An die
Datenschutzbehörde
Wickenburggasse 8
1080 Wien

dsb@dsb.gv.at.

Wien, am 03. August 2018

BETREFF: ISPA STELLUNGNAHME ZUM ENTWURF EINER VERORDNUNG DER DATENSCHUTZBEHÖRDE ÜBER VERARBEITUNGSVORGÄNGE, FÜR DIE EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN IST (DSFA-V)

Sehr geehrte Damen und Herren,

die ISPA dankt für die Möglichkeit Stellung nehmen zu dürfen und erlaubt sich im Interesse ihrer Mitglieds-Unternehmen zum Entwurf einer Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgeabschätzung durchzuführen ist (DSFA-V), wie folgt Stellung zu nehmen:

Zusammengefasst merkt die ISPA an, dass eine nationale Datenschutz-Folgeabschätzungsverordnung eine die Datenschutz-Grundvorordnung (DSGVO) präzisierende und nicht überschießende Regelung darstellen soll, um das Harmonisierungsniveau der DSGVO nicht zu untergraben. Ferner betont die ISPA, dass der Entwurf zwischen automatischer oder manueller Verarbeitung differenzieren soll und nur eine vollautomatisierte Entscheidungsfindung iSv § 2 Abs. 2 Z 2 DSFA-V als hochriskant gelten soll. Ferner merkt die ISPA an, dass sich diese Verordnung generell nur auf risikoreiche Verarbeitungsvorgänge beschränken soll, um eine überschießende Regulierung zu verhindern. Da das Rechtinstitut der gemeinsamen Verantwortlichen nicht pauschal als risikoreich eingestuft werden kann, lehnt die ISPA ab, dass die Datenverarbeitung durch gemeinsame Verantwortliche an sich als Kriterium für die Durchführung einer verpflichtenden Datenschutz-Folgeabschätzung (DSFA) eingestuft wird. Das Kriterium des Abgleichens und des Zusammenführens von Datensätzen soll weiter präzisiert und eingeschränkt werden. Aus Sicht der ISPA ist außerdem das bloße Vorliegen von besonderen Datenkategorien als Kriterium für eine verpflichtende DSFA ausufernd.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

1. Die DSFA-V sollte eine die DSGVO präzisierende und nicht überschießende Regelung darstellen

Einleitend begrüßt die ISPA die Initiative der Datenschutzbehörde (DSB), eine Verordnung zu veröffentlichen, welche eine Präzisierung des Textes der Datenschutz-Grundverordnung darstellt, und dadurch den rechtssicheren Umgang mit personenbezogenen Daten fördert. In ihrer Bestrebung eine umfassende Hilfestellung für Verantwortliche zu bieten, hat die DSB jedoch eine sehr weitreichende Auflistung der Verarbeitungstätigkeiten vorgenommen, welche möglicherweise ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellen könnten. Die ISPA weist darauf hin, dass die Verordnung keine taxative Aufzählung jener Anwendungsbereiche darstellen kann, die einer verpflichtenden Datenschutz-Folgeabschätzung unterliegen würden, da bei den meisten Verarbeitungsvorgängen allemal im Einzelfall zu prüfen ist, ob diese aufgrund der Art, des Umfangs, der Umstände oder des Zwecks ein hohes Risiko mit sich bringen. Im Hinblick dieser unabdingbaren Einzelfallprüfung ist zu hinterfragen, ob eine derart umfangreiche Auflistung von potentiell problematischen Verarbeitungstätigkeiten personenbezogener Daten in der DSFA-V nicht überschießend bzw. kontraproduktiv ist.

Zudem möchte die ISPA anmerken, dass es für die formale Abstimmung der DSFA-V im Europäischen Datenschutzausschuss gemäß Art. 63 DSGVO sehr förderlich wäre, wenn der österreichische Entwurf einer DSFA-V die best practice Beispiele aus anderen Mitgliedstaaten bereits berücksichtigen würde, um besser zu einer unionsweit einheitlichen und kohärenten Umsetzung der Verordnungsermächtigung des Art. 35 Abs. 4 DSGVO beizutragen. Beispielsweise haben die deutschen Aufsichtsbehörden bereits eine „Muss-Liste“ veröffentlicht, welche sich stark an die Leitlinien[1] der Art 29 Datenschutzgruppe, des heutigen Europäischen Datenschutzausschusses, orientiert.[2]

Die deutsche „Muss-Liste“ unterscheidet sich wesentlich von der österreichischen Umsetzung, indem die deutschen Behörden von einem hohen Risiko ausgehen, wenn zwei oder mehrere der beschriebenen Kriterien vorliegen. Im Gegensatz zur deutschen „Muss-Liste“ würde bereits das Vorliegen eines der in § 2 Abs. 2 des Entwurfs der österreichischen DSFA-V ausgewiesenen Kriterien ausreichend sein, um die Durchführung einer DSFA auszulösen.

Um das Harmonisierungsniveau der DSGVO nicht zu untergraben, regt die ISPA daher eindringlich die Abstimmung des Entwurfs der österreichischen DSFA-V mit der deutschen Muss-Liste sowie die Berücksichtigung des dort eingeführten Kriterienkatalogs[3] an. Ferner sollte der österreichische Entwurf einer DSFA-V der Leitlinie des Art. 35 Abs. 3 DSGVO folgen, welcher

[1] Artikel 29 Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, vom 04.04.2017 idF von 04.10.2017, WP 248 Rev. 01.
[2] „Muss-Liste“ der deutschen Bundesländer Rheinland-Pfalz, Baden-Württemberg, Brandenburg: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf ; https://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss-Liste_allgemein_180525.pdf ; https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf
[3] WP 248 Rev. 01, S. 10ff.

bereits bestimmte Kriterien für die Erforderlichkeit einer DSFA enthält, um eine überschießende Regulierung zu vermeiden.

2. Der Entwurf soll zwischen automatischer oder manueller Verarbeitung differenzieren

In § 2 Abs. 2 Z 1 und Z 2 DSFA-V normiert die DSB, dass bei der Datenverarbeitung zur Bewertung oder Einstufung natürlicher Personen eine DSFA durchzuführen ist. Dabei besteht das Risiko bei der Bewertung oder Einstufung natürlicher Personen aus Sicht der Behörde darin, dass sich durch das Erstellen von Profilen oder Prognosen, eine Rechtswirkung (z.B. Ablehnung eines Vertragsabschlusses) gegenüber der bewerteten Person entfaltet könnte, oder diese in ähnlicher Weise beeinträchtigt wird. Die beiden Ziffern unterscheiden sich im Wesentlichen nur durch das Kriterium der automatisierten Entscheidungsfindung. Diese ist bereits in Art. 22 DSGVO geregelt und erfasst jenen Fall, welcher tatsächlich ein hohes Risiko iS eines hohen Diskriminierungspotentials für betroffene Personen mit sich bringen könnte.

Die bloße Bewertung von Personen, welche potenzielle „*negative rechtliche, physische oder finanzielle Auswirkungen*“ haben könnte, kann nur im Einzelfall und keinesfalls pauschal als risikoreiche Datenverarbeitung eingestuft werden. Diese Argumentationslinie wird auch durch Art 35 Abs 3 lit a) bestätigt, da dieser eine DSFA nur im Fall einer „*systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet*“ vorschreibt, die ihrerseits als „*Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen*“.

In § 2 Abs. 2 Z 1 wird nicht differenziert, ob die Verarbeitung automatisch oder manuell erfolgt. Dadurch wird auch die nicht-automatisierte Überprüfung der Bonität, welche aus zivilrechtlichen aber auch insolvenzrechtlichen Vorgaben notwendig ist, und an rechtliche Folgen, wie die Ablehnung eines Vertragsabschlusses geknüpft ist, als hochriskante Tätigkeit eingestuft. Sinn und Zweck der Einordnung der automatisierten Entscheidungsfindung als spezielle Datenverarbeitung gemäß Art 22 DSGVO war die Bestrebung, einer durch technische Maßnahmen unbeabsichtigten Diskriminierung entgegenzuwirken.

Da das Kriterium der automatisierten Entscheidungsfindung vom § 2 Abs. 2 Z 1 DSFA-V nicht erfasst ist, besteht auch kein Diskriminierungsrisiko, welches zu minimieren gilt. Alle jene Beispiele in den erläuternden Bemerkungen zu den § 2 Abs. 2 Z 1 (Buchstaben a) bis e) einschließlich Profiling können als Auslöser einer DSFA und somit als hochriskant gelten, nur wenn sie durch eine vollautomatisierte Entscheidungsfindung iSd Art. 22 DSGVO erfolgen. Widrigenfalls ist die Erfassung der in Buchstabe a) - Bonitätsdatenbanken und in d) Verhaltens- oder Marketingprofile als eine hochriskante Verarbeitungstätigkeit strikt abzulehnen, da dies zu einem unverhältnismäßigen Eingriff in die tagtäglichen, bislang unproblematischen betrieblichen Abläufe führen würde. Buchstabe d) würde auch Personalisierungs-, Content- und Analysetools auf Websites erfassen, deren „*negative rechtliche, physische oder finanzielle Auswirkungen*“ nicht erkennbar sind.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at
UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705
UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

Die in Z 2 geregelte Datenverarbeitung zur Bewertung des Verhaltens und anderer persönlicher Aspekte aufgrund automatisierter Entscheidungsfindung entspricht aus Sicht der ISPA den Anforderungen der DSGVO und kann allein ausreichend sicherstellen, dass einer durch technische Maßnahmen unbeabsichtigte Diskriminierung verhindert wird. Daher regt die ISPA die Streichung des § 2 Abs. 2 Z1 DSFA-V als eine obsolete und überschießende Bestimmung aus dem Entwurf der DSFA-V an.

3. Die DSFA-V sollte sich nur auf hochriskante Verarbeitungstätigkeiten beschränken

Wie bereits in Art. 35 Abs. 3 lit c DSGVO ist auch gemäß § 2 Abs. 2 Z 3 DSFA-V bei der systematischen Überwachung öffentlich zugänglicher Bereiche eine DSFA durchzuführen. Indem der österreichische Entwurf auch „*über Netzwerke erfasste Daten*“ einschließt, geht dieser einen Schritt weiter als die DSGVO. Die erläuternden Bemerkungen enthalten keine näheren Ausführungen dazu, daher könnte man annehmen, dass auch ein Kontaktformular auf einer Webseite darunter subsumiert werden könnte, da dadurch auch personenbezogene Daten über ein Netzwerk erfasst werden. Darüber hinaus könnten sämtliche Datenverarbeitungsanlagen, welche für die Erbringung von Telekommunikationsdiensten erforderlich sind, auch hineinfallen (Vgl. § 96 Abs. 3 TKG).

Daher regt die ISPA die Einschränkung dieser Ziffer nur auf hochriskante Verarbeitungstätigkeiten an, wie dies vom Art. 35 Abs. 3 lit c DSGVO vorgesehen ist.

In § 2 Abs. 2 Z 4 DSFA-V wird die Nutzung oder Anwendung neuer bzw. neuartiger Technologien und in Art. 35 Abs. 1 DSGVO darüberhinausgehend auch organisatorische Lösungen als risikoreiche Verarbeitungsvorgänge, welche allein für sich eine DSFA auslösen würden, festgelegt. Dabei ist in den erläuternden Bemerkungen nicht präzisiert, was genau unter neuartigen organisatorischen Lösungen zu verstehen ist. Aus Sicht der ISPA kann eine neue technologische oder organisatorische Lösung, losgelöst von der Art und dem Umfang der verarbeiteten Daten, nicht pauschal als risikoreich eingestuft werden. Hinsichtlich des Kriteriums der Anwendung neuer bzw. neuartiger Technologien und organisatorischer Lösungen scheint der deutsche Ansatz zur „Muss-Liste“, welcher entweder ein weiteres Kriterium dazu verlangt oder aufgrund der Art der Technologie im Einzelfall diese als risikoreich einstuft, nachvollziehbar. Die ISPA regt daher an, dass die Bestimmung in diesem Sinne neue überdacht wird.

4. Die Datenverarbeitung durch gemeinsame Verantwortliche kann nicht pauschal als risikoreich eingestuft werden und ist daher als Kriterium abzulehnen

Die ISPA lehnt die pauschale Erfassung der gemeinsam Verantwortlichen ohne jegliche Differenzierung als Kriterium für die Durchführung einer DSFA strikt ab. Aus Sicht der ISPA ist das Rechtsinstitut der gemeinsamen Verantwortlichen genau deshalb geschaffen worden, um die Erfüllung der Betroffenenrechte sowie die Vereinbarungen zwischen den gemeinsamen Verantwortlichen transparenter zu machen und somit die Rechtedurchsetzung rechtssicherer zu

gestalten. Der Umstand, dass die personenbezogenen Daten durch gemeinsame Verantwortlichen verarbeitet werden, sollte eben an sich kein Risiko für die betroffenen Personen darstellen. Auch die Annahme in den erläuternden Bemerkungen, dass im Rahmen der gemeinsamen Verantwortlichkeit stets große Datenmengen verarbeitet werden, ist aus Sicht der ISPA überschießend und daher abzulehnen.

5. Das Kriterium des Abgleichens und des Zusammenführens von Datensätzen soll weiter präzisiert und eingeschränkt werden

Der Entwurf der DSFA-V stuft auch das Abgleichen und Zusammenführen von Datensätzen als ein Kriterium für die Durchführung von DSFA ein. Auch hier weist die ISPA darauf hin, dass das Abgleichen und Zusammenführen von Datensätzen an sich allein noch kein hohes Risiko für die Rechte und Freiheiten betroffener Personen darstellt und sollte daher, wie dies in der deutschen „Muss-Liste" vorgesehen ist, erst beim Vorliegen weiterer Kriterien eine DSFA auslösen.

Dieses Kriterium sollte aus Sicht der ISPA ferner auch an den Umfang der verarbeiteten Daten sowie an die Rechtswirkung gegenüber den betroffenen Personen anknüpfen. Daher regt die ISPA die Aufnahme der weiteren Voraussetzungen für die Erfüllung dieses Kriteriums, wie dies bereits in der deutschen „Muss-Liste" vorgesehen ist, in die Bestimmung an. Weitere Voraussetzungen sind,

- dass die Zusammenführung oder Weiterverarbeitung in großen Umfang vorgenommen werden muss und
- der Erzeugung von Datengrundlagen dienen soll, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkungen gegenüber den betroffenen Person entfalten, oder diese in ähnlicher erheblicher Weise beeinträchtigen können.

Ohne diese Einschränkung würde auch die Erstellung von Berichten zur Qualitätssicherung oder das Abspeichern von Daten in einem Data Warehouse immer automatisch eine DSFA auslösen.

Darüber hinaus fordert die ISPA eine Klarstellung, wie die anschließenden Ausführungen in § 2 Abs 2 DSFA-V, dass dies im Zusammenhang mit Beschäftigungsverhältnissen nicht gälte, „*wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt.[…]* ", im Kontext der obigen Ziffern zu verstehen ist, da sich dieser Absatz einer kohärenten Interpretation entzieht und die Erläuternden Bemerkungen keine nähren Informationen dazu hergeben.

6. Das bloße Vorliegen von besonderen Datenkategorien an sich ist als Kriterium für eine verpflichtende DSFA ausufernd

In § 2 (3) DSFA-V sind jene Kriterien erfasst, welche kumulativ mit einem oder mehreren anderen Kriterien geknüpft werden müssen, um eine Verpflichtung zur Durchführung einer DSFA zu begründen.

Dabei ist in Ziffer 1 und 2 bereits die bloße Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art 9 DSGVO bzw. strafrechtlich relevanten Daten nach Art 10 DSGVO erfasst. Hier könnten auch die Weiterleitung von Krankmeldungen innerhalb eines Unternehmens oder an die zuständige Krankenkasse oder die Bestellung von Bildschirmarbeitsbrillen darunter subsumiert werden. Dabei übersieht der österreichische Entwurf, dass Art. 35 Abs. 3 lit b) DSGVO zusätzlich eine umfangreiche Datenverarbeitung voraussetzt, um die Verarbeitung dieser besonderen Datensätze als risikoreich einzustufen. Das bloße Vorliegen von besonderen bzw. strafrechtlich relevanten Daten an sich, als Grundlage für die verpflichtende Durchführung einer DSFA ist aus Sicht der ISPA ausufernd und entspricht nicht dem Telos der DSGVO und ist daher abzulehnen.

Auch die pauschale Erfassung von Standortdaten iSd § 92 Abs. 3 Z 6 TKG 2003 als Kriterium für eine hochriskante Verarbeitungstätigkeit ist überschießend und lässt den Umstand außer Acht, dass Betreiber diese nicht für Big Data-Anwendungsfälle verarbeiten, sondern ihrer gesetzlichen Verpflichtung, Standortdaten u.a. an Notrufträger zu beauskunften, nachgehen.

Die ISPA ersucht um die Berücksichtigung ihrer Bedenken und Anregungen bei der Gestaltung des Verordnungsentwurfes, insbesondere im Hinblick seiner Kohärenz mit der DSGVO sowie mit den bisherigen Leitlinien der Artikel 29 Datenschutzgruppe.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675