Mag.ª Monika Juch
Mag.ª Nicole Garfias
(stimmberechtigte Mitglieder
in der Sitzung des DSR am 3. Juli 2018)

Dr. Peter Pointner
Abg.z.NR Walter Bacher

Ergänzende Stellungnahme zum Beschluss des Datenschutzrates vom 3. Juli 2018 betreffend Art. 3 des Antrages 303/A der Abgeordneten Peter Haubner, Ing. Wolfgang Klinger, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Arbeitszeitgesetz, das Arbeitsruhegesetz und das Allgemeine Sozialversicherungsgesetz geändert werden

Die beiden Mitglieder des Datenschutzrates Christian Schiesser und Dr. Peter Pointner haben ein schriftliches Ersuchen eingebracht, im Datenschutzrat den im Titel genannten Gesetzesentwurf in Verhandlung zu nehmen. Diesem Ersuchen wurde einstimmig Rechnung getragen und in Folge in einer eigens anberaumten Sitzung des Datenschutzrates am 3. Juli 2018 behandelt. Das damalige Ersuchen wurde wie folgt erläutert:

> **Zu Art. 3 Änderung des Allgemeinen Sozialversicherungsgesetzes:**
> Das Risiko-und Auffälligkeitsanalyse-Tool gemäß § 42b ASVG wurde auf Grund der Regierungsvorlage 692 dB, XXV. GP eingeführt, die das Ziel verfolgte, Sozialbetrug durch Unternehmer oder Scheinunternehmer in Österreich wirksam zu bekämpfen. In Kraft getreten ist diese gesetzliche Maßnahme mit 1. Jänner 2016. Die diesbezüglichen Strafbestimmungen der §§ 153c bis e StGB (Vorenthalten von Dienstnehmerbeiträgen zur Sozialversicherung, Betrügerisches Anmelden zur Sozialversicherung oder Bauarbeiter-Urlaubs- und Abfertigungskasse sowie Organisierte Schwarzarbeit) wurden bereits im Jahr 2004 eingeführt. Dabei handelt es sich um strafbare Handlungen, die mit Freiheitsstrafe von 2 Jahren, in Ausnahmefällen mit Freiheitsstrafe von 6 Monaten bis zu 5 Jahren, bedroht sind.
> Zur wirksamen Bekämpfung dieser oft organisiert begangenen Sozialbetrugs-Tatbestände sollten Daten der Krankenversicherungsträger mit dem Risiko-und Auffälligkeitsanalyse-Tool nach folgenden Gesichtspunkten geprüft werden: Schwarzarbeitsverdacht, Scheinanmeldung, Versichertenströme, Dienstgeberzusammenhänge, Insolvenzgefahr sowie Melde-und Beitragszahlungsverhalten.
> Nunmehr wird der Anwendungsbereich für dieses Tool dahingehend erweitert, dass dieses auch für den Dienstnehmer/innenbereich ab 1. Jänner 2019 verwendet werden soll, um missbräuchliche Inanspruchnahme von Leistungen, insbesondere aus dem Versicherungsfall der Arbeitsunfähigkeit infolge Krankheit, missbräuchlichen Bezug von Heilmitteln, Hilfsmitteln und Heilbehelfen sowie missbräuchliche Verwendung der e-card aufzuklären.
> Es handelt sich daher bei dieser Verarbeitung von Daten um insbesondere Gesundheitsdaten, die nach Art. 9 Datenschutz-Grundverordnung nicht oder nur nach strengen Ausnahmekriterien verarbeitet werden dürfen. Auf diesen Umstand wird weder im Gesetzestext, noch in den Erläuterungen eingegangen.
> Befremdlich erscheint aber, dass in den Erläuterungen ein Generalverdacht in die Richtung ausgesprochen wird, dass insbesondere jenen Personen, die von der Rezeptgebühr befreit sind, sowie deren Angehörigen bei missbräuchlichen Bezug von Heilmitteln, Hilfsmitteln und Heilbehelfen besondere Aufmerksamkeit zu widmen ist.
> Hinsichtlich der Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten (also nach altem Recht sensibler Daten) wird in den Erläuterungen auf Art. 9 Abs. 2 lit. g der Datenschutz--Grundverordnung verwiesen. Zu dieser Bestimmung führt der Kommentar Ehmann/Selmayr zur Datenschutz-Grundverordnung wörtlich folgendes aus:

Die Bestimmung des Art. 9 Abs. 2 Buchst. g stellt tatbestandlich die mit Abstand weiteste Ausnahmeregelung zum Verbot des Abs. 1 dar. Insbesondere weil sie nicht auf eine bestimmte Materie beschränkt ist, ist ihre Bedeutung im gesamten Regelungskomplex zur Verarbeitung sensibler Daten nicht zu unterschätzen. Es steht zu vermuten, dass sie vor allem im Recht der öffentlichen Sicherheit bzw. Gefahrenabwehr zum Tragen kommen wird. Insbesondere aufgrund ihrer tatbestandlichen Weite bedarf die Regelung einer präzisen, rechtsstaatlichen Handhabung, um **den Schutzzweck des Verbotsgrundsatzes trotz mancher Versuchungen und Herausforderungen stets Geltung zu verschaffen**.
Dabei ist die Regelung im Wortlaut an Art. 52 Grundrechte-Charta angelehnt, sodass in Detailfragen der Vergleich zu dieser Bestimmung durchaus lohnt.
Zum erheblichen öffentlichen Interesse führen die Autoren aus, dass dieses Interesse, weil erheblich, besonders qualifiziert sein muss. Es müsste daher ohne diese Maßnahmen die Allgemeinheit ernsthaft beeinträchtigt werden. Auch die Verhältnismäßigkeit der Maßnahme muss einer besonderen Prüfung unterzogen werden. Die Prüfung der Erforderlichkeit ist dabei das Herzstück der Verhältnismäßigkeitsprüfung.
Auch im Kommentar, herausgegeben von Sydow, zur genannten Bestimmung wird zum konkreten Fall ausgeführt:
Ausnahmen sind nur aus Gründen eines erheblichen öffentlichen Interesses zulässig. Aus der Zusammenschau mit Art. 6 Abs. 1 lit. e, der jede öffentliche Aufgabe ausreichen lässt, folgt, dass im Rahmen von lit. g nicht jeder im öffentlichen Interesse liegende Verarbeitungszweck ausreichend ist. Ein erhebliches öffentliches Interesse besteht vielmehr erst dann, wenn Belange des Allgemeinwohls in besonderen Maße berührt werden. **Erwägungsgrund 46 führt beispielhaft die Bekämpfung von Epidemien oder die Hilfeleistung im Katastrophenfall auf.** Von einem erheblichen öffentlichen Interesse wird allgemein dann auszugehen sein, wenn Gründe für die Verarbeitung ein ähnliches Gewicht aufweisen, wie die übrigen in Art. 9 Abs. 2 aufgeführten Verarbeitungsgründe.
Ein Blick in die beiden Standardkommentare zur Datenschutz-Grundverordnung zeigt also deutlich auf, dass die in Aussicht genommene Erweiterung des Anwendungsbereiches des Risiko- und Auffälligkeitsanalyse-Tools auf den Dienstnehmerbereich und damit auf Gesundheitsdaten nicht im Einklang mit den Bestimmungen der Datenschutz-Grundverordnung steht, daher EU rechtswidrig ist und unverhältnismäßig in das Grundrecht auf Datenschutz und das Recht auf Privatheit der Betroffenen eingreift.

Nach der Anhörung von insgesamt acht informierten Vertretern in der Sitzung des Datenschutzrates am 3. Juli 2018 wurde eine Stellungnahme verhandelt, die die Zustimmung der regierungsnahen Vertreter erhielt. Die unterzeichneten Mitglieder begrüßen zunächst die Vorgangsweise ausdrücklich, sehen in der Stellungnahme auch durchaus Fortschritte, erachten jedoch in ihrer Gesamtheit die Stellungnahme als zu wenig weitreichend und geben daher folgende ergänzende Stellungnahme ab:

1. Die Befragung der informierten Vertreter hat ergeben, dass bei den einzelnen Trägern durchaus funktionierende Kontrollsysteme im Einsatz sind. Eine Verrechtlichung dieser internen Kontrollsysteme wird befürwortet, jedoch ist eine darüberhinausgehende zentrale Kontrolle nicht erforderlich und daher überschießend. Auch in diesem Zusammenhang erscheint Art. 9 Abs. 2 lit g DSGVO als noch weniger tauglichere Rechtsgrundlage für den geplanten Eingriff.

2. Was die einheitliche Vollziehung betrifft, so ist dies durchaus auch in dezentralen Kontrollsystemen möglich, da gemeinsame Kriterien, wie diese Kontrollen stattfinden sollen, ohne weiteres festgelegt werden können.

3. Völlig unverständlich und wohl zu unerwünschten Ergebnissen führend ist der Umstand, dass diese Kontrolle nur für eine Versichertengruppe verrechtlicht werden soll. Einerseits ist eine solche Vorgangsweise aus Gleichheitsgründen auch in einem verfassungsrechtlichen Spannungsverhältnis zu sehen, andererseits führt dies darüber hinaus zur Konsequenz, dass Kontrollsysteme in den anderen Versicherungsbereichen auf rechtlich unsicherem Grund aufbauen.

4. Nach den vorliegenden Änderungsanordnungen bestehen auch Meldeverpflichtungen dieser Ergebnisse an die Abgabenbehörden des Bundes. So sehr dies bei der Bekämpfung von Sozialbetrug angezeigt erscheint, besteht jedoch bei den Daten der DienstnehmerInnen keinerlei Begründung für diese Datenübermittlung. Eine solche Datenübermittlung hätte daher gänzlich zu entfallen. Dem hat sich auch die Mehrheit der Mitglieder des Datenschutzrates angeschlossen.

5. Es fehlt bei der Struktur der vorgesehenen neuen Kontrolle des DienstnehmerInnenbereiches in vielen Fällen das Verständnis, dass es sich hier um Daten gemäß Art. 9 Abs. 1 DSGVO handelt, da ein großer Bereich Gesundheitsdaten betrifft. Es kann daher nicht auf alten Systemen aufgebaut werden, die dafür entwickelt wurden, Daten zu verarbeiten, die keine sensiblen Inhalte haben. Auch bei den Datensicherheitsmaßnahmen muss dies voll inhaltlich berücksichtigt werden.

6. Ein informierter Vertreter gab in der Debatte an, dass bei den verwendeten Kontrollsystemen anonymisierte Daten genügen. Auch dieser Umstand sollte bei der Gesetzesänderung berücksichtigt werden.

7. Das Büro des Datenschutzrates hat in der vorbereiteten Stellungnahme für das erhebliche öffentliche Interesse ausgeführt, dass dieses wohl vorhanden sei, wenn eine große Zahl von Fällen für die Erschleichung von Versicherungsleistungen durch die Kontrollsysteme aufgezeigt werden kann. Dafür gibt es jedoch auch nach der umfänglichen Diskussion keine Hinweise.

8. Unbestritten und auch von der Mehrheit der Mitglieder des Datenschutzrates so gesehen ist der Umstand, dass im Rahmen des Gesetzwerdungsprozesses keine Datenschutzfolgenabschätzung erstellt wurde, daher eine solche bei einer allfälligen Einführung dieses Systems nachzuliefern wäre.

Schlussbemerkung:
Diese ergänzende Stellungnahme konnte nicht auf die ausgefertigte Stellungnahme eingehen, da eine solche im Abgabezeitpunkt den Verfasserinnen und Verfassern nicht vorgelegen ist.

Wien, 4. Juli 2018