

REPUBLIK ÖSTERREICH  DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ • BKA-817.355/0002-DSR/2015
TELEFON • (+43 1) 53115/2527
FAX • (+43 1) 53115/2702
E-MAIL • DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Arbeit,
Soziales und
Konsumentenschutz

Per Mail:
walter.neubauer@sozialministeri
um.at
VII9@sozialministerium.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem ein Bundesgesetz zur Verbesserung der Sozialbetrugsbekämpfung (Sozialbetrugsbekämpfungsgesetz – SBBG) geschaffen wird sowie das Allgemeine Sozialversicherungsgesetz, das Gewerbliche Sozialversicherungsgesetz, das Bauern-Sozialversicherungsgesetz, das Beamten-Kranken- und Unfallversicherungsgesetz, das Arbeitsvertragsrechts-Anpassungsgesetz, der Artikel III des Bundesgesetzes BGBl. I Nr. 152/2004, das Firmenbuchgesetz, das Bauarbeiter-Urlaubs- und Abfertigungsgesetz, das Insolvenz-Entgeltsicherungsgesetz und das Ausländerbeschäftigungsgesetz geändert werden **Stellungnahme des Datenschutzrates**

Der **Datenschutzrat** hat in seiner **225. Sitzung am 9. Juni 2015 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Durch Sozialbetrug – besonders durch Scheinfirmen in der Baubranche – entgehen der öffentlichen Hand und der Sozialversicherung jährlich Steuern und Sozialversicherungsbeiträge in erheblichem Ausmaß. Bertoffen von derartigen Malversationen sind auch die Bauarbeiter-Urlaubs- und Abfertigungskasse (BUAK)

und der Insolvenz-Entgelt-Fonds. Auch legal operierende Unternehmen leiden unter den Wettbewerbsverzerrungen.

Ein besonderes Phänomen des Sozialbetrugs sind die sogenannten Scheinfirmen. Diese werden dazu verwendet, Lohn- und Sozialabgaben systematisch zu verkürzen. Zu diesem Zweck werden neue Gesellschaften gegründet oder bestehende – und bislang nicht rechtswidrig agierende – Gesellschaften übernommen bzw. verwendet. Sie dienen als Anmelde- und Verrechnungsvehikel, indem sowohl tatsächlich beschäftigte Personen als auch Personen ohne tatsächliche Beschäftigung (bei der Sozialversicherung, der BUAK oder der Finanzbehörde (an)gemeldet werden. Angehörige des letztgenannten Personenkreises erhalten so insbesondere de facto einen umfassenden Versicherungsschutz. Bei Personen, die tatsächlich beschäftigt werden, wird deren wahrer Vertragspartner bzw. Arbeitgeber regelmäßig verschleiert. Auch die missbräuchliche Inanspruchnahme von Krankenständen, die missbräuchliche Verrechnung von Leistungen durch Vertragspartner und auch die unrechtmäßige Verwendung von e-cards stellen Missstände dar und verursachen finanzielle Belastungen der Gebietskrankenkassen in erheblichem Ausmaß. Die missbräuchliche Verwendung der E-Card umfasst sowohl die Verwendung durch Personen, die nur zum Schein bei der Sozialversicherung angemeldet sind (jedoch mangels Beschäftigung nicht pflichtversichert sind [reine Scheinanmeldungen]) als auch durch Personen, die die e-card von versicherten Personen verwenden.

Mit der nun vorgeschlagenen Schaffung eines Sozialbetrugsbekämpfungsgesetzes wird die Zusammenarbeit der vom Sozialbetrug betroffenen und zur Bekämpfung desselben zuständigen Einrichtungen intensiviert. Weiters wird mit diesem Gesetz ein Instrumentarium zur Feststellung der Eigenschaft eines Unternehmens als Scheinunternehmen geschaffen. Die damit verbundenen rechtlichen Konsequenzen in Bezug auf bei Scheinunternehmen als Dienstnehmer angemeldeten Personen finden sich im Allgemeinen Sozialversicherungsgesetz (ASVG), BGBl. Nr. 189/1955. Diese Konsequenzen zielen darauf ab, ein (vermeintliches) Versicherungsverhältnis – inklusive reiner Scheinanmeldungen tatsächlich nicht beschäftigter Personen – zum Scheinunternehmen zu beenden und den wahren Dienstgeber zu eruieren. Von besonderer Bedeutung ist die gesetzliche Verpflichtung zur Durchführung einer Risiko- und Auffälligkeitsanalyse im Dienstgeberbereich – wobei die Oberösterreichische Gebietskrankenkasse bereits ein entsprechendes

Instrumentarium initiiert hat –, die sich mit bestimmten Aspekten des Sozialbetrugs wie etwa Schwarzarbeitsverdacht, Scheinanmeldung, Versichertenströme, Dienstgeberzusammenhänge, Insolvenzgefahr sowie Melde- und Beitragszahlungsverhalten auseinanderzusetzen hat.

Folgende Maßnahmen werden daher im gegenständlichen Entwurf vorgesehen:

Maßnahme 1: Verbesserung und Schaffung neuer Strukturen im Bereich der Zusammenarbeit der zuständigen Einrichtungen und Behörden

Die Einrichtungen und Behörden haben im Rahmen ihres gesetzmäßigen Wirkungsbereichs zur Sozialbetrugsbekämpfung zusammenzuwirken und sich gegenseitig zu unterstützen. Sie sind bei Bedarf verpflichtet, einen Verdacht auf Sozialbetrug den zuständigen Kooperationsstellen möglichst frühzeitig zu melden, für den regelmäßigen Informations- und Erfahrungsaustausch mit anderen Kooperations- und Informationsstellen zu sorgen und ihre Ermittlungen und Amtshandlungen bei der Verfolgung von Verstößen nach Möglichkeit aufeinander abzustimmen sowie bei Sachverhaltsermittlungen und Kontrollen koordiniert vorzugehen. Für Zwecke der Sozialbetrugsbekämpfung wird ein Beirat eingerichtet. Aufgabe des Beirats ist die Verbesserung der Bekämpfung des Sozialbetrugs. Dazu zählen insbesondere die Erörterung von Trends und Entwicklungen sowie Erarbeitung und Bewertung möglicher Maßnahmen zur Verbesserung der Sozialbetrugsbekämpfung sowie die Festlegung gemeinsamer Prioritäten in der Sozialbetrugsbekämpfung.

Maßnahme 2: Identifizierung von Scheinfirmen und Personen und deren Versicherungsverhältnissen, die von den Scheinfirmen zur Sozialversicherung angemeldet werden.

Scheinfirmen werden an Hand einer Reihe von Kriterien vorläufig identifiziert; der sich daraus ergebende Verdacht wird durch Ermittlungen überprüft und gegebenenfalls wird mit Bescheid festgestellt, dass tatsächlich ein Scheinunternehmen vorliegt. Dienstnehmer/innen werden von der Gebietskrankenkasse zur Mitwirkung bei Feststellungen hinsichtlich des Vorliegens des Sozialversicherungsverhältnisses herangezogen. Schlussendlich wird das Vorliegen eines Versicherungsverhältnisses festgestellt oder verneint.

Maßnahme 3: Weitere Zurückdrängung bzw. Eindämmung der unrechtmäßigen e-card Verwendung und der zu Unrecht erfolgten Verrechnungen von Leistungen.

Sozialbetrug – hier die missbräuchliche Verrechnung von Leistungen durch Vertragspartnerinnen und Vertragspartner wie auch die unrechtmäßige Verwendung von e-cards entstehende Schäden – soll in Hinkunft hintangehalten bzw. eingedämmt werden.

a) Um missbräuchliche Inanspruchnahmen der e-card vorzubeugen, soll die bestehende Rechtslage geschärft und die bisher nur bei Zweifeln an der Identität des Patienten oder der Patientin bestehende Pflicht zur Identitätsüberprüfung im spitalsambulanten Bereich dahingehend verschärft werden, dass die Identität des Patienten oder der Patientin in Krankenanstalten nun jedenfalls mittels Ausweiskontrolle zu überprüfen ist. Im niedergelassenen Bereich, wo es bislang ausreichte, dass die Identitätsüberprüfung im Zweifelsfall erfolgt, soll die Überprüfung im Zweifelsfall schon dann erfolgen, wenn der Patient oder die Patientin dem behandelnden Arzt oder der behandelnden Ärztin nicht persönlich bekannt ist.

b) Die Ermöglichung des sogenannten „Mystery Shoppings“ soll der missbräuchlichen Verrechnung von Leistungen präventiv entgegenwirken.

2) Datenschutzrechtlich relevante Bestimmungen

I. Artikel 1 (Sozialbetrugsbekämpfungsgesetz)

Vorbemerkungen

Aus datenschutzrechtlicher Sicht ist festzuhalten, dass der vorliegende Entwurf einen regelmäßigen Informations- und Erfahrungsaustausch mit anderen Kooperations- und Informationsstellen vorsieht. Das sind **Datenanwendungen** iSd § 4 Z 7 DSG 2000 und es handelt sich damit um einen **Eingriff in das Grundrecht auf Datenschutz** nach § 1 Abs. 1 DSG 2000. Ein solcher gesetzlich normierter Eingriff muss im **Interesse der Allgemeinheit** gelegen sein bzw. dem **Gemeinwohl** dienen und **verhältnismäßig** sein (siehe **EuGH-Urteil** vom 8.4.2014, verbundene Rechtssachen C-293/12 und C-594/12 zur Prüfung der Richtlinie über die **Vorratsspeicherung von Daten** (RL 2006/24/EG)).

Der Datenschutzrat hält fest, dass die Bekämpfung von Sozialbetrug dem Gemeinwohl dient und Eingriffe in das Grundrecht sind für diesen Zweck somit

– unter bestimmten Voraussetzungen – zulässig. Die gesetzlichen Rahmenbedingungen für die Zulässigkeit des Eingriffes müssen jedoch entsprechend den datenschutzrechtlichen Vorgaben ausgestaltet werden.

Weiters merkt der Datenschutzrat an, dass die informierten Vertreter in der Sitzung des Datenschutzrates datenschutzrechtliche Nachbesserungen des Entwurfes zugesichert haben. Wobei nach Ansicht des Datenschutzrates speziell beim „Mystery Shopping“ datenschutzrechtliche Rahmenbedingungen sichergestellt werden müssen.

Zu § 4:

a.) Zu der in § 4 Abs. 1 zwischen den **Kooperations- und Informationsstellen** vorgesehenen **Zusammenarbeit** ist vorweg anzumerken, dass – soweit im Zuge der Zusammenarbeit personenbezogene Daten (§ 4 Z 1 DSG 2000) übermittelt werden – die betreffenden Datenarten im Gesetz bezeichnet werden sollten. Gleiches gilt für den in § 4 Abs. 2 Z 2 geregelten Informations- und Erfahrungsaustausch sowie das in § 4 Abs. 2 Z 3 vorgesehene Abstimmen und koordinierte Vorgehen.

Weiters sollte geprüft werden, ob die vorgesehenen – offenbar weitgehenden – Datenübermittlungen allenfalls ein **Informationsverbundsystem** nach § 4 Z 13 DSG 2000 darstellen. Diesfalls müssten neben der Rollenverteilung (wer ist Auftraggeber, wer ist Dienstleister, wer ist Betreiber des Systems) und der Festlegung der Empfängerkreise auch entsprechende Datensicherheitsmaßnahmen nach § 14 DSG 2000 (zB Zutritts- und Zugriffsberechtigung, Protokollierung und Dokumentation) zumindest in Grundzügen im Gesetz festgelegt werden.

b.) Unklar ist, ob der **Sozialbetrugsbekämpfungsbeauftragte** nach § 4 Abs. 3 des Entwurfes ein eigenständiger Auftraggeber (§ 4 Z 4 DSG 2000) ist. Die gleiche Frage stellt sich hinsichtlich des in § 4 Abs. 4 eingerichteten **Beirates**. Dies sollte in den Erläuterungen klargestellt werden.

Wenn diese Einrichtungen **Auftraggeber** sind, müsste die Übermittlung von personenbezogenen Daten an diese Auftraggeber im Gesetz geregelt werden.

c.) Im Hinblick auf den in § 4 Abs. 2 Z 1 geregelten „**Verdacht auf Sozialbetrug**“ sollte näher dargelegt werden, unter welchen Voraussetzungen vom Vorliegen eines Verdachts, an den „frühzeitig“ Meldepflichten geknüpft sind, ausgegangen werden

kann. Gleiches ist hinsichtlich der Anknüpfung an das „Vorliegen eines Sozialbetrugsverdachts“ in § 5 Abs. 1 anzumerken.

Zu § 5:

a.) Aufgrund des in § 1 Abs. 2 DSG 2000 verankerten Verhältnismäßigkeitsgrundsatzes dürfen Daten nur dann verwendet werden, wenn sie zum Erreichen des Zwecks erforderlich sind und kein gelinderes Mittel zu Verfügung steht. Es sollte dementsprechend in den Erläuterungen klarer dargestellt werden, weshalb dieser Datenaustausch zwischen den Staatsanwaltschaften und den Kooperationsstellen **unbedingt erforderlich** ist und es **kein gelinderes Mittel** gibt. Dabei wäre zu berücksichtigen, dass Staatsanwaltschaften insbesondere auch Daten von Personen verarbeiten, bei denen eben noch nicht rechtskräftig festgestellt worden ist, ob sie das angezeigte Delikt tatsächlich begangen haben. Für die Verwendung solcher sogenannter „weicher Daten“ wäre vor allem auch dahingehend Vorsorge zu treffen, dass sie – sofern sich der Verdacht nicht bestätigt – auch bei den Kooperationsstellen gelöscht werden.

Im Lichte dieses Verhältnismäßigkeitsgrundsatzes sollte in § 5 Abs. 1 hinsichtlich der Zurverfügungstellung von erforderlichen Informationen und Daten sowie der Aufzählung der „in Frage kommenden Datenarten“ in der Sozialbetrugsdatenbank nach § 5 Abs. 2 **abschließend** dargelegt werden, welche Datenarten zur Erreichung des Zwecks erforderlich sind.

b.) Unklar erscheint im Hinblick auf die nach § 5 Abs. 2 einzurichtende „Sozialbetrugsdatenbank“, wie das Bundesministerium für Finanzen, das die „Sozialbetrugsdatenbank“ zu führen hat, die in den Z 1 bis 6 leg. cit. angeführten Daten erhält. Im Zusammenhang mit der Einrichtung der Sozialbetrugsdatenbank wird auf die Anmerkungen zu § 4 hinsichtlich der **Rollenverteilung** und der Frage der Einrichtung eines **Informationsverbundsystems** hingewiesen. Bei der Prüfung des Vorliegens eines Informationsverbundsystems sollte berücksichtigt werden, dass bereits in § 5 Abs. 1 ein **Datenaustausch** zwischen Kooperationsstellen und die Staatsanwaltschaften über die Sozialbetrugsdatenbank und in § 5 Abs. 3 entsprechende **Einsichtsrechte** dieser Einrichtungen in die Sozialbetrugsdatenbank vorgesehen sind.

c.) Zu § 5 Abs. 4 sollte näher erläutert werden, weshalb die Aufbewahrung der Daten für fünf Jahre bzw. für zehn Jahre erforderlich ist.

d.) Im Zusammenhang mit der Einrichtung der „Sozialbetrugsdatenbank“ sollten auch notwendige **Datensicherheitsmaßnahmen** nach § 14 DSG 2000 vorgesehen werden. Diese müssten (siehe etwa § 10 des Meldegesetzes 1991 – MeldeG, BGBl. Nr. 9/1992, sowie § 19 Abs. 4 des Vereinsgesetzes 2002 – VerG, BGBl. I Nr. 66/2002) – zumindest in Grundzügen – auf gesetzlicher Ebene determiniert und in der Folge auf Verordnungsebene konkretisiert werden. Durch den informierten Vertreter wurden diesbezügliche Verbesserungen zugesagt.

e.) Im Übrigen wäre – nachdem strafrechtlich relevante Daten zu bloßen Verdachtsfällen ausgetauscht werden – zu überlegen, ob strengere Strafbestimmungen für den Fall des Missbrauchs dieser sogenannten „weichen“ Daten geschaffen werden.

Zu § 6:

Es sollte in § 6 näher dargelegt werden, ob es sich bei der „Hilfe der Finanzstraf- und Abgabenbehörden“ um Amtshilfe handelt.

Zu § 8:

In § 8 sollte dargelegt werden, wer unter den Begriff „Rechtsträger/in“ fällt und zu welchem Zweck die IEF-Service GmbH nach § 8 Abs. 4 bereits über das Bestehen eines Verdachts informiert wird.

Dargelegt werden sollte auch, in welchen Fällen der rechtskräftige Bescheid (bzw. das Erkenntnis des Verwaltungsgerichts) nach § 8 Abs. 8 und 9 dem Baustellenkoordinator „**allfällig**“ zu übermitteln ist. Weiters sollte der Zweck des Anschlages des Bescheides bzw. des Erkenntnisses präzisiert werden. Unklar erscheint überdies, was unter einem „für **alle** Personen zugänglichen Ort der Baustelle“ gemeint ist, insbesondere ob dieser Anschlag auch solchen Personen, die nicht auf der Baustelle beschäftigt sind, zugänglich sein muss.

II. Artikel 2 (Änderung des Allgemeinen Sozialversicherungsgesetzes)

Zu Z 3 (§ 32a):

Im Hinblick auf die Ausstellung von e-cards für Prüforgane des Versicherungsträgers nach § 32a ist aufgrund des § 31a Abs. 4 ASVG der **Datenschutzrat** anzuhören.

Zu Z 5 (§ 35a):

Zu § 35a sollte – zumal daran eine Übermittlung von Daten geknüpft ist – näher erläutert werden, wann eine entsprechende „Vermutung“ des Vorliegens eines Scheinunternehmens angenommen werden kann.

Zu Z 7 (§ 42 Abs. 1a):

Hinsichtlich des in § 42 Abs. 1a genannten Verdachts auf das Vorliegen eines Verhaltens, das Sozialbetrug im Sinne des § 2 SBBG darstellt, wird auf die Ausführungen zu Art. 1 § 4 verwiesen.

Zu Z 8 (§ 42b):

Vorweg sollte in § 42b Abs. 1 klarer geregelt werden, wer **Auftraggeber der Risiko- und Auffälligkeitsanalyse** ist, **welche Daten** dafür verwendet werden bzw. **woher** diese Daten stammen und ob diese Daten zum Zweck der Risiko- und Auffälligkeitsanalyse von jedem Krankenversicherungsträger **alleine** oder von allen Krankenversicherungsträgern **gemeinsam** – allenfalls in Form eines **Informationsverbundsystems** – verarbeitet werden.

Weiters sollte klargestellt werden, ob die **Oberösterreichische Gebietskrankenkasse** nach § 42b Abs. 2 „als Kompetenzzentrum“ in der Rolle eines eigenständigen Auftraggebers oder allenfalls nur als Dienstleister (§ 4 Z 5 DSG 2000) tätig wird. Unklar erscheint auch, welche Daten hierbei konkret zu welchen Zwecken **verknüpft** werden und wer diese Daten an die **Oberösterreichische Gebietskrankenkasse** übermittelt oder überlässt. Auch sollte zumindest näher erläutert werden, welche Daten im Rahmen der **Ergebnisse** dieser Verknüpfung übermittelt werden.

Darüber hinaus hält der Datenschutzrat ausdrücklich fest, dass für die Vornahme dieses „Data Mining“ eine entsprechende datenschutzrechtlich-konforme Regelung im Gesetz geschaffen werden muss.

Zu den Z 16 (§ 148 Z 6), Z 17 (§ 149 Abs. 2) und 19 (§ 342 Abs. 1 Z 3):

Fraglich erscheint, ob im Rahmen der Prüfung der Identität des Patienten auch Daten erhoben bzw. gespeichert werden (zB die ausstellende Behörde des Lichtbildausweises sowie die Ausweisnummer), um die erfolgte Durchführung der

Identitätsüberprüfung zu dokumentieren. Im Zusammenhang mit der Dokumentation wird auf den Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000 hingewiesen.

III. Artikel 3 (Änderung des Gewerblichen Sozialversicherungsgesetzes)

Zu Z 1 (§ 98 Abs. 2):

Hinsichtlich der Prüfung der Identität des Patienten wird auf die Anmerkungen zu Art. 2 Z 16, 17 und 19 verwiesen.

IV. Artikel 4 (Änderung des Bauern-Sozialversicherungsgesetzes)

Zu Z 1 (§ 92 Abs. 2):

Hinsichtlich der Prüfung der Identität des Patienten wird auf die Anmerkungen zu Art. 2 Z 16, 17 und 19 verwiesen.

V. Artikel 9 (Änderung des Bauarbeiter-Urlaubs- und Abfertigungsgesetz)

Zu Z 4 (§ 31a Abs. 1a):

Auffällig erscheint, dass nach § 31a Abs. 1a **nur** die „BUAK“ zur Verarbeitung der Daten in der **Baustellendatenbank** ermächtigt ist, während nach § 31a Abs. 1 des Bauarbeiter-Urlaubs- und Abfertigungsgesetzes (BUAG), BGBl. Nr. 414/1972, die Urlaubs- und Abfertigungskasse und die Arbeitsinspektion **gemeinsamer** Auftraggeber der Baustellendatenbank sind. Im Lichte dessen sollte nochmals überdacht werden, wem die Auftraggebereigenschaft der in der Baustellendatenbank verarbeiteten Daten tatsächlich zukommt und eine entsprechend eindeutige Regelung getroffen werden.

Im Übrigen sollten die in der Baustellendatenbank zu erfassenden Daten abschließend aufgezählt werden.

10. Juni 2015
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt