SGB | USS
www.sgb.ch | www.uss.ch
Schweizerischer Gewerkschaftsbund
Union syndicale suisse
Unione sindacale svizzera

Bundesamt für Justiz

jonas.amstutz@bj.admin.ch

Bern, 07. April 2017

Vernehmlassungsverfahren: Totalrevision des Datenschutzgesetzes (DSG)

Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit, an der oben genannten Vernehmlassung teilnehmen zu dürfen.

Grundsätzliches

Die vielen Anfragen sowohl an die Rechtsdienste der Gewerkschaften wie auch an den Eidg. Datenschutzbeauftragten (EDÖB)[1] zeigen, dass sehr häufig weder den Arbeitgebern noch den Arbeitnehmern klar ist, was wirklich zulässig ist. Das hat u.a. mit der wenig klaren Sprache des heutigen DSG zu tun. Leider verpasst es die nun vorliegende Totalrevision, klare und spezifische Bestimmungen für Arbeitgeber und Arbeitnehmende zu erlassen. Damit hat es der Gesetzgeber verpasst, Rechtssicherheit in diesem Bereich zu schaffen.

Der SGB fordert deshalb im Rahmen der Überarbeitung der Vorlage, den Datenschutz am Arbeitsplatz spezifischer zu regeln bzw. beispielhaft anzugeben, welche Artikel am Arbeitsplatz wie umgesetzt werden müssen. Insbesondere müssen für die Videoüberwachung, Internet- und Email- sowie Telefonüberwachung klare Vorgaben im Gesetz gemacht werden. Aber auch neue Formen der möglichen (Big-Data-)Überwachung wie z.B. der "refraktiven Überwachung" von Arbeitnehmenden.[2] Somit würde auch gesetzessystematisch Kongruenz zwischen dem DSG und Art. 26 der Verordnung 3 zum Arbeitsgesetz (ArGV3) hergestellt werden.

Grundsätzlich muss ein revidiertes DSG auch die Datenhoheit der Arbeitnehmenden statuieren – auch dies ist in der Überarbeitung der Vorlage nachzuholen. Jeder Arbeitnehmende muss das Recht haben, über das Erheben der persönlichen Daten proaktiv informiert zu werden und dieses einzuschränken sowie zu bestimmen, was die Unternehmen mit seinen persönlichen digitalen Daten machen dürfen und was nicht.

[1] Vgl. bspw. Tätigkeitsbericht EDÖGB https://www.edoeb.admin.ch/dokumentation/00153/00154/00165/index.html?lang=de
[2] Zur refraktiven Datenüberwachung am Arbeitsplatz vgl. statt vieler https://hbr.org/2016/08/the-unintended-consequence-of-customer-data-collection .

Monbijoustrasse 61, 3007 Bern / Postfach, 3000 Bern 23
031 377 01 01, Fax: 031 377 01 02, info@sgb.ch, info@uss.ch

Zu den einzelnen Artikeln

Art. 2 – Räumlicher und persönlicher Geltungsbereich

Der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) sieht keine besondere Bestimmung zum räumlichen Geltungsbereich vor. Nach Auffassung des Bundesrates würde bereits das geltende Recht die Möglichkeit bieten, das Gesetz weitgehend auf Situationen mit internationalem Charakter anzuwenden. Er verweist hierzu auf das Bundesgerichtsurteil zu "Google Street View". In diesem Urteil ist, wie vom Bundesrat erwähnt, ein überwiegender Anknüpfungspunkt in der Schweiz gegeben, da Google Inc. mit Hilfe von Google Switzerland GmbH Bilder von Strassenzügen in der Schweiz aufnehmen liess. Diese Situation ist jedoch nicht mit Datenbearbeitern und Inhabern von Datensammlungen – nach heutiger Terminologie – vergleichbar, die komplett aus dem Ausland operieren, sich aber an Arbeitnehmende in der Schweiz richten. Zu erwähnen sind etwa Plattformen wie Amazon Turk, Uber oder andere Arbeitgeber im Bereich spezifischer Telearbeitsformen. Es ist hier aber auch an Tools zu denken, die im Arbeitsverhältnis, z.B. im Büro, zum Einsatz kommen, und die ebenfalls komplett aus dem Ausland operieren: Bspw. Amazon Web Services, Skype, Google Docs, Microsoft (unter anderem mit Office 365), Salesforce, etc.

In all diesen Fällen kann das schweizerische Datenschutzgesetz weiterhin nicht ohne Weiteres angewendet werden. Die Auffassung des Bundesrates, das geltende Recht biete bereits die Möglichkeit, das DSG weitgehend auf Situationen mit internationalem Charakter anzuwenden, lässt sich denn auch in der gängigen Praxis nicht nachvollziehen. Ein entsprechendes Marktortprinzip muss daher vorgesehen werden.

Der vorliegende Entwurf weist eine grosse Neuerung beim persönlichen Geltungsbereich auf: Der Schutz juristischer Personen fällt weg. Erfasst sein soll neu nur noch die Bearbeitung von Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Der SGB ist damit nicht einverstanden. Die Geschichte zeigt, dass auch juristische Personen wie Gewerkschaften oder Vereine Opfer zweifelhafter Datenbearbeitung sein können. Der Ausschluss der juristischen Personen vom Schutzbereich des DSG ist auch weder systemtreu noch wirklich konsequent. Nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB), welcher durch das DSG konkretisiert wird, geniessen auch juristische Personen Persönlichkeitsschutz, und sie tun es weiterhin; Art. 13 der Bundesverfassung (BV) gewährleistet den Schutz der Persönlichkeit auch von juristischen Personen. Diesen soll u.E. deshalb ein eigenständiger Schutz sowie Aktivlegitimation zustehen. Es muss deshalb auch juristischen Personen der Schutz des Gesetzes gewährt werden.

Art. 3 – Begriffe

Die Streichung des Begriffs und des Konzepts der "Datensammlung" wird ausdrücklich begrüsst. Entscheidend ist die Erschliessbarkeit der Daten: Alle Informationen über eine bestimmte Person, die mit einem vernünftigen Aufwand gefunden werden können, müssen als personenbezogene Daten gelten – unabhängig vom Speicherverfahren oder dem Speicherort.

Ebenfalls scheint begrüssenswert, dass der Begriff "Persönlichkeitsprofil" durch "Profiling" ersetzt wird. Die Begriffe sind allerdings nicht deckungsgleich. Wichtig ist, dass der Zweck der Datenbearbeitung durch den Begriff erfasst bleibt, der darauf abzielt, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Der SGB begrüsst grundsätzlich den vorliegenden Ersatz des bis heute unklaren Begriffs des "Persönlichkeitsprofils" (als "gefähr-

liche" Art von Daten) durch das "Profiling" (als "gefährliche" Art des Bearbeitens von Daten). Jedoch ist es ungenügend, wenn dann im bereichsspezifischen Datenschutzrecht (in den anzupassenden Bundesgesetzen) mit Blankettermächtigungen das Profiling quasi "durchgewinkt" wird. Zu fordern ist, dass klare und strenge Rahmenbedingungen für das Profiling in den Bundesgesetzen konkretisiert werden, insbesondere für das Profiling von Arbeitnehmenden durch den Arbeitgeber.

Der Begriff des Profiling muss nämlich sowohl traditionelle wie auch neuartige mögliche Formen der unerwünschten Überwachung am Arbeitsplatz beinhalten, welche z.B. durch Auswertung von Big Data und anderen Datenvolumen am Arbeitsplatz anfallen.

Weiter ist auch der Begriff der "biometrischen Daten" missverständlich. Auch in den Erläuterungen wird er nicht geklärt: Ein Gesichtsbild oder die Stimme sind grundsätzlich auch "biometrisches Daten", sollen aber hier nicht als Unterkategorie der besonders schützenswerten Personendaten erfasst werden. Deshalb ist die folgende Definition aufzunehmen:

"Ziff. 4. mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten)".

Weiter lassen biometrische Merkmale nicht immer eine eindeutige Identifizierung zu. Zudem werden die Möglichkeiten zur automatisierten Erkennung von Personen aufgrund ihrer Stimme, dem Aussehen oder der Art der Fortbewegung noch massiv zunehmen und sind heute schon am Arbeitsplatz gang und gäbe und sehr problematisch: So werden in der Logistik Bewegungsmuster von Logistik-Mitarbeitern oder Kurieren automatisch gespeichert und dem Arbeitgeber in Echtzeit übermittelt; oder automatische, durch Algorithmen ausgeführte Stimmkontrollen in Callcentern gemacht. Wenn folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation, zur Messung der Abläufe bzw. gar zur Bewertung der Mitarbeitenden bearbeitet werden, müssen sie als besonders schützenswerte Personendaten gelten.

Das Wort "eindeutig" ist daher zu streichen.

Art. 4 Abs. 2 – Verhältnismässigkeit

"Datenvermeidung" und "Datensparsamkeit" fehlen als explizite Grundkonzepte und als Teil der notwendigen Verhältnismässigkeit (s. Art. 4 Abs. 6). Gerade Arbeitgeber tendieren häufig dazu, unnötig Daten von Arbeitnehmenden zu sammeln, z.B. die Online-Tätigkeit im Home-Office, die je nach Verwendung des Computers oder bestimmter Programme dem Arbeitgeber mitgeteilt wird, ohne dass der Arbeitnehmende dies verhindern kann.

Der Absatz ist zu ergänzen mit: "Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahingehend auszurichten, dass so wenig personenbezogene Daten wie möglich von der Bearbeitung betroffen sind."

Art. 4 Abs. 3 – Zweckbestimmung

Da die Weiterverarbeitung von Personendaten zu kompatiblen Zwecken erlaubt sein soll, muss der Zweck – wie im Vorentwurf vorgesehen – für die betroffene Person klar erkennbar sein.

An der Bestimmung soll – wie im Vorentwurf vorgesehen – festgehalten werden.

Art. 4 Abs. 6 – Einwilligung

Die Bestimmung ist nur zusammen mit den Grundsätzen der Datenvermeidung und der Datensparsamkeit wirksam. Dies zeigen aktuelle Beispiele:

Ein „Cookies-Balken" oder eine Kommunikations-Software auf einem portablen Computer, auf welchem der Arbeitnehmer z.B. auch von zuhause aus arbeitet, der nicht abgelehnt oder ausgeschaltet werden kann, ist für die betroffene Person inakzeptabel. Es muss jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen gerade Personen in einem Abhängigkeitsverhältnis wie Arbeitnehmende vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden. Es darf nicht sein, dass Arbeitnehmende dem Arbeitgeber mit Pauschalvollmachten das Recht zur freien Überwachung geben. Dies gilt z.B. auch bei der Aufnahme in eine Kranken- oder Unfallversicherung oder Pensionskasse

An den Grundsätzen der Datenvermeidung und der Datensparsamkeit muss entsprechend festgehalten werden. Es darf auch nicht bereits davon ausgegangen werden, dass eine ausdrückliche Einwilligung vorliegt, wenn bspw. ein entsprechendes (Software-Dialog-)Kästchen – womöglich mit einer missverständlichen Beschriftung – bereits vorausgefüllt ist und auf die Schaltfläche "weiter" geklickt wird. Eine Verdeutlichung in Art. 4. Abs. 2 ist daher vorzunehmen.

Art. 8 – Empfehlungen der guten Praxis

Das Prinzip der "Empfehlungen der guten Praxis" wird begrüsst. Dieser Vorschlag ist insbesondere einer (alleinigen) Selbstregulierung durch die Branchen vorzuziehen, da erst der Einbezug interessierter und betroffener Kreise, d. h. sowohl der Anwender wie auch der Anbieter von Produkten und Dienstleistungen, zu angemessenen Regelungen der Empfehlungen der guten Praxis führen.

Art. 11 – Sicherheit von Personendaten

Der Artikel im Vorentwurf ist wie der bestehende Art. 7 DSG vage. Er hält insbesondere keine Schutzziele fest. Der SGB erwartet vom Bundesrat, dass die Schutzziele explizit im Gesetz zu erwähnen und die konkreten technischen Massnahmen in der Verordnung präzise vorzuschreiben sind.

Art. 15 Abs. 1 – Informationspflicht bei einer automatisierten Einzelentscheidung

Von Bedeutung ist diese Regelung vor allem im Privatrecht, also u.a. im Arbeitsrechtsverhältnis. Diese kann bei den oben erwähnten elektronischen bzw. Big-Data-Überwachungen zum Zuge kommen. Zum einen ist deshalb die Regelung (ohne Abs. 3) in den Abschnitt zum Datenbearbeiten durch Private zu verschieben.

Weiter ist zu befürchten, dass in der Praxis von einer Information über eine automatisierte Einzelentscheidung abgesehen werden dürfte, wenn eine rein theoretische Möglichkeit zur Einflussnahme besteht. Falls nicht, könnte sie gar zur Umgehung geschaffen werden.

In den nicht offensichtlichen Fehlbeurteilungen ist zudem nur die betroffene Person in der Lage, die Richtigkeit der automatisierten Einzelentscheidung abzuschätzen. Die Auswirkungen können aber dennoch erheblich sein. Das Wort "ausschliesslich" ist daher zu streichen.

Art. 15 Abs. 2 – Anhörungspflicht bei einer automatisierten Einzelentscheidung

Die betroffene Person muss sich nicht nur zur automatisierten Einzelentscheidung und den bearbeiteten Daten äussern können. Sie muss sich gegebenenfalls auch ein Bild des angewandten Verfahrens machen können. Da dies sinngemäss auch für das Profiling im Sinne von Art. 3 lit. f gelten muss, ist eine Regelung in der Auskunftspflicht nach Art. 20 vorzusehen.

Art. 16 – Datenschutz-Folgenabschätzung

Die Regelung der Datenschutz-Folgeabschätzung wird begrüsst. Dies entspricht dem gewählten, ausdrücklich risikobasierten Ansatz im revidierten DSG.

Art. 16 Abs. 5 (neu) – Periodische und rückwirkende Datenschutz-Folgenabschätzung

Eine einmalige Datenschutz-Folgeabschätzung ist in einem schnell ändernden Umfeld ungenügend. Es gilt explizit festzuhalten, dass diese periodisch oder bei Änderung der Risiken erneut vorzunehmen sei. Dies muss gerade angesichts der sich ständig ändernden digitalen Arbeitswelt gelten.

Art. 16 Abs. 1, 3, 4 sowie 5 (neu) – Datenschutz-Folgeabschätzung für Gesetzeserlasse i.V.m. Art. 59 lit. a

Nicht nur private Verantwortliche oder Bundesorgane sollen zu Datenschutz-Folgeabschätzungen verpflichtet werden. Bereits beim Erlass neuer Gesetze muss dem Datenschutz und dem Schutz der Persönlichkeitsrechte mehr Beachtung geschenkt werden. Entsprechend ist auch in diesen Fällen eine Datenschutz-Folgeabschätzung zu erstellen und bei Änderungen zu wiederholen.

Auch diese Datenschutz-Folgenabschätzungen müssen rückwirkend für bereits bestehende Gesetze (spätestens fünf Jahre nach Inkrafttreten des DSG) durchgeführt werden:

“[...] der Verantwortliche oder der Auftragsbearbeiter” ist jeweils zu ergänzen: “der Verantwortliche, der Auftragsbearbeiter oder Gesetzgeber”.

Dies ist insbesondere für Gesetze im Bereich des Arbeitsrechts zu machen.

Art. 16 Abs. 6 (neu): Evaluation von Gesetzeserlassen

Gesetze, welche eine Überwachung von Personen beinhalten, werden mit einem “Verfallsdatum” versehen. Sie müssen nach den ersten fünf Jahren seit Inkrafttreten zwingend einer Evaluation, welche die Wirksamkeit und Verhältnismässigkeit prüft, unterzogen werden. Das Resultat bestimmt darüber, ob das Gesetz weiter angewendet werden kann. Wir schlagen daher folgende Ergänzung vor:

“Handelt es sich um ein Gesetz, welches eine Überwachung von Personen beinhaltet, ist es auf eine Anwendungsdauer von fünf Jahren zu beschränken. Eine Evaluation der Wirksamkeit und Verhältnismässigkeit bestimmt darüber, ob das Gesetz weiter angewendet werden darf.”

Alternativ kann das Resultat der Evaluation auch als Grundlage für eine zwingende Neuberatung durch das Parlament verwendet werden.

Art. 19 lit. a – Weitere Pflichten

Gemäss dem erläuternden Bericht wird dadurch für Private die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren. Dies ist für den SGB nicht akzeptabel.

Vielmehr muss weiterhin über eine Registrierung nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden.

Art. 20 – Auskunftsrecht

Das Auskunftsrecht ist ein zentrales Element des Datenschutzes und schafft die Grundlage für die Durchsetzung weiterer Rechtsansprüche der betroffenen Personen.

Art. 20 Abs. 1 – Auskunftsrecht und Kosten

Der SGB begrüsst diese Bestimmung. Die Auskunft ist zu Recht kostenlos vom Verantwortlichen zu leisten.

Art. 20 Abs. 2 lit. c – Auskunftsrecht zur Rechtsgrundlage

Gegenüber der Bestimmung im geltenden DSG wurden hinsichtlich des Auskunftsrechts die Angaben zur Rechtsgrundlage gestrichen. In den Erläuterungen lässt sich keine Begründung hierzu finden. Eine Angabe zur Rechtsgrundlage dient dazu, dass die betroffene Person ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.

Wir schlagen daher vor, lit. c. zu ergänzen: "…der Zweck der Bearbeitung und die Rechtsgrundlage;"

Art. 20 Abs. 2 lit. g – Auskunftsrecht und Informationspflicht

Zur Erfüllung der Informationspflicht ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger gemäss Art. 13 Abs. 3 und 4 ausreichend. Die Auskunftspflicht hingegen muss neben den Daten auch die Empfänger der Daten – und nicht nur deren Kategorien umfassen. Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher sinnvoll.

Lit. g und h (neu) sind wie folgt zu formulieren:

"g. gegebenenfalls Empfängerinnen und Empfänger der Personendaten;

h. gegebenenfalls die Identität und Kontaktdaten des Auftragsbearbeiters der Personendaten."

Art. 20 Abs. 3 – Auskunftsrecht und Entscheidungen

Bereits heute finden massenhaft automatisierte Einzelentscheidungen – die ausschliesslich auf Algorithmen beruhen und ohne menschliches Eingreifen getroffen werden – auf Grund von Personendaten, die z.B. gewisse Arbeitsmuster und Abläufe der Arbeitnehmenden registrieren, statt.

In Zukunft werden noch viel mehr persönliche Daten aus der Leistungsmessung, über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten zur automatisierten Auswertung zur Verfügung stehen.

Für die Nachvollziehbarkeit sind Informationen über die verwendeten Algorithmen wichtig. Die Bestimmung greift daher zu kurz und muss grundsätzlich ein Auskunftsrecht über die Bearbeitung mit Algorithmen enthalten. Die Mechanismustransparenz muss in geeigneter Form (beschreibend oder als Algorithmus selber) erfolgen.

Neue Formulierung für Art. 20 Abs. 3:

“Werden Personendaten automatisiert bearbeitet, erhält die betroffene Person das Ergebnis und Informationen über das Zustandekommen des Ergebnisses, bei einer automatisierten Einzelentscheidung zusätzlich die Auswirkungen der Entscheidung, mitgeteilt.”

Art. 20 Abs. 7, 8, 9 und 10 (neu) – Datenauskunft und Daten Portabilität

Bis anhin ist es für Betroffene nur umständlich und mit viel zeitlichem Aufwand möglich, das Datenauskunftsrecht wahrzunehmen. Die Anfragen werden von den Verantwortlichen oft (lange) ignoriert, unvollständig gewährt und beinhalten lediglich einige ausgedruckte Screenshots. Auch die neuen Bestimmungen zum Auskunftsrecht enthalten keine zeitlichen und formellen Vorgaben, keine Pflicht zur Vollständigkeitsbestätigung und keine Angaben zu den Rechten der Betroffenen, einschliesslich Angaben entsprechend einer Rechtsmittelbelehrung. Diese wären zum Ausgleich des Machtgefälles wichtig.

Das Recht auf Datenportabilität ist im vorliegenden Entwurf nicht vorgesehen. Dies ist unverständlich. Wir schlagen folgende Ergänzungen vor:

Abs. 7 (neu): “Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt. Ist die Informationsbeschaffung mit unverhältnismässigem Aufwand verbunden, erhält die betroffene Person nach spätestens 30 Tagen eine Übersicht zu den Kategorien und dem Zweck der bearbeiteten Daten. Die betroffene Person bestimmt, zu welchen Kategorien die vollständige Auskunft zu erteilen ist.”

Abs. 8 (neu): “Die Auskunft hat in der Regel elektronisch und in einem Format zu erfolgen, das sich zur Weiterverarbeitung eignet, es sei denn die Bearbeitung der Daten findet nicht elektronisch statt.”

Abs. 9 (neu): “Die Vollständigkeit und Korrektheit der Datenauskunft ist zu bestätigen.”

Abs. 10 (neu): “Die Datenauskunft enthält Angaben zu den Betroffenenrechten.”

Art. 25 – Rechtsansprüche

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze. Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 “Strafbestimmungen” vorzusehen (siehe Art. 50).

Bei Verstössen gegen das Datenschutzrecht ist in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen, z.B. einzelner Arbeitnehmenden, ist u.E. nicht relevant. Anstatt Strafrecht anzuwenden, wären u.E. eher Verwaltungssanktionen vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 25 Abs. 4 (neu) – Verbands- und Sammelklagen

Bereits heute kann sich der Beauftragte aufgrund knapper Ressourcen nur auf wenige exemplarische Fälle von (möglichen) Datenschutzverletzungen konzentrieren. Mit dem totalrevidierten Datenschutzgesetz sollen dem Beauftragten neue Aufgaben zufallen. Gleichzeitig dürften die Ressourcen nicht nennenswert aufgestockt werden.

Auch mit dem neuen Gesetz bleibt die Grundschwierigkeit bestehen, die zustehenden Rechte in der Praxis durchsetzen zu können. In Art. 25 ist zum Beispiel nicht vorgesehen, dass Verstösse

gegen den Kernbereich des Datenschutzes der Schwere entsprechend sanktioniert werden können.

Als Arbeitnehmer in einem Abhängigkeitsverhältnis ist es schwierig gegen (mögliche) Datenschutzverstösse vorzugehen. Ein wirkungsvolles Mittel wäre eine Regelung zur kollektiven Rechtsdurchsetzung (Erweiterung des Verbandsklagerechts und Einführung einer Sammelklage bzw. eines Sammelvergleichs).

Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbandsklagerecht und Sammelklage), analog beispielsweise zum Arbeitsgesetz etc., vorgesehen sein. Gewerkschaften müssen die Möglichkeit haben, gemäss DSG zu klagen, wenn die Interessen von Arbeitnehmenden tangiert wurden.

Art. 25 Abs. 4 (neu): "Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Arbeitnehmerschutz bzw. Datenschutz widmen."

Art. 25 Abs. 5 (neu) – Beweislastumkehr

Eine unrechtmässige Bearbeitung von Daten ist nur schwierig und/oder in einem langwierigen Verfahren nachzuweisen, wenn zur Klärung des Sachverhalts die Mitarbeit und Informationen der beschuldigten Partei notwendig sind. In schwerwiegenden Fällen muss die Beweislast daher umgedreht werden.

Der Anbieter ist zu einer angemessenen Mithilfe zu verpflichten. Den Beweis einer rechtmässigen Bearbeitung kann durch den Verantwortlichen beispielsweise durch Darlegung der Einhaltung von Empfehlungen der guten Praxis erbracht werden. Andernfalls muss davon ausgegangen werden, dass eine unrechtmässige Bearbeitung vorliegt. Daher schlagen wir folgende Präzisierung vor:

"Besteht der Verdacht auf eine schwerwiegende und systematische Verletzung der Persönlichkeit, ist der Verantwortliche verpflichtet, die rechtmässige Bearbeitung der Daten nachzuweisen."

Art. 41 – Untersuchung

Die erweiterten Untersuchungsbefugnisse werden begrüsst. Der anzeigenden Person sollte ein Recht auf einen Entscheid und eine Anfechtmöglichkeit zugestanden werden:

Abs. 1: "Der Beauftragte eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte."

Abs. 5: Ist verbindlicher zu formulieren und eine Behandlungsfrist festzuhalten.

Art. 50 bis 52 - Strafbestimmungen

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze gemäss Art. 25. Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 "Strafbestimmungen" vorzusehen.

Bei Verstössen gegen das Datenschutzrecht ist ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner, abhängiger Personen wie Arbeitnehmer ist nicht relevant. Dies ist so zu präzisieren.

Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen.

Art. 52 – Verletzung der beruflichen Schweigepflicht

Der SGB lehnt diese Bestimmung mit Bestimmtheit ab.

Mit der Bestimmung würde (im Bereich der Personendaten) ein Tatbestand für Mitarbeiter von Privatfirmen geschaffen, welcher der Amtsgeheimnisverletzung bei staatlichen Angestellten entspricht. Dies wird negative Auswirkungen für Informanten (Whistleblower) haben, welche berechtigterweise auf Missstände in ihren Unternehmen aufmerksam machen wollen. Wir lehnen die neue Bestimmung deshalb ab.

Zivilprozessordnung (ZPO)

Die Erleichterungen für die private Rechtsdurchsetzung durch den Verzicht auf Gerichtskosten und Leistung einer Sicherheit werden begrüsst.

Besten Dank für die Berücksichtigung der oben gemachten Ausführungen.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

Paul Rechsteiner
Präsident

Luca Cirigliano
Zentralsekretär