scienceINDUSTRIES
SWITZERLAND

Eidgenössiches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

scienceindustries
Wirtschaftsverband Chemie Pharma Biotech

Nordstrasse 15 · Postfach · 8021 Zürich
info@scienceindustries.ch
T +41 44 368 17 11
F +41 44 368 17 70

Zürich, 30. März 2017

Vorentwurf zum Bundesgesetz über den Datenschutz
Stellungnahme von scienceindustries

Sehr geehrte Damen und Herren

Wir beziehen uns auf den erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) sowie die Änderungen weiterer Erlasse zum Datenschutz und danken Ihnen für die Gelegenheit, dazu Stellung nehmen zu können.

scienceindustries ist der Schweizer Wirtschaftsverband Chemie Pharma Biotech. Sie vertritt die wirtschaftspolitischen Interessen von mehr als 250 in der Schweiz tätigen in- und ausländischen Unternehmen aus genannten und verwandten Branchen. Unsere Mitgliedunternehmen, darunter nicht weniger als sechs SMI- und zahlreiche andere kotierte Firmen, beschäftigen in der Schweiz rund 70‘000 Mitarbeitende und leisten einen sehr wesentlichen Beitrag zum Wohlstand unseres Landes: rund 45% aller Schweizer Exporte stammen von ihnen und 40% der gesamten privatwirtschaftlichen Investitionen in Forschung und Entwicklung in der Schweiz werden von unseren Mitgliedfirmen getätigt. Die überwiegende Mehrheit unserer Mitgliedunternehmen sind global tätig, erzielen dabei im Schnitt rund 98% ihrer Umsätze im Ausland und beschäftigen dort zusätzlich über 320‘000 Mitarbeitende. Die vielfältigen Aktivitäten unserer Industrie führen zwangsläufig zu mannigfachen Datenbearbeitungen sowie zu einem regen Datenaustausch im In- wie Ausland resp. auch grenzüberschreitend. Die Thematik ist entsprechend von eminenter Bedeutung für alle unsere Mitgliedfirmen: eine pragmatische Regelung ist dabei genauso anzustreben, wie auch gleichzeitig eine international kompatible Lösung, die einen reibungslosen Datenaustausch in andere Länder garantiert.

Klärend sei an dieser Stelle festgehalten, dass die vorliegende Stellungnahme aus Rücksicht auf die unmittelbare Betroffenheit der Unternehmen sowie die vorhandene Expertise nur auf den Vorentwurf zum Bundesgesetz über den Datenschutz (das DSG) und hierbei ausschliesslich auf jene Regelungen eingeht, welche die Privatwirtschaft direkt betreffen. Zu den übrigen sich in Revision befindlichen Rechtserlassen resp. Bestimmungen werden wir uns nicht äussern.

Äquivalenz als Massstab

Die Mitgliedfirmen von scienceindustries betreiben ein internationales Geschäft und finden sich dabei in einem sehr kompetitiven Umfeld wieder. Entsprechend wichtig ist es, dass die Rahmenbedingungen am Standort, wo die Firmen einen wesentlichen Teil ihrer Wertschöpfung erzielen, ein erfolgreiches Wirtschaften ermöglichen. Das Datenschutzrecht beschlägt zahlreiche Aktivitäten der Firmen und entfaltet somit direkte Auswirkungen auf die Rahmenbedingungen des Wirtschaftsstandortes, wobei das Schweizer Datenschutzkonzept sich bislang über weite Strecken bewährt hat. Im Bewusstsein um die Wichtigkeit des Themas sprechen sich unsere Mitgliedfirmen für einen angemessenen Datenschutz aus und setzen die entsprechenden Vorgaben in ihren Unternehmen um, was bereits heute einen beachtlichen Aufwand verursacht. Entsprechend gilt es Augenmass zu halten und inskünftig keine Regelungen einzuführen, die bei den Firmen zu weiteren grossen Aufwendungen führen, ohne dass gleichzeitig ein berechtigter Nutzen für die schutzbezogenen Personen resultiert. Auch bietet die Totalrevision die Gelegenheit, gewisse Regelungen im bestehenden Datenschutzgesetz, die sich nicht bewährt haben, zu überdenken und anzupassen.

Nach Ansicht von scienceindustries hat sich die Revision des DSG weitgehend auf das Notwendige zu beschränken und sich dabei an der Kompatibilität mit grundlegenden internationalen Vorgaben (insbes. das Übereinkommen SEV 108 sowie die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten) zu orientieren. Die grundsätzliche Äquivalenz des Schweizer Datenschutzniveaus mit diesen Vorgaben ist vor allem mit Blick auf die Fortführung des heute schon bestehenden Angemessenheitsbeschlusses durch die Kommission der Europäischen Union (EU) gerade für den grenzüberschreitenden Datenaustausch von zentraler Bedeutung. Ein revidiertes DSG muss diesen Anforderungen genügen, soll indes aus unserer Sicht nicht darüber hinausgehen und gleichzeitig bestehende Freiräume ausschöpfen.

Zentrale Anliegen der Lifescience-Industrie

- **Der Grundsatz der lex specialis ist umfassend zu verstehen: bereichsspezifische Datenschutzbestimmungen auf Gesetzes- sowie auf Verordnungsstufe müssen auch inskünftig dem DSG stets vorgehen, was insbes. für die Humanforschung von Bedeutung ist.**
- **Die Begriffe genetische wie biometrische Daten sind zu präzisieren sowie der gewählte Ansatz zum Profiling zu überarbeiten.**
- **Die Informations- und Auskunftspflichten müssen überarbeitet werden.**
- **Das Konzept des unabhängigen internen Datenschutzbeauftragten ist beizubehalten und damit verbunden sind Erleichterungen für die Verantwortlichen vorzusehen.**
- **Es sind Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen vorzusehen.**
- **Das Sanktionssystem ist in wesentlichen Teilen zu verbessern: insbes. ist auf Freiheitsstrafen zu verzichten und die fahrlässige Begehung straffrei zu halten.**

Grundsatz der lex specialis

Dem erläuternden Bericht zur DSG-Revision ist auf Seite 39 zu entnehmen, dass die lex specialis Regel uneingeschränkte Geltung haben soll und damit bereichsspezifische Datenschutznormen dem DSG auch weiterhin vorgehen sollen. Die uneingeschränkte Geltung dieses Grundsatzes ist angesichts der zahlreichen bereichsspezifischen Regelungen im Datenschutz von besonders grosser Bedeutung, weshalb scienceindustries die **ausnahmslose Geltung des Grundsatzes der lex specialis ausdrücklich begrüsst**. Gerade für die Lifescience-Industrie und hier im besonderen Ausmass für jene Unternehmen, die im Bereich der Humanforschung tätig sind, ist es von höchster Bedeutung, dass die bestehenden, spezifischen Datenschutzbestimmungen des Humanforschungsrechts sowie weiterer, unsere Industrie betreffende Rechtsbereiche uneingeschränkte Geltung behalten und ausnahmslos dem DSG vorgehen. Dabei ist zu beachten, dass eine Vielzahl entsprechender Regelungen nicht auf Gesetzesstufe, sondern in Verordnungen geregelt ist. Der **Grundsatz der lex specialis muss also umfassend verstanden** sein und sich nicht nur auf bereichsspezifische Bestimmungen **in anderen Gesetzen als dem DSG beziehen, sondern auch für entsprechendes Verordnungsrecht gelten**.

In diesem Zusammenhang führen die Erläuterungen unter Seite 70 des erläuternden Berichts doch zu einiger Verunsicherung, wenn die Bestimmung von Art. 24 Abs. 2 lit. e Ziff. 1 VE DSG (Rechtfertigungsgrund der Forschung, Planung und Statistik) inskünftig verschärft ausgelegt und deshalb nur noch erschwert angerufen werden kann, dies insbes. auch im Kontext der Datenaufbewahrung (Art. 4 Abs. 4 VE DSG). Diese Aussage gilt es vor dem Hintergrund der lex specialis Regel klar zu relativieren und festzuhalten, dass von dieser einschränkenden Auffassung abweichende, bereichsspezifische Datenschutzbestimmungen auf Gesetzes- wie Verordnungsstufe auch inskünftig dem DSG klar vorgehen werden. Für den Bereich der Humanforschung bedeutet dies konkret, dass auch weiterhin nicht nur die spezifischen Datenschutzbestimmungen des Humanforschungsgesetzes (HFG) sondern auch all dessen Verordnungen (wie z.B. die Humanforschungsverordnung [HVF] und die Verordnung über klinische Versuche [KlinV]) weiterhin uneingeschränkte Gültigkeit haben und auch gegenüber dem revidierten DSG stets vorgehen müssen. Eine entsprechende **explizite Klarstellung muss u.E. mindestens Eingang in die Botschaft an das Parlament** finden, ansonsten in dieser eminent wichtigen Frage eine zu grosse Rechtsunsicherheit geschaffen wird. Wird dieser Weg aus staatsrechtlichen Überlegungen als ungenügend erachtet, so muss eine Lösung gefunden werden, der den umfassenden Vorrang bereichsspezifischer Datenschutzbestimmungen ausnahmslos sicherstellt.

Werden also Daten in Übereinstimmung mit den gesamten spezifischen Vorgaben bearbeitet, so können keine Datenschutzverletzungen resultieren. Gerade am Beispiel des Humanforschungsrechts zeigt sich die sachliche Rechtfertigung zu einem solchen Ansatz, wurden dessen datenschutzspezifischen Bestimmungen insgesamt nach internationalen Grundsätzen ausgestaltet und dabei auf die berechtigten Interessen sowie das Schutzbedürfnis der Patienten gebührend Rücksicht genommen. Der Humanforschungsplatz Schweiz ist darauf angewiesen, dass diese Bestimmungen, die durchaus von gewissen Vorgaben des DSG abweichen, weiterhin uneingeschränkte Geltung haben, ansonsten die Schweiz Gefahr läuft, inskünftig noch weniger Humanforschung betreiben zu können, als sie dies heute aufgrund der administrativen Hürden und der vergleichsweise hohen Kosten schon tut. Selbstverständlich **gelten diese Ausführungen stellvertretend auch für alle anderen bereichsspezifischen Datenschutzbestimmungen**, die in anderen Gesetzen und den dazugehörigen Verordnungen geregelt sind.

Geltungsbereich und Begrifflichkeiten

Während scienceindustries die Streichung des Schutzes **juristischer Personen** begrüsst, so ortet sie einigen Anpassungsbedarf beim Geltungsbereich und den Begrifflichkeiten. Es fällt auf, dass einige Formulierungen im VE DSG nicht konsequent verwendet werden, was es mit Blick auf eine konsistente Rechtsanwendung zu verbessern gilt. Sodann soll nach unserem Verständnis des VE DSG das Datenschutzgesetz inskünftig auch im Rahmen **bereits hängiger Zivilprozesse und laufender Strafverfahren** uneingeschränkt zur Anwendung kommen, was faktisch zu einer Ausweitung des Auskunftsrechts führt. Davon ist abzusehen, denn eine solche Ausweitung des Geltungsbereichs des DSG birgt ein grosses Missbrauchspotential, weil sich damit die zivilprozessualen Editionsregeln umgehen liessen. Auch möchten wir zu einer konsequenteren Verwendung des Begriffes „**Personendaten**" anstelle des Miteinbezugs des Ausdrucks „Daten" anregen, da dies u.E. die Definitionen einzelner Konzepte unnötig ausweitet. Ebenso sind die Pflichten zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter unklar verteilt resp. ist nicht ersichtlich, nach welcher Logik diese vergeben wurden, was es auch zu verbessern gilt. Desweitern ist für uns nicht nachvollziehbar, warum inskünftig auf die Definition des Begriffs des „**Gesetzes im formellen Sinn**" verzichtet werden soll, wenn dieser im Gesetz weiterhin Verwendung findet; u.E. sollte an der bisherigen Definition festgehalten werden.

Anzupassen sind sodann Art. 3 lit. c Ziff. 3 und 4 VE DSG, welche die **genetischen** sowie die **biometrischen Daten** als besonders schützenswerte Daten festschreiben. Beide Definitionen sind zu präzisieren, indem es heissen muss: *genetische resp. biometrische Daten, die den Zweck haben, eine natürliche Person eindeutig zu identifizieren*. Die im Vorentwurf verwendete Begrifflichkeit ist zu weit gefasst und bedarf zwingend der Präzisierung, ansonsten jegliche genetischen und biometrischen Daten als besonders schützenswert gelten, dies verbunden mit den entsprechenden Erschwernissen im Umgang mit diesen Daten. Sowohl bei genetischen wie auch den biometrischen Daten muss berücksichtigt werden, dass etliche Personendaten nicht mit der Absicht zur eindeutigen Identifikation einer Person erhoben werden und dann in Ermangelung des Bearbeitungszwecks nicht unter den Anwendungsbereich des DSG fallen sollen. Zudem ist zu beachten, dass es keine allgemein zugänglichen Datenbanken über Geninformationen gibt, mittels welcher Personen allein aufgrund einer DNA-Sequenz identifiziert werden könnten. Vielmehr sind solche Datenbanken besonders geschützt, wobei für jene mit Klartext-Identifikationselementen sehr grosse Sicherheitsmassstäbe gelten, was gut und richtig ist. Umgekehrt bedeutet dies aber auch, dass in der Realität im Regelfall eine Person nicht alleine durch eine DNA-Sequenz identifiziert ist.

Ebenso ist der Begriff oder anders ausgedrückt das Konzept des **Profilings**, wie er/es in Art. 3 lit. f VE DSG vorgeschlagen wird, zu verwerfen, da auch diese Definition viel zu weit gefasst ist und im Unterschied zur Datenschutzgrundverordnung der EU (DSGVO) auch manuelle Auswertungen miterfasst sind, wie bspw. eine Mitarbeiterbewertung. Bereits der Begriff des Persönlichkeitsprofils, wie er im aktuell gültigen DSG definiert ist, hat sich in der Praxis nicht bewährt und die Gelegenheit der Totalrevision sollte dahingehend genutzt werden, Abstand von diesem Konzept zu nehmen. Der Datenschutz bezieht sich auf Daten resp. alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Damit ist das Schutzobjekt des DSG umfassend bestimmt und zudem wird präzisiert, welche dieser Angaben als besonders schützenswert gelten. Es macht deshalb keinen Sinn, eine zusätzliche Schutzkategorie hinzuzufügen, die letztlich auf einen Arbeitsprozess - die Auswertung von Daten - abzielt. Denn sollten so gewonnene Arbeitsergebnisse für sich genommen den Begriff der Personendaten wieder erfüllen, so fallen sie ohnehin unter den Anwendungsbereich des DSG. Die Auswertung als Vorgang kann indes u.E. per se materiell den Datenbegriff gar nicht erfüllen. Auch ist der im VE DSG gewählte Ansatz aus Sicht des Schutzgedankens

nicht angezeigt, denn das Profiling wird für das Datensubjekt erst dann relevant, wenn ein Profil verwendet wird und nicht bereits mit dessen Erstellung. Dies gilt es unbedingt im Auge zu behalten.

Insofern würde scienceindustries es begrüssen, wenn sich das DSG in dieser Hinsicht stärker am Ansatz der DSGVO orientiert. In Anlehnung an diese sollte das Profiling nicht mehr als eine zusätzliche Schutzkategorie umschrieben werden. Vielmehr sollte sich dessen Begriffsumschreibung darin erschöpfen, dass unter diesem ein **Verarbeitungsvorgang**, bei welchem es **mittels technischer Hilfsmittel** zu einer **automatisierten, systematischen Verarbeitung von Personendaten** kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen hervorzusagen. Gleichzeitig wäre dann im Gesetz festzuschreiben, welches die spezifischen Pflichten der Verantwortlichen im Zusammenhang mit dem so definierten Profiling sind, wobei keinesfalls über das Schutzniveau der DSGVO hinausgegangen werden darf. Zu denken wäre an wenige Informations- und Auskunftspflichten sowie allenfalls ein Widerspruchsrecht beim Profiling zu Zwecken der Direktwerbung. Klar **Abstand zu nehmen** ist indes vom Konzept, dass **Profiling per se bereits als Persönlichkeitsverletzung** gilt und damit im Ergebnis für jedes Profiling eine ausdrückliche Einwilligung der betroffenen Person vorliegen muss (Art. 23 Abs. 2 lit. d VE DSG). Wenn ein Profiling erfolgt und im Ergebnis Personendaten daraus resultieren, dann stehen diese wiederum unter dem Schutz des DSG, weshalb sich eine zusätzliche Erwähnung des Profilings ohne ausdrückliche Einwilligung als Persönlichkeitsverletzung u.E. als unnötig erweist. Angesichts des damit verbundenen erheblichen Aufwands und der entstehenden Rechtsunsicherheiten auf Seiten der Unternehmen ist dieser Vorschlag abzulehnen.

Wollte man nicht Abstand vom vorgeschlagenen Konzept nehmen, dann wäre immerhin die Definition des Profilings auf mittels technischer Hilfsmittel automatisierte, systematische Entscheidungen zur Analyse und Bewertung von auf eine bestimmte Person bezogene persönliche Merkmale zu reduzieren und zur Verneinung einer Persönlichkeitsverletzung müsste die konkludente Einwilligung genügen.

Grundsätze

Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zwecks unnötigerweise mit dem Zusatz der **«klaren» Erkennbarkeit**. Diese Anpassung an die Terminologie des DSGVO ist verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert unnötige Rechtsunsicherheit, weshalb der Zusatz zu streichen ist.

Bezugnehmend auf Art. 4 Abs. 6 VE DSG, wonach eine gültige **Einwilligung eindeutig** zu erfolgen hat, nehmen wir zur Kenntnis, dass mit der Neuformulierung wohl eine terminologische Annäherung an das Übereinkommen SEV 108 und die DSGVO beabsichtigt wurde. Unserer Ansicht nach ist jedoch die Abgrenzung zur im zweiten Satz erwähnten ausdrücklichen Einwilligung im Rahmen des Profilings nicht ersichtlich und wirft lediglich Fragen der Unterscheidung dieser beiden Begriffe auf. Der Zusatz „eindeutig“ sollte daher ersatzlos gestrichen werden.

Auch wenn die **Nachführungspflicht** bereits heute im DSG vorgesehen ist, so ist dennoch festzuhalten, dass diese weit geht und bei den Firmen zu hohen Aufwendungen führt. Es wird zu beachten sein, hier auf Verordnungsstufe die Vorgaben minimal zu halten.

Datentransfer ins Ausland

scienceindustries begrüsst grundsätzlich die gegenüber dem aktuellen Gesetz beibehaltene Regelung zur Datenübertragung ins Ausland, **kritisiert indes die erweiterten Notifikations- und Genehmigungspflichten**. Zustimmend zur Kenntnis nehmen wir die vorgesehene Regelung, Daten ohne Vorliegen eines Angemessenheitsbeschlusses auf Basis von Standardklauseln exportieren zu können, stellen hierzu jedoch die Informationspflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) aufgrund des aus unserer Sicht ungünstigen Verhältnisses von Aufwand und Nutzen in Frage. Vielmehr regen wir eine Abkehr im Sinne eines weitgehenden Verzichts auf diese Pflicht – ganz im Sinne der DSGVO (Art. 46) – an.

Der Vorentwurf sieht zudem vor, dass „**verbindliche unternehmensinterne Datenschutzvorschriften**“ (sog. Binding Corporate Rules - BCR) neu einer Genehmigung durch den EDÖB unterstellt sind, was uns inkonsequent erscheint, da BCRs in der Regel dann zum Tragen kommen, wenn nicht mit Standardklauseln operiert werden soll und daher als Subgruppe von spezifischen Garantien nach Art. 5 Abs. 3 lit. b VE DSG aufgefasst werden können, diese jedoch lediglich einer Informationspflicht gegenüber dem EDÖB unterstehen. Desweitern stufen wir die genannte Frist zur Genehmigung von BCRs als nicht praktikabel ein, indem aufgrund der möglichen mehrmonatigen Unklarheit die Unternehmen in ihrer Entscheidungsfreiheit, nichtstandardisierte Datenexportverträge einzugehen, eingeschränkt wären. Die Frist ist deshalb auf das heutige Mass von maximal 30 Tagen zu kürzen und von einer unbeschränkt möglichen Verlängerung abzusehen. Wünschenswert wäre aus Sicht der Rechtssicherheit zudem, dass einmal bewilligte Garantien oder BCRs bis auf weiteres Gültigkeitsstaus erhalten und nicht ohne triftige Gründe widerrufen werden können sowie eine **Beibehaltung des heutigen Art. 6 Abs. 2 lit. g DSG** (Bekanntgabe von Personendaten innerhalb derselben Unternehmung), da diese Regelung zu einer erheblichen Erleichterung des Datenaustauschs innerhalb eines Unternehmens führt.

Hervorheben und kritisch würdigen möchten wir die neue Bestimmung in Art. 6 Abs. 2 VE DSG, wonach **Datenexporte auch in jenen Fällen dem EDÖB gemeldet** werden müssen, die durch Vertragsabschluss, Vertragserfüllung oder ein ausländisches Rechtsverfahren statthaft sind. Eine solche erweiterte Notifikationspflicht würde einerseits zu einer Überflutung an Meldungen an den EDÖB führen, welche dieser kaum innerhalb nützlicher Frist bearbeiten könnte. Andererseits gilt es den damit unerwünscht herbeigeführten Effekt zu beachten, dass Unternehmen gezwungenermassen gegenüber dem EDÖB Geschäftsgeheimnisse offenzulegen hätten, was unserer Ansicht nach zu weit geht. Dies hätte zur Konsequenz, dass etwa Unterlagen aus ausländischen Gerichtsverfahren oder Untersuchungen über das Öffentlichkeitsgesetz publik gemacht werden müssten, was jedoch vielmehr der Unternehmenstätigkeit schaden als den Datenschutz verstärken würde. Aus diesen Überlegungen sprechen wir uns für eine ersatzlose Streichung der genannten Bestimmung aus.

Informations-, Auskunfts- und weitere Pflichten

Informationspflicht

Auch wenn die Informations- und Auskunftspflichten zum Kern des VE DSG gehören und aus Sicht des Datensubjekts von grosser Wichtigkeit sind, so führen sie in der nun vorgeschlagenen Form zu einer verwirrenden Überinformation der betroffenen Personen, die der gewünschten Transparenz letztlich gar zuwiderläuft. Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen auf Grund des öffentlich-rechtlichen Charakters der Bestimmungen sowie den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Entsprechend muss die Regel grundsätzlich im Sinne einer **risikobasierten Transparenzpflicht** überarbeitet werden. In grundsätzlicher Hinsicht wäre u.E. eine einfache, transparente Information der betroffenen Personen allenfalls mit einer freiwillig vorzusehenden Kontaktmöglichkeit zur Ausübung ihrer Rechte nicht nur für die Unternehmen einfacher zu handhaben, sondern auch für die betroffenen Personen transparenter und würde zu deren besseren Schutz führen.

Dem VE DSG ist zum einen nicht zu entnehmen, wie die betroffene Person zu informieren sein wird. Individualisierte Informationspflichten würden mit beachtlichen Mehraufwänden einhergehen und stellten für die Unternehmen einen wesentlichen kostentreibenden Faktor dar. Daher regen wir die Einführung von **„standardisierten" Informationspflichten** an. Dies könnte beispielsweise durch einmalige datenschutzrechtliche Erläuterungen in den Allgemeinen Geschäftsbedingungen (AGB), einer Erklärung auf der Webseite („Privacy Note") oder auch durch das Anbringen von Piktogrammen, die etwa auf eine bestimmte datenschutzrelevante Verarbeitung von Daten hinweisen, erfolgen. Solche standardisierten Informationspflichten sollten durch die Verantwortlichen autonom oder allenfalls im Rahmen der guten Praxis entwickelt werden können.

Zum andern ist für uns nicht ersichtlich, über welche Einzelheiten dann im Detail informiert werden soll. Obwohl in Art. 13 Abs. 2-4 VE DSG einige konkrete Angaben enthalten sind, muss die Information letztlich dennoch alle Aspekte umfassen, die für eine betroffene Person notwendig sind, um ihre Rechte nach DSG geltend zu machen. Der erläuternde Bericht hält auf Seite 57 diesbezüglich fest, dass durch die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht ermöglicht werden soll, um dadurch ein Übermass an Informationen zu verhindern. Wenngleich sich dies vernünftig liest, so führt u.E. jedoch die strafrechtliche Sanktionierung der Informationspflicht vielmehr dazu, dass Verantwortliche und Auftragsbearbeiter infolge einer Risikominimierung und der Absicherung ihrer eigenen Beurteilung sich gezwungen sehen, deutlich mehr Informationen zu liefern, als an sich gesetzlich vorgesehen wäre. Will man den durchaus begrüssenswerten flexiblen Ansatz beibehalten, so wäre die **Sanktionierung dieser Pflicht zu überdenken und nötigenfalls nur geringfügig auszugestalten**.

Hinsichtlich der Begrifflichkeiten in Art. 13 Abs. 3 VE DSG fällt sodann auf, dass die Ausdrücke „**Dritter**" und „**Empfängerinnen** und **Empfänger**" nicht definiert werden sowie keine Klarheit zur **Abgrenzung der Pflichten** des Verantwortlichen und des Auftragsdatenbearbeiters besteht. U.E. sollte dieser lediglich für Verwirrung stiftende Absatz ersatzlos gestrichen werden. Überdies geht die vorgesehene **Informationspflicht bei der indirekten Datenbeschaffung** zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein; das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus

sind solche direkten Informationspflichten nicht erforderlich: eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist deshalb ebenso zu streichen.

Mit Blick auf die entsprechenden Regelungen der EU stellen wir weiter fest, dass insbesondere Art. 13 Abs. 4 VE DSG, wonach der Verantwortliche die **Identität sowie Kontaktdaten der Auftragsbearbeiter und darüber hinaus „die Daten oder Kategorien von Daten"** mitzuteilen hat, weiter als die entsprechenden Bestimmungen in Art. 13 und 14 DSGVO geht. Wir können aus dieser Bestimmung keinen Mehrwert für die betroffenen Personen erkennen, zumal mit diesen zusätzlichen Informationen nicht der Transparenz gedient wird, sondern vielmehr eine dieser zuwider laufende Informationsüberflutung auslösen würde. scienceindustries spricht sich deshalb für eine Streichung von Art. 13 Abs. 4 VE DSG aus.

Die in Art. 14 VE DSG vorgesehenen Ausnahmeregelungen entsprechen weitgehend jenen des heutigen Gesetzestextes, wirken sich u.E. im Ergebnis jedoch enger aus, als dies mit der revidierten Konvention 108 beabsichtigt wurde. Kritisch stehen wir insbesondere Art. 14 Abs. 4 lit. a VE DSG gegenüber, wonach die Berufung auf ein **überwiegendes privates Interesse** nur dann möglich ist, wenn Personendaten nicht an Dritte weitergegeben werden. Unserer Ansicht nach wäre hierbei lediglich zu prüfen, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person vorgeht. Ansonsten führte dies zu einer Ungleichbehandlung von Konzerngesellschaften im Vergleich zu einzelnen, unabhängigen Unternehmen, da sich erstere bei konzerninterner Weitergabe von Daten zum Zweck der Auftragsbearbeitung nicht auf diese Bestimmung berufen könnten. Aus diesem Grund regen wir an, den Zusatz *„…und er die Personendaten Dritten nicht bekannt gibt."* ersatzlos zu streichen.

Die Reichweite der neu eingeführten Informations- und Anhörungspflicht bei **automatisierten Einzelfallentscheiden** ist ebenso zu weitgehend und so nicht akzeptabel. Zwar kennen sowohl die Konvention 108 als auch die DSGVO eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE DSG ist jedoch viel breiter: der Entwurf unterscheidet stärker zwischen Profiling sowie automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden.

So bringt v.a. das vorgesehene **Äusserungsrecht** keinen Mehrwert. Es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Eine solche Regelung wäre entsprechend auf schwere Fälle - also solche, die erhebliche Auswirkungen auf die betroffene Person haben - zu begrenzen und der Wortlaut an die entsprechende Bestimmung in der DSGVO anzupassen. Auch dann wären sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen wären. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung erschiene uns dabei als ausreichend.

Im Kontext der Informationspflicht spricht sich scienceindustries zudem für eine Prüfung des Konzepts des **„unabhängigen betriebsinternen Datenschutzbeauftragten"** (Data Protection Officer - DPO) aus, da die Ernennung eines mit umfassenden Kompetenzen und Verantwortungen ausgestatteten DPOs hierbei zu einer begrüssenswerten Entlastung des EDÖB wie auch der Unternehmen führen dürfte (vgl. dazu Ausführungen unter dem entsprechenden Absatz auf Seite 12).

Auskunftsrecht

scienceindustries nimmt die vorgesehene Ausweitung des Auskunftsrechts gemäss Art. 20 VE DSG zur Kenntnis, erachtet jedoch den in Abs. 2 eingefügten Zusatz, wonach eine **transparente Datenbearbeitung gewährleistet** sein soll, als unzweckmässig und in einem gewissen Sinne verfänglich. In extensiver Auslegung kann dieser Zusatz dahingehend verstanden werden, dass sich das Auskunftsrecht nicht auf die Daten an sich zu beschränken hat, sondern damit zusätzlich auch die Datenbearbeitungsprozesse impliziert werden. Dies könnte zur Folge haben, dass der Verantwortliche diese auch offenlegen muss, was jedoch nicht den Absichten der Auskunftspflicht entsprechen würde und darüber hinaus möglicherweise bereits an der technischen Umsetzung scheitern könnte. Aus diesen Gründen regen wir an, auf diesen Zusatz zu verzichten.

Desweitern geht der Vorentwurf auch hier hinsichtlich der **automatisierten Einzelentscheide** einiges weiter als die DSGVO, indem in Abs. 3 ein Verantwortlicher verpflichtet wird, bei jedem Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er zu seinem Entscheid gelangt ist und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die hierzu verwendet wurden. Eine derart umfassend verstandene Auskunftspflicht greift in erheblichem Ausmass in die Freiheiten der Unternehmen ein und führt bei diesen zu einem unverhältnismässigen Aufwand, ohne dass daraus ein erkennbarer Nutzen für die betroffenen Personen ersichtlich ist. Die Auskunftspflicht wäre vielmehr auf das Vorliegen einer (automatisierten) Entscheidung zu beschränken, gleichzeitig kann allenfalls noch über deren Ergebnis informiert werden, **indes nicht über deren Wirkungen**, da diese gar nicht immer erkenn- oder gar abschätzbar sind. So sind übrigens vermehrt auch (automatisierte) Einzelentscheidungen denkbar, die gar nicht primär auf eine besondere (Rechts-)Wirkung ausgerichtet sind, sondern der Untersuchung von allgemeinen Verhaltensweisen dienen, womit verbunden kein Schutzbedürfnis erkennbar ist und damit auch keine Auskunftspflichten angezeigt sind. In diesem Kontext sei angefügt, dass uns Art. 20 Abs. 2 lit. e VE DSG nur dann akzeptabel erscheint, wenn ausschliesslich **Auskunft über das blosse Vorliegen einer automatisierten Einzelentscheidung** erteilt werden muss. Wird jedoch beabsichtigt, zusätzlich die Logik der automatischen Verarbeitung miteinzubeziehen, hätte dies die Offenlegung und Umschreibung einer umfassenden Anzahl an hinterlegten Algorithmen in allgemeinverständliche Erklärungen zur Folge, was bei den Unternehmen ebenso einen unverhältnismässigen Aufwand verursachen würde und daher abzulehnen ist.

Schliesslich nehmen wir zustimmend zur Kenntnis, dass die bisherige Regelung, wonach die Auskunft in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist, gestrichen wurde, indes aber kostenlos sein muss. Hierzu regen wir an, spätestens auf dem Verordnungsweg **Ausnahmen von der Kostenlosigkeit** vorzusehen, wie dies in Art. 12 Abs. 5 lit. a DSGVO vorgesehen ist. Ansonsten würde das Prinzip der Kostenlosigkeit dazu führen, dass die Auskunft selbst bei wiederholten, ungerechtfertigten und extrem aufwändigen Anfragen gratis sein muss, was uns nicht hinnehmbar erscheint.

Meldung von Datenschutzverstössen

Mit Art. 17 Abs. 1 VE DSG ist neu vorgesehen, dass jeder Datenschutzverstoss dem EDÖB „unverzüglich“ gemeldet werden muss, es sei denn, dieser führe „voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person“. scienceindustries stellt sich auf den Standpunkt, dass keine plausiblen Gründe ersichtlich sind, weshalb die Schweizer Regelung über den entsprechenden Art. 33

DSGVO hinausgehen soll. Die DSGVO sieht eine Meldung für den Fall vor, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine **getroffene Sicherheitsmassnahme verletzt** wurde und diese **Verletzung zu einem Verlust der Kontrolle an den Daten** führt (vgl. Art. 33 DSGVO i.V.m. Ziff. 87 und 88 der Präambel). In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst: bspw. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Die Ausnahme, wann keine Meldung zu erfolgen hat, ist dabei wiederum derart formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, da gemäss Gesetzestext eine unbefugte Datenbearbeitung stets eine Persönlichkeitsverletzung darstellt. Aufgrund des Dargelegten und den Ausführungen zur Inkonsistenz der Bestimmung mit dem restlichen VE DSG ist dieser Artikel u.E. auf das umschriebene Niveau der DSGVO zu reduzieren. Wir regen auch in diesem Kontext an, das Konzept des unabhängigen betrieblichen Datenschutzbeauftragten zu prüfen. Soweit ein solcher in einem Unternehmen eingesetzt ist und in dieser Funktion festgestellte Datenschutzverstösse dokumentiert, könnten u.E. die Auswirkungen von Art. 17 VE DSG gemildert und damit auch die Belastung des EDÖB reduziert werden.

Weitere Pflichten

scienceindustries erachtet die in Art. 19 lit. a VE DSG erwähnte Dokumentationspflicht als umfassend und zeigt sich besorgt über die Ausführungen auf Seite 65 im erläuternden Bericht, wonach die Datenbearbeiter verpflichtet sind, ebenfalls **Datenschutzverstösse** im Sinne von Art. 17 VE DSG zu dokumentieren. Angesichts des breiten Begriffsverständnisses von Art. 17 VE DSG erscheint uns diese Dokumentation unermesslich und ohne sichtbaren Mehrwert für den Datenschutz. Wir regen deshalb an, die **Dokumentationspflicht im Grundsatz auf das Führen eines Verzeichnisses aller Datenbearbeitungen zu beschränken**, für die der Verantwortliche zuständig ist. Selbstverständlich können Unternehmen freiwillig weiter gehen. Ebenso ist die Einführung einer Ausnahme für Kleinstunternehmen sowie der kleinen und mittleren Unternehmen im Sinne einer Entlastung zu prüfen. Die DSGVO sieht hierzu beispielsweise abweichende Regelungen vor für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen.

Weitaus kritischer beurteilt scienceindustries Art. 19 lit. b VE DSG, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten sowie bei Verletzungen des Datenschutzes der Verantwortliche und Auftragsbearbeiter Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtigungen etc. mitteilen müssen, soweit dies nicht oder nur mit „unverhältnismässigem“ Aufwand möglich ist. Wiederum ist für uns der Mehrwert dieser Ausweitung des entsprechenden Art. 19 DSGVO nicht ersichtlich. Notwendig wäre unserer Ansicht nach die Einführung einer **Begrenzung auf jene Fälle, in denen die betroffene Person ein schützenswertes Interesse** hat, zumal die vorgesehene Bestimmung nicht vorsieht, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Aufgrund der mannigfaltigen Gründe einer Berichtigung, Löschung oder Vernichtung von Daten, ohne dass sich dabei eine Nachinformation bisheriger Empfänger der Daten aufdrängt, kann dies zu bizarren Situationen führen. Es ist durchaus denkbar, dass eine Löschung erfolgt, weil der Inhaber die Daten nicht mehr braucht, nicht aber, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat. In solchen Fällen sollte keine Pflicht nach Art. 19 lit. b VE DSG ausgelöst werden, müsste doch sonst jedes Unternehmen, das seine Archive und dergleichen bereinigt, laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese Empfänger darüber informieren. Es erscheint uns daher nicht opportun, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 lit. b VE DSG ist dahingehend weiter einzuschränken, indem die Be-

stimmung nur zum Tragen kommt, wenn eine Person die **Nachinformation gestützt auf ein überwiegendes privates Interesse ausdrücklich verlangt**.

Sodann erschliesst sich uns auch in diesem Kontext der **Begriff der „Empfängerinnen und Empfänger"** nicht. Hier ist eine klärende Umschreibung zu fordern, wobei wir den Begriff so verstehen, dass der Auftragsbearbeiter nicht tangiert wird.

Datenschutz-Folgenabschätzung

scienceindustries stuft das im Vorentwurf vorgeschlagene Konzept der Datenschutz-Folgenabschätzung in verschiedener Hinsicht als problematisch ein. So erscheinen uns die Voraussetzungen für die Durchführung einer Abklärung gemäss Art. 16 Abs. 1 VE DSG äusserst tief. Ein „erhöhtes" Risiko dürfte sich in der Praxis rasch abzeichnen, wodurch für beinahe alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen. Seite 61 des erläuternden Berichts entnehmen wir zudem, dass die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling bereits ein Indiz für ein erhöhtes Risiko darstellen sollen, wie auch die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Es ist davon auszugehen, dass aufgrund der Strafandrohungen selbst in Fällen, in denen grundsätzlich kein erhöhtes Risiko besteht, ein entsprechendes Verfahren durchgeführt und eine Meldung an den EDÖB erfolgen wird. Der absehbare Aufwand – sei es für die Unternehmen oder den EDÖB – fiele enorm aus, ohne dass der Datenschutz dadurch gestärkt würde. Deshalb befürworten wir den Ansatz, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was die Interessenswahrung der schutzbezogenen Personen als wirklich nötig erkennen lässt. Daher schlagen wir vor, diesbezüglich an Art. 36 DSGVO anzulehnen, der **entsprechende Abklärungen erst bei Vorliegen eines „hohen" Risikos für eine Persönlichkeitsverletzung vorsieht**.

Sodann ist der Begriff der „Voraussehbarkeit" u.E. in der Schweizer Rechtspraxis nicht etabliert. Es bietet sich vielmehr an, den **Begriff der „überwiegenden Wahrscheinlichkeit"** zu verwenden, welcher im Sozialversicherungsrecht gebräuchlich ist und dort eine langjährige Konkretisierung erfahren hat. Gemäss diesem Beweisgrad genügt bundesgerichtlicher Rechtsprechung nach die blosse Möglichkeit eines bestimmten Sachverhaltes nicht; vielmehr ist im konkreten Fall jener Sachverhaltsdarstellung zu folgen, die von allen möglichen Geschehensabläufen als die wahrscheinlichste zu würdigen ist (vgl. BGE 126 V 360). Mit Blick auf die mit einer Datenschutz-Folgenabschätzung zu erwartenden erheblichen Aufwände besteht ein Interesse an einer rechtssicheren Formulierung, die möglichst Klarheit schafft ohne den Schutzgedanken zu unterwandern. Was hierbei für das Sozialversicherungsrecht genügt, darf auch für den Datenschutz als angemessen erachtet werden.

Desweitern bewerten wir die **Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung praxisfern** und sind der Meinung, dass die Datenbearbeiter dadurch in ihrer Arbeit massiv behindert würden. Einige der Unternehmen aus unserer Industrie führen jährlich weit über hundert Datenschutz-Folgenabschätzungen durch, wobei eine konsequente Prüfung durch den EDÖB wohl zur Folge haben würde, dass für jedes dieser Unternehmen nur für diese Prüfungen eine eigene Person abgestellt werden müsste, was weder sinnvoll erscheint, noch möglich ist. Auch die DSGVO geht in Art. 35 weniger weit: sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm **ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit**

der betroffenen Personen verbleibt. Zudem erscheint uns die dem EDÖB gewährte Frist zur Beurteilung viel zu lange: in der EU (Art. 36 Abs. 2 DSGVO) muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht; die Frist kann überdies nur in komplexen Fällen um sechs Wochen verlängert werden. In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen. Zudem sollte klar geregelt werden, welche Informationen dem EDÖB weitergeleitet werden müssen und wie diese insbesondere bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz (BGÖ) geschützt werden können. Datenschutz-Folgenabschätzungen von Unternehmen werden aber oftmals Geschäftsgeheimnisse enthalten, weshalb eine Einsichtnahme durch Mitbewerber vermieden werden muss.

Zusammenfassend regt scienceindustries aufgrund obiger Ausführungen an, einerseits die Begriffe des erhöhten Risikos sowie der Voraussehbarkeit im vorgeschlagenen Sinn anzupassen und den zeitlichen Rahmen zur Beurteilung der Massnahmen enger zu setzen. Desweitern soll auch die Datenschutz-Folgenabschätzung mit dem Konzept des „unabhängigen internen Datenschutzbeauftragten“ verknüpft werden (vgl. dazu Ausführungen unter dem nachfolgenden Absatz).

Konzept des unabhängigen internen Datenschutzbeauftragten

scienceindustries bedauert es, dass im VE DSG das Konzept des unabhängigen internen Datenschutzbeauftragten (Data Protection Officer - DPO) keinerlei Niederschlag gefunden hat. Wir erkennen darin nicht zuletzt im Vergleich mit der DSGVO einen Mangel, den es zu beheben gilt. Denn das Konzept des DPO scheint den Bedürfnissen der Wirtschaft zu entsprechen, wie ein Blick in die entsprechende Liste des EDÖB deutlich aufzeigt. So ist im revidierten Gesetz in Analogie zur bisherigen Regelung von Art. 11a DSG am **„Institut“ des DPO festzuhalten**, wobei die Unternehmen auch weiterhin **frei in der Entscheidung sein** sollen, einen solchen einzusetzen oder nicht. Die Voraussetzungen an die Stellung sowie die Aufgaben des DPO können in Anlehnung an die heute dazu bestehende Praxis zu den Art. 11a Abs. 5 lit. e DSG sowie Art. 12a und Art. 12b DSG weiterhin auf Verordnungsebene geregelt werden, wobei gleichzeitig die Äquivalenz mit den Art. 37 ff. DSGVO im Auge zu behalten wäre. Angesichts der Tatsache, dass der DPO im VE DSG gar nicht mehr vorgesehen ist, geht man seitens des Bundes offenbar von erheblichem Handlungsspielraum aus, was wir zwar ebenso einschätzen, indes vor dem Hintergrund der Äquivalenz mit den europäischen Vorgaben nicht gar soweit gehen würden, dieses Konzept überhaupt nicht mehr vorzusehen. Entscheidet sich ein Unternehmen, einen DPO einzusetzen, wäre sodann eine damit verbundene **Meldepflicht an den EDÖB** vorzusehen, der analog zur heutigen Regelung ein öffentlich einsehbares Register dieser Firmen führt. Damit ist transparent, welche Firmen von diesem Konzept Gebrauch machen, was mit Blick auf die nachfolgenden Ausführungen von Bedeutung ist.

Neben der Möglichkeit zur freiwilligen Bezeichnung eines DPO sind alsdann die im Zusammenhang mit dieser Bezeichnung verbundenen Rechtswirkungen im DSG aufzuführen. So sollten insbes. diverse **Informations- und Meldepflichten wegfallen** oder aber **mindestens gelockert** werden – soweit sie überhaupt beibehalten werden. Kommt ein DPO beispielsweise im Rahmen einer betriebsinternen Datenschutz-Folgenabschätzung zum Schluss, dass keine wesentlichen Risiken mit Blick auf den Datenschutz gegeben und entsprechend keine nennenswerten Massnahmen angezeigt sind, so können sämtliche damit zusammenhängende Meldungen an den EDÖB unterbleiben. Eine solche wäre nur dann angezeigt, wenn der DPO einerseits hohe Risiken für den Datenschutz der betroffenen Personen erkennt und anderseits deshalb

Massnahmen zur Eindämmung resp. Behebung der erkannten Risiken vorschlägt. Mit dieser Lösung wäre eine breite Abdeckung von Datenschutz-Folgenabschätzungen in den Unternehmen zu erreichen und gleichzeitig würde der EDÖB nur dann in den Prozess involviert, wenn eine Risikosituation sich manifestiert. Dies erscheint uns ein sachgerechter Ansatz, der einen effizienten Umgang mit den knappen Ressourcen auf beiden Seiten sicherstellt und gleichzeitig das Schutzniveau hoch hält. Ebenso wäre in diesem Zusammenhang eine Reduktion allfälliger Meldepflichten im Zusammenhang mit dem Datentransfer ins Ausland vorzusehen.

In diesem Kontext sei angefügt, dass scienceindustries den **Verzicht auf die Anmeldung von Datensammlungen durch private Personen begrüsst**. Ein DPO könnte auch hierbei eine wesentliche Aufgabe erfüllen, indem diese Person gestützt auf ihr Fachwissen, die Kenntnisse über das Unternehmen und seine Geschäftstätigkeiten sowie deren unabhängige Stellung am besten geeignet ist, betriebsinterne Standards für die Etablierung der notwendigen Prozesse auszuarbeiten und dabei den Datenschutz betriebsintern auf hohem Schutzniveau durchzusetzen. Verbunden mit der unsererseits geforderten Lockerung hinsichtlich der Melde- und Informationspflichten sowie ggf. weiterer Pflichten, wäre damit ein erheblicher Anreiz zur Schaffung einer solchen Stelle gegeben, was zum einen wiederum den betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes und zum andern einer Entlastung des EDÖB dienen würde. Entscheidet sich hingegen ein Unternehmen, keinen DPO einzusetzen, so könnte es im Gegenzug von den damit zusammenhängenden Rechtswirkungen nicht profitieren und sähe sich schneller mit Melde- und Informationspflichten konfrontiert. Aus diesem Grund sind wir der Ansicht, dass die mit der Bezeichnung und Bekanntgabe eines DPO verbundenen Rechtswirkungen bis zu einem gewissen Grad positivrechtlich im DSG vorzusehen sind, um diesbezügliche Klarheit und im Ergebnis Rechtssicherheit zu schaffen.

An dieser Stelle wollen wir gleichzeitig festgehalten wissen, dass das unsererseits geforderte Konzept des unabhängigen internen Datenschutzbeauftragten **nicht** dazu führen soll, dass diese **Personen eine erhöhte strafrechtliche Verantwortung** trifft. Vielmehr schlagen wir dazu einen anderen Ansatz als der im Entwurf gewählte vor und verweisen aber hier auf die nachfolgenden Ausführungen zum Sanktionssystem.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

scienceindustries spricht sich im Grundsatz positiv zum Konzept des Datenschutzes durch Technik und datenschutzfreundlichen Voreinstellungen (Art. 18 VE DSG) aus, auch wenn wir der Ansicht sind, dass sich die Bestimmungen bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes gemäss Art. 11 VE DSG ergeben, wonach im Rahmen einer Datenbearbeitung jeweils angemessene technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte Datenbearbeitung zu verhindern. Unter Berücksichtigung der entsprechenden DSGVO-Vorgaben stellen wir jedoch fest, dass die vorgeschlagene Formulierung gemäss VE DSG im Vergleich zu Art. 32 DSGVO deutlich zu restriktiv ausfällt. Insbesondere sollte berücksichtigt werden, dass die in Art. 18 Abs. 1 und 2 VE DSG vorgesehene Verpflichtung einen einklagbaren Anspruch einzelner Personen auf die Einführung solcher Massnahmen nach sich ziehen kann, was u.E. nicht die Absicht der europäischen Regelwerke war und eindeutig zu weit geht. Vielmehr sollte sich das **Schweizer Datenschutzgesetz an der entsprechenden DSGVO-Formulierung ausrichten**, in dem Sinne, dass *„Der Verantwortliche und der Auftragsbearbeiter geeignete (oder angemessene) technische und organisatorischen Massnahmen trifft/treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen“*.

Dabei handelt es sich zwar um im Gesetz festgelegte Ziele, die es anzustreben gilt, indes können diese **nicht zu einklagbaren Ansprüchen einzelner Personen** führen. Diese Differenzierung ist wesentlich, um einer möglichen diesbezüglichen Klageflut entgegen zu wirken. Denn es ist zu vermeiden, dass in gewissen Kontexten realisierbare Standards auf dem Klageweg auf Branchen übertragen werden, in welchen diese keinen Sinn machen oder aus technischen Gründen noch nicht im gleichen Ausmass etabliert sind. U.E. würde sich auch eine entsprechende **Klärung in der Botschaft an das Parlament** aufdrängen.

Keine spezifischen Regelungen für verstorbene Personen

scienceindustries spricht sich aus mehreren Gründen **gegen die Einführung von spezifischen Regelungen für verstorbene Personen** aus. Vorweg möchten wir auf den in Art. 31 Abs. 1 ZGB verankerten Grundsatz hinweisen, wonach die Persönlichkeit mit dem Tod endet und eine verstorbene Person folglich auch keinen Datenschutz erlangen kann. Allenfalls kommt dieser für Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung derer Daten ebenfalls betroffen sind, zum Tragen. Aus Sicht der Unternehmen sind die vorgesehenen Regelungen insofern problematisch, als sie aufgrund ihrer generell abstrakten Natur unzählige weitere, grundsätzlich mit der Bestimmung nicht beabsichtigte Anwendungsfälle miteinbeziehen und daher unvorhergesehene Nebenwirkungen entfalten können. In diesem Zusammenhang gilt es auch die Übertragung von Persönlichkeitsrechten auf Dritte zu berücksichtigen. Würde beispielsweise ein einzelner Erbe die Löschung von Daten beantragen, könnte sich das betroffene Unternehmen lediglich auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen, jedoch nicht auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. die Aufbewahrungspflicht gemäss Art. 12 Abs. 4 VE DSG. Daraus lässt sich schlussfolgern, dass der Erbe wesentlich mehr Rechte gegenüber einem Datenbearbeiter hat als der Erblasser zu Lebzeiten, was kaum die Absicht hinter Art. 12 VE DSG sein dürfte. Die Tatsache, dass weder in der Konvention 108 noch in der DSGVO spezifische Regelungen für verstorbene Personen aufgenommen wurden, lässt uns auch an der Relevanz einer spezifischen Regelung hinsichtlich der Fortführung der Angemessenheitserklärung durch die EU zweifeln. Angesichts des oben ausgeführten fehlenden datenschutzrechtlichen Nutzens und verbunden mit den einhergehenden Rechtsunsicherheiten muss **Art. 12 VE DSG u.E. unbedingt ersatzlos gestrichen werden**. Solche Sachverhalte sollen hinreichend im Zivilrecht geklärt werden und allfällige Lücken wären entweder über dieses oder durch vertragliche Lösungen zu schliessen.

Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen

scienceindustries lehnt den Vorschlag des VE DSG, das Sanktionssystem über das ordentliche Strafrecht auszugestalten, entschieden ab, denn dies führte im Ergebnis zu einer Vielzahl unerwünschter Folgen. So zeitigte ein solches Konzept die primäre strafrechtliche Verantwortlichkeit der natürlichen Personen für die Verletzung sanktionierter Tatbestände und nur subsidiär könnte auf die Unternehmen durchgegriffen werden, wobei uns gerade in dieser Hinsicht Art. 53 VE DSG als untauglich erscheint. Angesichts der vorgesehenen, beachtlichen Strafdrohungen ist eine primäre strafrechtliche Verantwortung der natürlichen Personen – sprich der Mitarbeiter von Unternehmungen – nicht nur unverhältnismässig, sondern birgt auch die Gefahr, dass es unternehmensintern zu einer erhöhten gegenseitigen Anzeigeaktivität durch Mitarbeitende kommt. Dies dürfte auch kaum mehr durch interne Vorgaben des Unternehmens in Bahnen gelenkt werden können, weil jeweils ein persönliches Schicksal einer Person mit diesen Fragestellungen verbunden ist, was bekanntlich – und bis zu einem gewissen Grade auch nachvollziehbar – unberechenbare Kräfte auslöst. Mit Blick auf die vielfältigen Aktivitäten, die angesichts der verschärften Datenschutzanforderungen im Tagesgeschäft von Unternehmen zu ungewollten Datenschutzverletzungen führen können, bestünde eine eminente Gefahr, dass ein sehr weiter Kreis von Mitarbeitern laufend zur strafrechtlichen Verantwortung gezogen würde. Entsprechend sähen sich die Unternehmen im Falle von Verurteilungen der betroffenen Personen nur schon aus Gründen ihrer eigenen Compliance gezwungen, das Arbeitsverhältnis mit solchen Mitarbeitern aufzulösen, währenddem diese auf dem Arbeitsmarkt aufgrund möglicher Strafregistereinträge eine deutlich reduzierte Wiedereinstellungschance zu gewärtigen hätten. So dürfte es sich dann auch alsbald als äusserst schwierig erweisen, überhaupt noch Mitarbeiter für solche Positionen rekrutieren zu können, mit dem Ergebnis, dass das unsererseits geforderte **Konzept des unabhängigen internen Datenschutzbeauftragen faktisch nicht mehr greifen würde.** In der Konsequenz wäre gerade der Durchsetzung des Datenschutzes damit nicht gedient, währendem dieser eine zusehends lähmende Wirkung auf das Geschäftsleben entfaltet und zu einem vergifteten Betriebsklima führt. Überdies müssten sich 26 kantonale Strafuntersuchungsbehörden und Jurisdiktionen mit dem strafrechtlichen Vollzug der Datenschutzbestimmungen befassen, was angesichts der oft schwierig lokalisierbaren Datenschutzverletzungen nicht nur zu stetigen Zuständigkeitsfragen, sondern auch zu unterschiedlichen Rechtsauslegungen und entsprechender inkonsistenter Rechtsanwendung führen dürfte.

Aufgrund dieser Analyse **spricht** sich **scienceindustries** für ein System mittels **Verwaltungssanktionen verbunden mit einer primären Verantwortlichkeit** der gegebenenfalls **fehlbaren Unternehmen aus**. Denn die Datenbearbeitung findet in aller Regel in Verrichtung geschäftlicher Aktivitäten statt und generiert letztlich in diesem Kontext einen Vorteil für das Unternehmen, weshalb dieses auch in der Verantwortung stehen soll. Verwaltungssanktionssysteme existieren in der Schweiz bereits heute und man kann auf den gemachten Erfahrungen aufbauen, wobei zu beachten wäre, dass der Bereich des Datenschutzes nicht unbesehen vergleichbar mit anderen Rechtsgebieten ist, in welchen dieser Ansatz bereits gilt (insbes. Kartellrecht) und entsprechend differenzierte Vorgaben und Regelungen angezeigt wären. Wie bereits erwähnt, besteht bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, wobei festzustellen ist, dass solche Verstösse in aller Regel nicht zu nennenswerten finanziellen Vorteilen der Unternehmen führen. Im Bereich des Datenschutzes hätte sich das Verwaltungssanktionssystem deshalb nicht an der Massgabe der Abschöpfung von unrechtmässig erworbenen Gewinnen zu orientieren, sondern an jener der Durchsetzung einer effizienten Umsetzung der datenschutzrechtlichen Vorgaben. Deshalb sind wir der Ansicht, dass der Strafrahmen auch bei der Einführung von Verwaltungssanktionen bei der vorgeschlagenen **Höchstbussengrenze von einer halben Million**

CHF begrenzt bleiben muss und dieser nicht nach oben geöffnet werden soll. Vielmehr soll der Sanktionsrahmen nach dem Grundsatz des **Auswirkungsprinzips** ausgestaltet sein, wobei je nach Schwere der vorsätzlich begangenen Datenschutzverletzung in örtlicher wie sachlicher Hinsicht die Strafe höher oder tiefer festzusetzen wäre, begrenzt eben bei der Höchststrafe von CHF 500‘000.-. Eine entsprechende Differenzierung erscheint uns sachgerecht, fällt denn ein Sachverhalt mit lokaler oder regionaler Auswirkung weniger ins Gewicht, als einer mit internationaler Betroffenheit. Dasselbe gilt u.E. wenn beispielsweise eine einfache Informationspflichtverletzung gegenüber einer Einzelperson ins Verhältnis gesetzt wird mit mehrfacher Widerhandlungen gegen das DSG, welche eine Vielzahl von Personen betreffen würde.

Ebenso wäre die Gelegenheit zu nutzen, die seit Jahren im Raum stehende Kritik des ungenügenden Rechtsschutzes der Parteien im Rahmen des verwaltungsstrafrechtlichen Untersuchungsverfahrens zu beherzen und sich stärker an den Grundsätzen der Europäischen Menschenrechtskonvention (EMRK) zu orientieren. Es sollte neu vorgesehen werden, im **gesamten Verwaltungsstrafverfahren dem Grundsatz des „nemo tenetur“ ungeschmälerte Geltung durch gesetzgeberische Auflagen** zu verschaffen, so dass die Parteien sich nach Eröffnung des Verfahrens nicht mehr selber belasten müssen. Möglicherweise könnte Art. 113 der eidgenössischen Strafprozessordnung (StPO) für dieses Untersuchungsverfahren für anwendbar erklärt oder eine analoge Bestimmung im entsprechenden Gesetz vorgesehen werden. Schliesslich wäre ein **System von Rechtfertigungsgründen** oder aber **mindestens Strafmilderungs- resp. Strafminderungsgründen** vorzusehen, welche die Unternehmungen im Verwaltungsstrafverfahren vorbringen können. Zu denken wäre insbes. an vorsätzlich begangene Datenschutzverletzungen durch Mitarbeitende, wie z.B. Datendiebstahl. In diesen Ausnahmefällen könnte scienceindustries auch eine zusätzliche, unmittelbare strafrechtliche Verantwortlichkeit der fehlbaren natürlichen Personen akzeptieren, falls dies dann eben zu einer Reduktion des Strafmasses beim Unternehmen führt. Auch sollte das kooperative Verhalten der Unternehmungen im Rahmen der Untersuchung, das möglicherweise bis hin zu freiwillig selbstbelastenden Aussagen gehen kann, ebenso als klar strafmildernder Grund vorgesehen werden. Schliesslich wären auf technischen Fehlleistungen basierende Datenschutzverletzungen mit geringfügigen Auswirkungen auf den Datenschutz strafmildernd auszugestalten.

Sanktionenkatalog und Strafmass

Nach Ansicht von scienceindustries ist nicht nur das **strafrechtliche Bestimmtheitsgebot** in vielen vorgeschlagenen Strafbestimmungen oft **fraglich**, sondern der **Sanktionskatalog tendenziell überladen** und deshalb ist eine **Reduktion der Straftatbestände** zu prüfen. Im Umfang, wie wir uns in dieser Stellungnahme für eine Reduktion der Rechte der Datenschutzsubjekte und der Pflichten der Verantwortlichen aussprechen, führt dies entsprechend auch zur Aufhebung der damit verbundenen Sanktionierungen, denn wo keine Rechte verbrieft resp. keine Pflichten bestehen, können solche auch nicht verletzt werden und entsprechend keine Sanktionen greifen. Insbesondere sei an dieser Stelle wiederholt, dass die Strafbarkeit der Verletzung von Informationspflichten generell zu überdenken ist oder aber mindestens hierbei nur geringfügige Sanktionen festzulegen wären. Zudem halten wir fest, dass mit Blick auf die Fortführung eines mit Europa äquivalenten Datenschutzniveaus nach unserer Einschätzung gerade in diesem Bereich eine Orientierung am Übereinkommen SEV 108 des Europarates als genügend zu erachten ist.

Ersatzlos zu streichen ist sodann Art. 52 VE DSG, sind denn die angedrohten Freiheitsstrafen von bis zu drei Jahren zum einen absolut unverhältnismässig und diese Straftatbestände zum andern mit Blick auf ein

äquivalentes Datenschutzniveau mit Europa u.E. nicht erforderlich. **Generell ist von Freiheitsstrafen Abstand zu nehmen** und gänzlich auf deren Einführung zu verzichten, wurden denn auch keine solchen in den europäischen Regelwerken vorgesehen, welche ja allesamt wirksame und abschreckende, indes eben auch verhältnismässige Sanktionen verlangen. Offenbar wurde sowohl im Europarat als auch in den Institutionen der EU keine Notwendigkeit zur Einführung derart drastischer Sanktionen erkannt, was sachgerecht ist. Vielmehr erscheint die Strafandrohung von Freiheitsstrafe mit Blick auf den begangenen Rechtsbruch als unverhältnismässig kriminalisierend. Eine derart strenge Straffolge lähmte den Geschäftsverkehr übermässig und stellte einen beachtlichen Standortnachteil für die Schweiz dar.

scienceindustries **lehnt** des weitern jegliche **Strafbarkeit** für **fahrlässige Begehung** von Datenschutzverletzungen entschieden **ab**. Es sei erneut wiederholt, dass bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, besteht. Diesem Umstand ist gebührend Rechnung zu tragen, dies nicht zuletzt auch in Anerkennung, dass die Unternehmen dem Schutz von Personendaten ohnehin einen hohen Stellenwert einräumen. Auch wenn heute schon grosse Anstrengungen zur Einhaltung der datenschutzrechtlichen Vorgaben getätigt werden, sind angesichts der zahlreichen Verarbeitungsaktivitäten sowie mit Blick auf die oft komplexen Prozesse unbeabsichtigte Datenschutzverletzungen auch bei Einhaltung hoher Standards in grossen wie in kleinen Unternehmen nicht immer zu vermeiden. Darin kann indes kein kriminelles Verhalten erkannt werden, weshalb die **Strafbarkeit von Datenschutzverstössen ausschliesslich auf deren vorsätzliche Begehung zu begrenzen** ist. Ein auf Vorsatz beschränkter Strafrahmen erscheint auch angesichts der typischerweise schwierigen sowie sehr aufwendigen Bewertungs- und Meldevorgängen bei der Aufklärung als auch Behebung von fahrlässigen Rechtsverstössen als angemessen und entsprechend geboten.

Stellung und Kompetenzen des Eidgenössischen Datenschutzbeauftragten

Vor dem Hintergrund der vorangegangen Ausführungen und in Anerkennung der internationalen Vorgaben, die neu im Bereich des Datenschutzes eine mit beachtlichen Kompetenzen ausgestattete (nationale) Aufsichtsbehörde fordern, schlägt scienceindustries ein vom VE DSG abweichendes Modell vor. Der **EDÖB** mit seiner beratenden, empfehlenden und letztlich anzeigenden Funktion hat sich im Grundsatz bewährt und wir würden es begrüssen, wenn an diesem **System unverändert festgehalten** wird. Nur schon mit Blick auf seine Bezeichnung als „Beauftragter“ und seine organisatorische Einordnung bei der Bundeskanzlei, die von Bundesverfassung (BV) wegen als Stabsstelle des Bundesrates agiert (Art. 179 BV), drängt sich eine Beibehaltung des Systems auf. Im Übrigen wäre es auch fraglich, ob eine mit Verfügungsgewalt ausgestaltete Behörde von Verfassung wegen überhaupt der Bundeskanzlei angehören darf, sind doch die Exekutivgewalten in aller Regel den Departementen zugeordnet. Zudem orten wir Interessenskonflikte, wenn der mit umfassenden beratenden Funktionen ausgestattete Beauftragte des Bundes gleichzeitig auch Untersuchungsaufgaben - bis hin zur Kompetenz zur unangekündigten Hausdurchsuchung - erhält sowie weitere vorsorgliche Massnahmen verfügen kann. Abgesehen von solchen Konflikten führte dieser Umstand auch nicht zur notwendigen Vertrauensbasis, auf welcher beispielsweise das Konzept der guten Praxis wirksam greifen kann.

Wir regen deshalb an, dass der **EDÖB** unverändert als eine **bundesbeauftragte Stelle ohne Verfügungskompetenzen erhalten** bleibt und weiterhin alle im Zusammenhang mit der Umsetzung des DSG bestehenden Beratungs- und Empfehlungstätigkeiten wahrnimmt. So soll er auch inskünftig sowohl private Personen

wie auch Unternehmen in allen Belangen des Datenschutzes beraten, das Verzeichnis der Länder mit vergleichbarem Datenschutzniveau sowie das Verzeichnis der Firmen führen, die auf freiwilliger Basis einen internen unabhängigen Datenschutzbeauftragten gemeldet haben (vgl. Ausführungen auf Seite 12). Er würde im Rahmen der guten Praxis Empfehlungen ausarbeiten, wobei alleine schon aufgrund seiner Stellung nicht zu befürchten wäre, dass dabei eine „Schattengesetzgebung" entstünde, was mit Blick auf die Rechtssicherheit zentral ist. An ihn wären die meldepflichtigen Datenschutz-Folgenabschätzungen sowie weitere gesetzliche Meldepflichten zu richten und ebenso die meldepflichtigen Datenschutzverletzungen anzuzeigen. Zudem würde es in seiner Kompetenz liegen, Datenschutzverletzungen, von denen er Kenntnis erhalten hat, nach seinem Ermessen an eine **neu zu schaffende Bundesspruchbehörde** zu melden, die dann ihrerseits das Verwaltungsverfahren eröffnet, durchführt und allenfalls Verwaltungssanktionen ausspricht.

Entsprechend wäre somit eine **neue Bundesspruchbehörde** zu schaffen, die in einem Departement anzusiedeln wäre (wobei sich u.E. wohl das Eidgenössische Justiz- und Polizeidepartement [EJPD] als am geeignetsten erwiese) und die mit allen notwendigen Verfügungskompetenzen zur Durchführung eines Verwaltungsstrafverfahrens bis mit zur Verhängung von Verwaltungssanktionen auszustatten wäre. Damit würde die Schweiz die internationalen Vorgaben einer bestehenden **Aufsichtsbehörde mit Verfügungskompetenzen** samt jener zur **Verhängung von Verwaltungssanktionen** erfüllen, ohne dass sie das bewährte Institut des EDÖB aufgeben und diesen zudem mit Aufgaben und Kompetenzen ausstatten müsste, die zum einen zu Interessenkonflikten führen dürften und zum andern auch unter dem Aspekt der Gewaltenteilung fragwürdig sind. Zudem bestünde die Chance, eine zentrale Behörde zu etablieren, welche eine einheitliche Rechtsauslegung und -anwendung im Bereich der Sanktionierung gewährleisten könnte – dies im Unterschied zum im VE DSG vorgeschlagenen Ansatz über das ordentliche Strafrecht mit 26 kantonalen Vollzugsorganen. Sie wäre letztlich auch in der Lage, auf Datenschutz spezialisiertes und damit notwendigerweise versiertes Personal zu verpflichten, wie dies auf kantonaler Ebene unmöglich der Fall sein könnte. Dass damit beim Bund zusätzliche Kosten anfallen würden, ist nicht von der Hand zu weisen, doch muss dem auch entgegen gehalten werden, dass die zusätzliche Belastung der kantonalen Strafverfolgungsbehörden sowie deren Justiz vermutlich infolge der geringeren Professionalität volkswirtschaftlich betrachtet gar zu höheren Kosten führen dürfte. Wie bereits erwähnt, sprich sich scienceindustries auch dafür aus, gleichzeitig die Chance zu nutzen und **konkrete Verfahrensvorgaben zu machen, welche die Rechte der Verantwortlichen im Verwaltungsstrafverfahren in adäquater Weise garantieren**. Insbesondere wäre dabei an den Grundsatz des „nemo tenetur" zu denken und festzuschreiben, dass sich Verantwortliche auch dann im Verfahren nicht weiter selber belasten müssen, wenn sie vorgängig ihrer Pflicht zur Meldung der Datenschutzverletzung nachgekommen sind.

Ein solches System getrennter Kompetenzen – beratender EDÖB und Aufsichtsbehörde mit Verfügungs- und Sanktionskompetenzen – führte u.E. zu einer effektiveren Durchsetzung des Datenschutzes in der Schweiz und gleichzeitig könnten all die negativen Konsequenzen, die mit einer Sanktionierung von Datenschutzverletzungen über das ordentliche Strafrecht resultierten, weitgehend vermieden werden. Zudem könnte der EDÖB an sich nur so seine beratende und empfehlende Funktion glaubwürdig wahrnehmen, was in besonderem Mass auch für den Ansatz der guten Praxis gilt. Schliesslich würde die Schweiz damit eine dem Wortsinn der europäischen Regelwerke entsprechende Aufsichtsbehörde schaffen.

Wir sind uns bewusst, dass wir hiermit einen **neuartigen Vorschlag skizzieren**, den es im Detail zu vertiefen und konkret auszugestalten gälte. scienceindustries würde es begrüssen, wenn das **Bundesamt für Justiz**

diesen Ansatz aufnehmen und im Rahmen einer Arbeitsgruppe mit weiteren interessierten Kreisen einen **konkreten Vorschlag ausarbeiten** würde, wobei wir gerne unsere aktive Beteiligung anbieten.

Abschliessend halten wir fest, dass soweit vorliegende Stellungnahme sich nicht explizit zu weiteren Themen im Kontext der DSG-Revision äussert, wir auf die Stellungnahme von economiesuisse verweisen, die wir grundsätzlich unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Dr. Beat Moser
Direktor

Jürg Granwehr
Leiter Pharma Schweiz

Kopie an:
economiesuisse, SwissHoldings
ASSGP, Intergenerika, Interpharma, vips