliegen gemeinsam mit einem anderen Kriterium zu einer Folgenabschätzung führen sollen.

Dabei wird einerseits auf die Definition gemäß Telekommunikationsgesetz TKG 2003 verwiesen ("*Standortdaten im Sinne des § 92 Abs. 3 Z 6 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I. Nr. 70/2003*"), andererseits auch der Kreis der Verantwortlichen gemäß TKG 2003 festgelegt ("*die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden*").

Diese Festlegung ist zu eng, da die meisten Verarbeitungen von Standortdaten durch Dienstangebote der "Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999" erbracht werden. Hier ist etwa an die zahllosen Tracking-Apps zu denken, die über GSM Location-Based-Services, vom Restaurantführer bis zur interaktiven Landkarte, anbieten.

Genau diese Dienste sind jedoch in der zitierten Stelle des Telekommunikationsgesetzes ausgenommen. Es sollte daher entweder direkt auf die zutreffende e-Commerce Bestimmung (§ 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001) verwiesen werden oder in der Verordnung klar gestellt werden, dass alle Verantwortlichen erfasst sind, sobald sie für ihre Verarbeitungen systematisch Standortinformationen - unabhängig von der eingesetzten Technik und unabhängig vom formalen gewerberechtlichen Status, verarbeiten.

5. "unmündige Minderjährige"

§ 2 Abs. 3 Z 4 des Verordnungentwurfs spricht von "*unmündige Minderjährigen*". Es handelt sich vermutlich um ein Redaktionsversehen. Gemeint sind offenbar Unmündige und Minderjährige.

6. "Arbeitnehmern"

§ 2 Abs. 3 Z 4 des Verordnungentwurfs spricht weiters von "Arbeitnehmern" als Betroffenengruppe, bei der von einer Datenschutz-Folgenabschätzung auszugehen ist. Dies ist grundsätzlich zutreffend, steht aber im Widerspruch zu § 2 Abs 2 letzten Absatz, in dem generell Verarbeitungen im Beschäftigtenkontext von einer Folgenabschätzung ausgenommen sind, wenn ein Betriebsrat existiert.

Hier wird vorgeschlagen auf die Ausnahmebestimmung des § 2 Abs 2 letzten Absatz zu verzichten.

7. "Bonitätsdatenbanken"

In den Erläuterungen zum Entwurf wird auf Seite zwei von "*Bonitätsdatenbanken*" gesprochen, "*mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrages gestattet, geändert oder verwehrt werden soll.*"

In zahllosen Entscheidungen der Datenschutzbehörde, davor der Datenschutzkommission wurde festgestellt, dass Wirtschaftsauskunftsdienste bloß Bonitätsdaten verarbeiten, daraus jedoch keine Entscheidungen ableiten. Umgekehrt die Kunden dieser Unternehmen zwar auf Basis dieser Daten Entscheidungen treffen, jedoch keine Datenbank führen.

Der Begriff "*Bonitätsdatenbanken*" ist daher irreführend und nicht geeignet bestimmte riskante Verarbeitungsvorgänge zu beschreiben.

Es wird vorgeschlagen, konkret die Datenbank der Wirtschaftsauskunftsdienste (iS der Gewerbeordnung) als jene Verarbeitungen zu bezeichnen, die der Folgenabschätzung unterliegen.

8. Zusammenfassung

Der vorliegende Entwurf ist nicht geeignet für Betroffene oder Verantwrtliche Klarheit zu schaffen, wann eine Folgenabschätzung vorzunehmen ist.

Durch unbestimmte Formulierungen, zu weitreichende Ausnahmen und fehlerhafte Verweise besteht sogar die Gefahr, dass das durch das bisherige Vorabkontrollverfahren erreichte Schutzniveau grob unterschritten wird.