

Stellungnahme der ARGE DATEN vom 28.08.2012 zur DSG - Novelle 2012

1.	EINLEITUNG	2
1.1	Etablierung von Datenschutzbeauftragten.....	2
1.2	Abschaffung der Vorabkontrolle.....	3
1.3	Zukunft der Datenschutzkommission	4
2.	DIE ÄNDERUNGEN IM DETAIL	6
2.1	§ 17 Abs 2 Z 6 – Standardanwendungen	6
2.2	§ 17 Abs 2 Z 7– Datenschutzbeauftragte / Meldepflicht	7
2.3	§ 17a Abs 1 – Datenschutzbeauftragte / Bestellung	8
2.4	§ 17a Abs 2 – Datenschutzbeauftragte / Unbefangenheit	8
2.5	§ 17a Abs 3 – Liste der Datenschutzbeauftragten.....	9
2.6	§ 17a Abs 4 – Datenschutzbeauftragte / Datenanwendungen	9
2.7	§ 17a Abs 5 – Datenschutzbeauftragte / Unterrichtung	10
2.8	§ 17a Abs 10 – Datenschutzbeauftragte / Verantwortung	11
2.9	§ 18 Abs 2, 3 und 4 – Vorabkontrolle / allgemein	11
2.10	§ 18 Abs 2 – Vorabkontrolle / strafrechtlich relevante Daten	12
2.11	§ 18 Abs 2 – Vorabkontrolle / Informationsverbundsysteme	13
2.12	§ 18 Abs 2 Z 2 – Vorabkontrolle / Bewertung von Betroffenen.....	13
2.13	§ 18 Abs 3 – Vorabkontrolle / Zustimmung der Betroffenen	14
2.14	§ 18 Abs 3 – Vorabkontrolle / Datenanwendungen aufgrund von Gesetzen oder Verordnungen	15
2.15	§ 18 Abs 4 – Vorabkontrolle / Liste gesetzlicher Datenanwendungen	15
2.16	§ 30 Abs 1a – Datenschutzbeauftragte / Eingaberecht	16
2.17	§ 30 Abs 2a – Überprüfung der Meldepflicht.....	16
2.18	§ 30 Abs 4a – Unterstützung der Datenschutzkommission.....	16
2.19	§ 38 Abs 3 – Stellungnahme durch die Datenschutzkommission.....	17
2.20	§ 50a Abs 7 – Videoüberwachung / Bewertung von Betroffenen.....	17
2.21	§§ 50b Abs 2, 50c Abs 1 – Videoüberwachung / Vorabkontrolle.....	18
2.22	§ 50c Abs 2 – Analoge Videoüberwachungen.....	19
2.23	§ 52 Abs 2 Z 10 – Strafbestimmung / Behinderung von Datenschutzbeauftragten	19
2.24	§ 52 Abs 2 – Strafbestimmung / Abberufung von Datenschutzbeauftragten .	19
2.25	§ 61 Abs 9 und Abs 10 – Automatische Registrierung	20
3.	FAZIT.....	21

1. EINLEITUNG

Das Bundeskanzleramt hat einen Entwurf eines Bundesgesetzes, mit dem das Datenschutzgesetz 2000 (DSG 2000) geändert wird, die sogenannte DSG-Novelle 2012 in Begutachtung gebracht. Hauptziel dieser Novelle ist es, durch Änderungen der Bestimmungen zur Vorabkontrolle, Bürokratie abzubauen und die Datenschutzkommission von administrativen Aufgaben im Rahmen der Vorabkontrolle zu entlasten.

Dies soll dadurch erreicht werden, dass für Auftraggeber zukünftig freiwillig die Möglichkeit bestehen soll, Datenschutzbeauftragte zu bestellen, wodurch Datenanwendungen fortan nicht mehr an das Datenverarbeitungsregister gemeldet werden müssen. Dies stellt vor allem für Mittel und Großunternehmen eine deutliche Verringerung des Verwaltungsaufwandes dar.

Weiters sollen in Zukunft weder Datenanwendungen die strafrechtlich relevante Daten enthalten, noch Informationsverbundsysteme oder Videoüberwachungen der Vorabkontrolle unterliegen. Datenanwendungen zu deren Betrieb Betroffene ihre ausdrückliche Zustimmung erteilt haben oder Datenanwendungen die aufgrund von Gesetzen bzw. Verordnungen betrieben werden, zu denen die Datenschutzkommission im Rahmen der Ausarbeitung eine Stellungnahme abgegeben hat, sollen ebenfalls nicht mehr der Vorabkontrolle unterliegen. Dies stellt eine de facto Abschaffung der Vorabkontrolle dar.

Daneben enthält der vorliegende Entwurf eine Reihe neuer Aufgaben und Pflichten für die - zum Stichtag 1.1.2014 - aufgelöste Datenschutzkommission. Dabei handelt es sich um eine kurzsichtige Vorgehensweise. Vielmehr sollte der Entwurf die Schaffung einer neuen, unabhängigen Kontrollstelle mit klaren Kompetenzen vorsehen, die die Aufsichts- und Kontrollfunktionen der Datenschutzkommission übernimmt.

Während die Absicht des Entwurfs, die Datenschutzkommission zu entlasten zu begrüßen ist, soll dies zum Teil durch die drastische Beschneidung von Betroffenenrechten erreicht werden. Dies ist klar abzulehnen. Der vorliegende Entwurf ist daher, insbesondere in Bezug auf die Änderungen an der Vorabkontrolle, dringend zu überarbeiten.

1.1 Etablierung von Datenschutzbeauftragten

Durch die Möglichkeit, dass Auftraggeber Datenschutzbeauftragte bestellen können, wird nicht nur eine langjährige Forderung der ARGE DATEN erfüllt, sondern das österreichische Datenschutzgesetz europäischen Standards angeglichen.

Während die Richtlinie 95/46/EG (DatenschutzRL) noch die freiwillige Möglichkeit vorsieht, Datenschutzbeauftragte zu bestellen, soll dies, der geplanten Datenschutz-Grundverordnung nach, für öffentliche Auftraggeber sowie Auftraggeber bestimmter Größe verpflichtend sein.

Bereits in ihrer Stellungnahme zur geplanten DSGVO-Novelle 2008 (<ftp://ftp.freenet.at/privacy/gesetze/dsg-stellungnahme.pdf>) hat die ARGE DATEN umfangreich den Sinn und die Notwendigkeit von Datenschutzbeauftragten dargestellt. Darüberhinaus zeigen laufende Erfahrungen, dass sich vor allem mittlere und große Betriebe Datenschutzbeauftragte mit gesetzlich verankerten Kompetenzen wünschen.

Datenschutzbeauftragte sollen Auftraggeber zukünftig in datenschutzrechtlichen Angelegenheiten beraten, Betroffenen als Ansprechperson zur Verfügung stehen und Auftraggeber aufgrund ihrer fachlichen Kompetenz von der Pflicht, Datenanwendungen zu melden, befreien.

Der vorliegende Gesetzesentwurf schafft die grundlegenden Voraussetzungen damit Auftraggeber Datenschutzbeauftragte bestellen können. Besonders begrüßt wird dabei, dass der vorliegende Entwurf eine ausreichende Kompetenz des Datenschutzbeauftragten fordert und auch dessen Fort- und Weiterbildung gesetzlich sichert. Die geplanten Bestimmungen erscheinen aber an mehreren Stellen unausgereift und sind entsprechend zu überarbeiten bzw. zu ergänzen.

Die DSGVO-Novelle 2012 sollte die Unbefangenheit von Datenschutzbeauftragten stärker betonen und ausdrücklich die Möglichkeit vorsehen, dass auch externe Personen zum Datenschutzbeauftragten bestellt werden können.

Die Arbeit von Datenschutzbeauftragten sollte grundlegenden Aufsichts- und Kontrollmöglichkeiten durch die Datenschutzkommission unterliegen.

1.2 Abschaffung der Vorabkontrolle

Umfangreiche Änderungen an der Vorabkontrolle sollen dazu führen, dass Datenanwendungen mit strafrechtlich relevanten Daten, Informationsverbundsysteme und Videoüberwachungen nicht mehr der Vorabkontrolle unterliegen, da derartige Datenanwendungen kein spezifisches Risiko für die Betroffenen bieten sollen.

Dies ist schlicht falsch. Sowohl die Verwendung von strafrechtlich relevanten Daten als auch der Betrieb von Informationsverbundsystemen oder Videoüberwachungen stellt für Betroffene ein spezifisches Risiko dar. Während strafrechtlich relevante Daten besonders dazu geeignet sind Personen zu brandmarken, können Betroffene die Auswirkungen der Verarbeitung von Daten in einem Informationsverbundsystem nur schwer bis unmöglich abschätzen - der Betrieb von Videoüberwachungen sorgt für einen ständigen Überwachungsdruck.

Von der geplanten Abschaffung der Vorabkontrolle für Informationsverbundsysteme, Videoüberwachungen oder Datenanwendungen, die strafrechtlich relevante Daten verwenden, muss abgesehen werden.

Grundsätzlich wäre es zwar zu begrüßen, dass zukünftig sämtliche Datenanwendungen, die Bewertungen von Personen vorsehen (sogenanntes „Scoring“) der Vorabkontrolle unterliegen. Die geplante Bestimmung ist aber zu allgemein formuliert und damit unzureichend.

Im Sinne der Betroffenen sollte das Datenschutzgesetz vorsehen, dass „Scoringverfahren“ generell gegenüber der Datenschutzkommission offengelegt werden müssen und im Rahmen der Vorabkontrolle auf sachliche Notwendigkeit, auf die Anwendung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens sowie die Eignung der verwendeten Datenarten für das „Scoring“ überprüft werden.

Falls „Scoringverfahren“ Voraussetzung oder Grundlage eines Vertragsabschlusses darstellen, sind sie vor Vertragsabschluss den Interessenten offen zu legen.

Gleichzeitig wird die geplante Änderung zu „Scoring“ dadurch ad absurdum geführt, dass Datenanwendungen, die aufgrund der ausdrücklichen Zustimmung durch Betroffene betrieben werden, von der Vorabkontrolle ausgenommen sein sollen. „Scorings“ sind schließlich bereits bei einer großen Anzahl von Wirtschaftszweigen wie beispielsweise dem Versandhandel, Banken, Leasingunternehmen, Möbelhändlern und Telekom-Unternehmen zwingende Voraussetzung für einen Vertragsabschluss. Aufgrund des wirtschaftlichen Ungleichgewichts, zwischen Betroffenen und Unternehmen, sind Betroffene regelmäßig dazu genötigt ihre Zustimmung zu einem „Scoringverfahren“ zu erteilen, sofern sie nicht aus dem Wirtschaftsleben ausgeschlossen werden möchten.

Darüberhinaus kann die Zustimmung der Betroffenen die Vorabkontrolle durch eine unabhängige Kontrollinstanz nicht ersetzen, da Betroffene nicht über die Aufsichts- und Kontrollfunktionen verfügen die derzeit der Datenschutzkommission zustehen. Betroffene haben gemäß § 14 Abs 2 Datenverarbeitungsregister-Verordnung 2002 (DVRV 2002) nicht einmal das Recht sich über ergriffene Datensicherheitsmaßnahmen eines Auftraggebers zu informieren.

In Kombination mit der geplanten Bestimmung, nach der Datenanwendungen die in Gesetzen oder Verordnungen vorgesehen sind und zu denen die Datenschutzkommission im Rahmen der Ausarbeitung eine Stellungnahme abgegeben hat ebenfalls von der Vorabkontrolle ausgenommen sein sollen, führt dies dazu, dass die Vorabkontrolle de facto abgeschafft wird.

Denn auch die Verwendung von sensiblen Daten ist, bis auf wenige Sonderfälle, ausschließlich aufgrund von gesetzlichen Vorschriften oder aufgrund der ausdrücklichen Zustimmung der Betroffenen zulässig (§ 9 DSG 2000) und würde somit, den geplanten Änderungen zufolge, im Normalfall nicht mehr der Vorabkontrolle unterliegen.

Von der geplanten Abschaffung der Vorabkontrolle für Datenanwendungen, die aufgrund der Zustimmung von Betroffenen erfolgt, ist daher dringend abzusehen.

1.3 Zukunft der Datenschutzkommission

Obwohl die Auflösung der Datenschutzkommission bereits beschlossen ist, sieht der Entwurf der DSG-Novelle 2012 eine Reihe neuer Aufgaben und Verpflichtungen für diese vor. Dabei ist unklar welche Einrichtung zukünftig die Aufgaben der Datenschutzkommission übernehmen soll.

Sowohl in der DatenschutzRL als auch in der geplanten Datenschutz-Grundverordnung ist die Einrichtung einer unabhängigen, kompetenten Kontrollstelle, welche die Einhaltung der entsprechenden europarechtlichen Bestimmungen und die Wahrung der Betroffenenrechte überwachen soll, vorgesehen. Fest steht, dass ein Verwaltungsgericht nicht in der Lage ist diese Kontroll- und Aufsichtsfunktionen zu übernehmen.

Des Weiteren ist in Kürze im Vertragsverletzungsverfahren der Europäischen Kommission gegen die Republik Österreich, aufgrund der nicht gegebenen Unabhängigkeit der Datenschutzkommission, mit einer Entscheidung zu rechnen, wobei der Generalanwalt des Europäischen Gerichtshofs eine Verurteilung von Österreich nahe legt. Die DSG-Novelle 2012 sollte diese Entwicklungen berücksichtigen.

Die DSG-Novelle 2012 hat die Schaffung einer unabhängigen, kompetenten, finanziell und personell ausreichend ausgestatteten Kontrollstelle vorzusehen.

2. DIE ÄNDERUNGEN IM DETAIL

2.1 § 17 Abs 2 Z 6 – Standardanwendungen

Derzeit können Datenanwendungen, die „von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist“ (§ 17 Abs 2 Z 6 DSG 2000), per Verordnung vom Bundeskanzler zu einer Standardanwendung erklärt werden.

„In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen“ (§ 17 Abs 2 Z 6 DSG 2000). Diese Anforderungen an die Verordnung, mit der Datenanwendungen zu Standardanwendungen erklärt werden können, soll ersatzlos gestrichen werden um Standardanwendungen zukünftig „in vereinfachter Form“ (Erläuterungen zu § 17 Abs 2 Z 6 DSG-Novelle 2012) ausgestalten zu können.

Es soll dem Bundeskanzler also ermöglicht werden Standardanwendungen auszugestalten ohne Angaben darüber machen zu müssen welche Datenarten verarbeitet werden dürfen, wer die Betroffenen bzw. die Übermittlungsempfänger sind und wie lange Daten aufbewahrt werden dürfen (§ 17 Abs 2 Z 6 DSG-Novelle 2012). Die DSG-Novelle 2012 lässt es somit völlig offen welche Angaben Standardanwendungen zukünftig enthalten sollen.

Art 18 Abs 2 DatenschutzRL sieht eine vereinfachte Meldung, wie dies im Rahmen der österreichischen Standard- und Muster-Verordnung vorgesehen ist jedoch nur vor, sofern folgendes festgelegt wird:

- die Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist,
- die Zweckbestimmungen der Verarbeitung,
- die Daten oder Kategorien der verarbeiteten Daten,
- die Kategorie(n) der betroffenen Personen,
- die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden und
- die Dauer der Aufbewahrung.

Der derzeitige § 17 Abs 2 Z 6 DSG 2000 stellt somit bereits jetzt die EU-rechtlich zulässige Mindestumsetzung dar. Standardanwendungen können daher nicht EU-rechtskonform in weiter vereinfachter Form ausgestaltet werden.

Darüberhinaus sollen Meldungen von Datenanwendungen, die nicht der Vorabkontrolle unterliegen, ab dem 1. September 2012 ohnehin ausschließlich automationsunterstützt auf ihre Vollständigkeit und Plausibilität geprüft und anschließend sofort registriert werden (§ 13 Abs 1 Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012). Durch die Meldung von Datenanwendungen die keiner Standardanwendung entsprechen und nicht der Vorabkontrolle unterliegen, entsteht sodann für das Datenverarbeitungsregister kein Aufwand mehr. Es ist somit nicht nachvollziehbar warum eine Notwendigkeit besteht Standardanwendungen abweichend von der derzeitigen Regelung auszugestalten.

Auch den Erläuterungen kann keine ausreichende Begründung entnommen werden, warum die derzeitige gesetzliche Regelung als unbefriedigend erachtet wird.

Um die Rechte der Betroffenen zu wahren und nicht gegen Art 18 Abs 2 DatenschutzRL zu verstoßen, ist von den vorgesehenen Änderungen des § 17 Abs 2 Z 6 DSG-Novelle 2012 abzusehen.

2.2 § 17 Abs 2 Z 7– Datenschutzbeauftragte / Meldepflicht

Es ist zu begrüßen, dass Datenanwendungen, die ohnehin der Kontrolle durch Datenschutzexperten – den Datenschutzbeauftragten – unterliegen, grundsätzlich nicht gemeldet werden müssen.

Vor allem in Hinblick darauf, dass durch den Wegfall der Meldepflicht auch die Vorabkontrolle von Datenanwendungen durch die Datenschutzkommission entfällt, sollten Datenschutzbeauftragte verpflichtet sein, sich, wie dies in Art 20 Abs 2 DatenschutzRL vorgesehen ist, bei Zweifeln über die Rechtmäßigkeit einer geplanten Datenanwendung, an die Datenschutzkommission zu wenden.

Durch eine derartige Regelung wäre sichergestellt, dass Datenschutzbeauftragte nicht warten müssen bis eine, ihrer Meinung nach zweifelhaft rechtmäßige Datenanwendung betrieben wird und damit potentiell Betroffenenrechte verletzt würden, sondern sie sich bereits vor Inbetriebnahme einer Datenanwendung an die Datenschutzkommission wenden können, um eine Verletzung von Betroffenenrechten zu verhindern.

In der DSG-Novelle 2012 ist klarzustellen, dass Datenschutzbeauftragte verpflichtet sind, sich bereits bei Zweifeln über die Rechtmäßigkeit von geplanten Datenanwendungen an die Datenschutzkommission zu wenden.

Systematisch könnte dies in § 30 Abs 1a DSG-Novelle 2012 festgehalten werden, der regelt, dass Datenschutzbeauftragte sich bei einem Verdacht einer Verletzung datenschutzrechtlicher Vorschriften an die Datenschutzkommission wenden können.

2.3 § 17a Abs 1 – Datenschutzbeauftragte / Bestellung

Während die DatenschutzRL die freiwillige Bestellung von Datenschutzbeauftragten vorsieht, ist in der geplanten Datenschutz-Grundverordnung bereits die verpflichtende Bestellung eines Datenschutzbeauftragten für sämtliche öffentliche Datenverarbeiter sowie für private Datenverarbeiter die 250 oder mehr Mitarbeiter beschäftigen vorgesehen (Art. 35 Datenschutz-Grundverordnung). Dadurch soll sichergestellt werden, dass das Grundrecht auf Privatsphäre der Betroffenen, ausreichend beachtet und nicht verletzt wird.

Es ist daher zu begrüßen, dass der Vorschlag der ARGE DATEN aus ihrer Stellungnahme zur DSG-Novelle 2010 (<ftp://ftp.freenet.at/privacy/gesetze/dsg-novelle-2010.pdf>) aufgegriffen wurde und nunmehr auch in Österreich die freiwillige Bestellung von Datenschutzbeauftragten vorgesehen sein soll.

Schließlich ist die Artikel-29-Datenschutzgruppe bereits 2005 zu folgendem Erkenntnis gelangt: „In Anbetracht der positiven Erfahrungen in den Mitgliedstaaten, in denen Datenschutzbeauftragte bereits eingeführt worden sind bzw. traditionell vorhanden waren, empfiehlt sich ein verstärkter Rückgriff auf Datenschutzbeauftragte anstelle von Meldeanforderungen“¹.

Neben der freiwilligen Möglichkeit, einen Datenschutzbeauftragten zu bestellen, sollte für Auftraggeber mit einer bestimmten Mindestanzahl von Beschäftigten, die verpflichtende Bestellung eines Datenschutzbeauftragten vorgesehen werden.

Sowohl in der DatenschutzRL als auch in der geplanten Datenschutz-Grundverordnung ist ausdrücklich die Möglichkeit vorgesehen, dass interne aber auch externe Personen die Aufgaben des Datenschutzbeauftragten übernehmen können.

Während diese Möglichkeit im geplanten § 17a Abs 1 DSG-Novelle 2012 grundsätzlich nicht ausgeschlossen wird, wird sie nicht ausdrücklich erwähnt. In den Erläuterungen finden sich keine Hinweise darüber, ob auch die Bestellung eines externen Datenschutzbeauftragten zulässig sein soll.

In § 17a Abs 1 DSG-Novelle 2012 ist ausdrücklich klarzustellen, dass auch externe Personen zum Datenschutzbeauftragten bestellt werden können.

2.4 § 17a Abs 2 – Datenschutzbeauftragte / Unbefangenheit

§ 17a Abs 2 DSG-Novelle 2012 hält zwar allgemein fest, dass ausschließlich fachkundige und zuverlässige Personen zum Datenschutzbeauftragten bestellt werden dürfen, insbesondere in Hinblick auf die Zuverlässigkeit fehlt aber ein Hinweis auf eine entsprechende Unbefangenheit. Dies könnte zu der Situation führen, dass ein Geschäftsführer sich selbst zum Datenschutzbeauftragten ernennt, wodurch die Aufsichts- und Kontrollfunktion des Datenschutzbeauftragten nicht mehr gegeben wäre.

¹ Art-29-Datenschutzgruppe: WP 106

§ 17a Abs 2 DSG-Novelle 2012 muss festhalten, dass ausschließlich Personen zu Datenschutzbeauftragten bestellt werden können, deren sonstige berufliche Verpflichtungen der Erfüllung der Aufgaben des Datenschutzbeauftragten nicht entgegen stehen.

2.5 § 17a Abs 3 – Liste der Datenschutzbeauftragten

Gemäß dieser Bestimmung hat die Datenschutzkommission auf ihrer Homepage eine Liste der zu Datenschutzbeauftragten bestellten Personen inkl. derer beruflicher Kontaktdaten zu veröffentlichen. Dadurch ist sichergestellt, dass Betroffene unmittelbar wissen, ob ein Auftraggeber einen Datenschutzbeauftragten bestellt hat und wie dieser kontaktiert werden kann. Diese geplante Liste erfüllt somit den Informationszweck des Datenverarbeitungsregisters in Hinblick auf Datenanwendungen die von Auftraggebern betrieben werden welche einen Datenschutzbeauftragten bestellt haben.

Die geplante, öffentliche Liste der Datenschutzbeauftragten ist zu begrüßen.

2.6 § 17a Abs 4 – Datenschutzbeauftragte / Datenanwendungen

Dass der Datenschutzbeauftragte ein Verzeichnis der betriebenen Datenanwendungen führen soll ist logisch und ergibt sich bereits dadurch, dass Datenanwendungen die seiner Kontrolle unterliegen nicht gemeldet werden müssen. Somit übernimmt das zu führende Verzeichnis den Informationszweck des Datenverarbeitungsregisters.

Beim Datenverarbeitungsregister handelt es sich um eine öffentlich zugängliche Datenanwendung - jedermann kann kostenlos in dieses Einsicht nehmen. In das geplante Verzeichnis sollen allerdings ausschließlich Betroffene Einsicht nehmen können – dies ist problematisch und EU-rechtswidrig.

Datenschutzbeauftragte könnten schließlich nur beurteilen, ob es sich bei einer Person die in das Verzeichnis der Datenanwendungen Einsicht nehmen möchte um einen Betroffenen handelt, sofern abgeklärt wird, ob tatsächlich Daten über die anfragende Person verarbeitet werden. In diesem Zusammenhang müssten Datenschutzbeauftragte sodann auch die Identität der anfragenden Person überprüfen.

Weiters bestimmt Art 21 Abs 3 DatenschutzRL, dass, sofern Datenanwendungen nicht gemeldet werden müssen, wie dies bei der Bestellung von Datenschutzbeauftragten der Fall ist, Auftraggeber jedermann Informationen über die von ihnen betriebenen Datenanwendungen verfügbar machen müssen.

§ 17a Abs 4 DSG-Novelle 2012 muss insofern konkretisiert werden, als dass – analog zum Datenverarbeitungsregister – jedermann in das Verzeichnis der Datenanwendungen des Auftraggebers, welches durch den Datenschutzbeauftragten zu führen ist, Einsicht nehmen kann.

In § 17a Abs 4 DSG-Novelle 2012 ist festzuhalten, dass die Einsicht in das Verzeichnis der Datenanwendungen des Auftraggebers kostenlos ist.

Weder im vorgeschlagenen Gesetzestext zu § 17a Abs 4 DSG-Novelle 2012 noch in den Erläuterungen finden sich Mindestanforderungen die das Verzeichnis der Anwendungen erfüllen muss. Es ist somit unklar welche Informationen das Verzeichnis enthalten soll. Dies entspricht ebenfalls nicht den Vorgaben des Art 21 Abs 3 DatenschutzRL.

§ 17a Abs 4 DSG-Novelle 2012 hat, gemäß Art 21 Abs 3 DatenschutzRL, Mindestanforderungen vorzugeben, denen das Verzeichnis der Datenanwendungen, welches durch den Datenschutzbeauftragten geführt werden soll, gerecht werden muss.

Als Orientierungshilfe für Mindestanforderungen kann neben Art 21 Abs 3 DatenschutzRL auch § 19 DSG 2000 bzw. die Anlage 2 der Datenverarbeitungsregister-Verordnung 2012 dienen in denen festgehalten ist welche Angaben bei der Meldung einer Datenanwendung zu machen sind.

Weiters enthält der geplante § 17a Abs 4 DSG-Novelle 2012 keinerlei Bestimmungen in Bezug auf die Kontrolle des Datenschutzbeauftragten. Zwar würde das Nichtführen des Verzeichnis der Datenanwendungen womöglich gegen den geplanten § 52 Abs 2 Z 11 DSG-Novelle 2012 verstoßen, in Zusammenhang mit fehlenden Mindestanforderungen die das Verzeichnis erfüllen muss, wäre ein vorsätzliches Fehlverhalten eines Datenschutzbeauftragten allerdings nur schwer bis unmöglich nachzuweisen. Das Nichtführen oder das Führen eines informationslosen Verzeichnisses von Datenanwendungen würde die Rechte der Betroffenen aber unverhältnismäßig beeinträchtigen. Aus diesem Grund sollten der Datenschutzkommission entsprechende Kontrollbefugnisse eingeräumt werden.

In der DSG-Novelle 2012 ist vorzusehen, dass der Datenschutzkommission ein ständiges Recht eingeräumt wird, das vom Datenschutzbeauftragten zu führende Verzeichnis der Datenanwendungen, in Hinblick auf Vollständigkeit und die Erfüllung bestimmter Mindestanforderungen zu kontrollieren.

Nur dadurch kann sichergestellt werden, dass die Rechte der Betroffenen nicht beeinträchtigt werden. Systematisch könnte das Kontrollrecht der Datenschutzkommission in § 30 DSG 2000 geregelt werden welcher auch die sonstigen Kontrollbefugnisse der Datenschutzkommission festhält.

Darüberhinaus hält § 17a Abs 4 DSG-Novelle 2012 fest, dass sich Betroffene jederzeit an den Datenschutzbeauftragten wenden können.

§ 17a Abs 4 DSG-Novelle 2012 hat klar zu stellen, dass nicht nur Anfragen von Betroffenen an Datenschutzbeauftragte, sondern bereits Anfragen von Personen die glaubhaft machen Betroffene zu sein, mit keinen Kosten für diese verbunden sind.

Um zu Verhindern, dass das Anfragerecht von Betroffenen missbraucht wird, hat § 17a Abs 4 DSG-Novelle 2012 festzuhalten, dass Anfragen an Datenschutzbeauftragte sich auf dessen Tätigkeit bzw. dessen Pflichten gegenüber Betroffenen beziehen müssen.

2.7 § 17a Abs 5 – Datenschutzbeauftragte / Unterrichtung

Gemäß dieser Bestimmung sind Datenschutzbeauftragte vom Auftraggeber „rechtzeitig“ über das Vorhaben neue Datenanwendungen einzusetzen zu informieren.

§ 17a Abs 5 DSGVO-Novelle 2012 hat festzuhalten, dass Datenanwendungen erst in Betrieb genommen werden dürfen, sofern dem Datenschutzbeauftragten ausreichende Gelegenheit zur Abgabe einer Stellungnahme gegeben wurde.

§ 17a Abs 5 DSGVO-Novelle 2012 hat vorzusehen, dass Stellungnahmen von Datenschutzbeauftragten bzw. durch diese ergriffene Handlungsmaßnahmen ordnungsgemäß dokumentiert werden müssen und der Datenschutzkommission auf Anfrage zur Verfügung gestellt werden müssen.

Auf diese Art wird sichergestellt, dass die Information des Datenschutzbeauftragten nicht zu einer Nebensache verkommt, sondern eine zentrale Rolle bei der Planung von neuen Datenanwendungen einnimmt. Darüberhinaus sorgt die Dokumentationspflicht für mehr Transparenz und trägt somit letztlich zur Wahrung der Betroffenenrechte bei.

2.8 § 17a Abs 10 – Datenschutzbeauftragung / Verantwortung

§ 17a Abs 10 DSGVO-Novelle 2012 sieht vor, dass die letztendliche Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen beim Auftraggeber verbleibt. Wie aus den Erläuterungen richtig hervorgeht ist nur dadurch sichergestellt, dass Auftraggeber sich nicht durch die Bestellung eines Datenschutzbeauftragten von ihrer datenschutzrechtlichen Verantwortung befreien können. Diese Bestimmung trägt somit zur Stärkung von Datenschutzbeauftragten bei, da Auftraggeber, aufgrund ihrer Verantwortung dazu angehalten werden, Maßnahmen, die von Datenschutzbeauftragten vorgeschlagen werden, umzusetzen.

Dass gem. § 17a Abs 10 DSGVO-Novelle 2012 die datenschutzrechtliche Verantwortung bei den Auftraggebern – und nicht den Datenschutzbeauftragten – verbleibt ist zu begrüßen.

Unabhängig von den Bestimmungen der §§ 17a Abs 1 und 52 Abs 2 Z 10 DSGVO-Novelle 2012 sollte § 17a DSGVO-Novelle 2012 für Datenschutzbeauftragte die Möglichkeit vorsehen ihre Position freiwillig niederzulegen, sofern ihnen Auftraggeber, beispielsweise durch die Vernachlässigung ihre Pflichten nach dem § 17a Abs 5 bis 8 DSGVO-Novelle 2012, die Erfüllung Ihrer Aufgaben unmöglich machen oder diese selbst zu der Ansicht gelangen, dass sie die Voraussetzungen für die Erfüllung ihrer Aufgaben nicht mehr erfüllen.

§ 17a DSGVO-Novelle 2012 sollte für Datenschutzbeauftragte die freiwillige Möglichkeit zur Zurücklegung ihrer Funktion vorsehen, sofern diese zur Ansicht gelangen, dass sie ihre Pflichten nicht mehr erfüllen können.

2.9 § 18 Abs 2, 3 und 4 – Vorabkontrolle / allgemein

Die DSGVO-Novelle 2012 plant § 18 DSGVO 2000 umfassend zu überarbeiten und zahlreiche Datenanwendungen die derzeit der Vorabkontrolle unterliegen zukünftig von der Vorabkontrollpflicht auszunehmen.

In diesem Zusammenhang muss darauf hingewiesen werden, dass die Vorabkontrolle eine zentrale und wichtige Rolle im europäischen Datenschutzrecht einnimmt. Sinn und Zweck der Vorabkontrolle ist es, dass Datenanwendungen die spezifische Risiken für Betroffene bergen, erst nach einer Prüfung betrieben werden dürfen (Art 20 Abs 1 DatenschutzRL).

Gleichzeitig gelangen mehrere Bestimmungen des österreichischen Datenschutzgesetzes nur bei vorabkontrollpflichtigen Datenanwendungen zur Anwendung. So muss beispielsweise die geplante Heranziehung von Dienstleistern der Datenschutzkommission mitgeteilt werden, falls diesen Daten einer vorabkontrollpflichtigen Datenanwendung überlassen werden sollen (§ 10 Abs 2 DSG 2000). Weiters kann die Datenschutzkommission den Betrieb einer vorabkontrollpflichtigen Datenanwendung von der Erfüllung von Auflagen, Bedingungen oder Befristungen abhängig machen (§ 21 Abs 2 DSG 2000). Nicht zuletzt dürfen ausschließlich vorabkontrollpflichtige Datenanwendungen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden (§ 30 Abs 3 DSG 2000).

Die Unterscheidung zwischen vorabkontrollpflichtigen und nicht-vorabkontrollpflichtigen Datenanwendungen ist - in Hinblick auf die Wahrung der Betroffenenrechte - von entscheidender Bedeutung und muss mit der notwendigen Sorgfalt getroffen werden.

2.10 § 18 Abs 2 – Vorabkontrolle / strafrechtlich relevante Daten

Zukünftig soll, gemäß § 18 Abs 2 DSG-Novelle 2012, die Verwendung von strafrechtlich relevanten Daten (Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen - § 8 Abs 4 DSG 2000) nicht mehr der Vorabkontrolle unterliegen.

Somit soll es letztendlich den Auftraggebern überlassen sein zu beurteilen, ob ihre eigenen Interessen die schutzwürdigen Geheimhaltungsinteressen der Betroffenen überwiegen bzw. die Interessen der Betroffenen gewahrt werden. Die Annahme, dass Auftraggeber eine derartige Interessensabwägung objektiv durchführen können ist realitätsfremd.

Ausschließlich ein unabhängiger, in Datenschutzangelegenheiten sensibilisierter Dritter – wie die Datenschutzkommission oder ein unabhängiger Datenschutzbeauftragter – kann diese Interessensabwägung objektiv durchführen.

Auch wenn strafrechtlich relevante Daten nicht zu den in § 4 Z 2 DSG 2000 definierten sensiblen bzw. besonders schutzwürdige Daten zählen, handelt es sich doch um Daten die spezifische Risiken für die Betroffenen bergen. Schließlich sind strafrechtlich relevante Daten ganz besonders dazu geeignet, Personen öffentlich bloß zu stellen – zu brandmarken. Dabei birgt nicht erst die Verwendung von Daten über strafrechtliche Verurteilungen spezifische Risiken für die Betroffenen. Bereits die Verwendung von Daten über den Verdacht der Begehung einer Straftat ist geeignet um eine Person in schlechtes Licht zu rücken oder ihren Ruf zu zerstören.

Bei strafrechtlich relevanten Daten handelt es sich um Daten die spezifische Risiken für die Rechte und Freiheiten der Betroffenen bergen. Die Verarbeitung von strafrechtlich relevanten Daten muss daher weiterhin der Vorabkontrolle unterliegen.

2.11 § 18 Abs 2 – Vorabkontrolle / Informationsverbundsysteme

§ 18 Abs 2 DSG-Novelle 2012 sieht ebenfalls vor, dass Datenanwendungen, die in einem Informationsverbundsystem betrieben werden, nicht mehr der Vorabkontrolle unterliegen.

Informationsverbundsysteme erlauben die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber. Unterschiedlichen Auftraggebern ist es somit möglich Daten über ein und dieselben Betroffenen zu verarbeiten bzw. können Auftraggeber auch auf die Daten anderer Auftraggeber zugreifen. In Summe ergibt sich dadurch für die an einem Informationsverbundsystem teilnehmenden Auftraggeber ein weit umfassenderes Bild über die Betroffenen bzw. erhalten Auftraggeber Zugriff auf die Daten einer Vielzahl von Betroffenen zu denen ansonsten womöglich keine (Geschäfts)Beziehung besteht.

Trotz der Bestimmung des per 1. September in Kraft tretenden § 6 Abs 1 DVRV 2012, wonach Betroffene per DVR-Online Einsicht in die Liste der registrierten Informationsverbundsysteme, sowie die an diesen teilnehmenden Auftraggeber nehmen können, wissen Betroffene grundsätzlich nicht welche Auftraggeber tatsächlich auf ihre Daten zugreifen – dies stellt ein spezifisches Risiko für die Beeinträchtigung der Rechte der Betroffenen dar.

Zur Wahrung der Rechte der Betroffenen müssen Informationsverbundsysteme, aufgrund der von diesen ausgehenden spezifischen Risiken, auch zukünftig der Vorabkontrolle durch die Datenschutzkommission unterliegen.

Die Vorabkontrolle von Informationsverbundsystemen sorgt aufgrund des § 50 Abs 2a DSG 2000, demnach Meldungen über die Teilnahme an einem Informationsverbundsystem sich auf die Meldung eines bereits registrierten Auftraggebers beziehen können, nicht für unverhältnismäßigen Arbeitsaufwand für die Datenschutzkommission, da ein Informationsverbundsystem – genau wie eine Datenanwendung – nur einmal geprüft werden muss.

2.12 § 18 Abs 2 Z 2 – Vorabkontrolle / Bewertung von Betroffenen

§ 18 Abs 2 Z 2 DSG-Novelle 2012 sieht vor, dass nicht wie bisher, Datenanwendungen welche die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben, der Vorabkontrolle unterliegen, sondern sämtliche Datenanwendungen deren Zweck es ist, die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeit, seiner Leistung, seiner wirtschaftlichen Lage oder seines Verhaltens zu bewerten.

Dass generell Datenanwendungen die, die Bewertung von Betroffenen vorsehen (sog. „Scoring“), der Vorabkontrolle unterliegen sollen ist grundsätzlich zu begrüßen.

Diese Regelung ist allerdings zu allgemein formuliert und damit zu kurz gefasst. Zwar sieht das DSG 2000 in § 49 DSG 2000 vor, dass Betroffene grundsätzlich keiner „Automatisierten Einzelentscheidung“ unterworfen werden dürfen. Diese Schutzmaßnahme gegen die willkürliche Verwertung - oft allgemeiner – Persönlichkeitsangaben, hat sich aber als nicht tragfähig erwiesen, da diese auf eine vollautomatisierte Entscheidung abstellt. Eine solche findet beim „Scoring“ in der Praxis aber nicht statt, denn „Scoringwerte“ werden offiziell nur als Empfehlungen ausgewiesen. Mitarbeiter von Unternehmen, die „Scorings“ anwenden haben praktisch aber keine Möglichkeit eine andere Entscheidung zu treffen als es das „Scoring“ „empfiehlt“ bzw. vorgibt.

Die DSG-Novelle 2012 sollte daher dazu genutzt werden den Bereich „Scoring“ umfassend zu Regeln, wie dies beispielsweise in Deutschland (§ 28b Bundesdatenschutzgesetz) der Fall ist.

Im Sinne der Betroffenen sollte das Datenschutzgesetz vorsehen, dass „Scoringverfahren“ generell gegenüber der Datenschutzkommission offengelegt werden müssen und im Rahmen der Vorabkontrolle auf sachliche Notwendigkeit, auf die Anwendung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahren sowie die Eignung der verwendeten Datenarten für das „Scoring“ überprüft werden.

Falls „Scoringverfahren“ Voraussetzung oder Grundlage eines Vertragsabschlusses darstellen, sind sie vor Vertragsabschluss den Interessenten offen zu legen.

§ 18 Abs 2 Z 2 DSG-Novelle 2012 sollte darüberhinaus auf die Verwendung iSd § 4 Z 8 DSG 2000 abzielen und in Hinblick auf grammatikalische Korrektheit überarbeitet werden.

2.13 § 18 Abs 3 – Vorabkontrolle / Zustimmung der Betroffenen

Dass Datenanwendungen, die mit ausdrücklicher Zustimmung des Betroffenen vorgenommen werden, zukünftig generell keiner Vorabkontrolle unterliegen sollen ist entschieden abzulehnen.

Selbst wenn außer Acht gelassen wird, dass Zustimmungserklärungen, aufgrund von Informationsdefiziten oder Abhängigkeitsverhältnissen, regelmäßig nicht den Anforderungen des § 4 Z 14 DSG 2000 gerecht werden, kann die Zustimmung von Betroffenen nicht die Aufsichts- und Kontrollfunktion der Datenschutzkommission ersetzen.

Schließlich haben Betroffene nicht - wie die Datenschutzkommission - das Recht Datenanwendungen auf rechtswidrige Datenverwendung zu überprüfen (§ 30 Abs 3 DSG 2000) oder Einschau bei Auftraggebern vorzunehmen (§ 30 Abs 4 DSG 2000).

Aus diesem Grund kann ausschließlich eine unabhängige und mit dem nötigen Fachwissen ausgestattete Kontrollstelle, wie die Datenschutzkommission oder wie Datenschutzbeauftragte, abschätzen, in wie weit eine Datenanwendung, die spezifische Risiken für Betroffene birgt, geeignete Garantien zu deren Schutz bietet und daher betrieben werden darf.

Die Zustimmung von Betroffenen darf, bei der Beurteilung ob eine Datenanwendung spezifische Risiken birgt - und demnach vorabkontrollpflichtig ist - keine Rolle spielen.

2.14 § 18 Abs 3 – Vorabkontrolle / Datenanwendungen aufgrund von Gesetzen oder Verordnungen

Dass, wie in § 18 Abs 3 DSG-Novelle 2012 vorgesehen, Datenanwendungen, die aufgrund von Gesetzen oder Verordnungen vorgenommen werden und geeignete Garantien zum Schutz der Betroffenen vorsehen, nicht mehr der Vorabkontrolle unterliegen sollen, sofern der Datenschutzkommission im Zuge der Ausarbeitung Gelegenheit zur Stellungnahme gegeben wurde und einer eventuellen Stellungnahme entsprochen wird, ist grundsätzlich zu begrüßen und entspricht der DatenschutzRL.

Zur abschließenden Klarstellung sollte § 18 Abs 3 DSG-Novelle 2012 vorsehen, dass auch eventuelle Empfängerkreise von Datenübermittlungen aus Datenanwendungen, die aufgrund entsprechend erlassener Gesetze bzw. Verordnungen nicht vorabkontrollpflichtig sind, im Gesetz bzw. der Verordnung genannt werden müssen.

Denn während aufgrund Art 20 Abs 3 iVm Art 2 lit b DatenschutzRL, an dem sich § 18 Abs 3 DSG-Novelle 2012 orientiert, unter dem Begriff Verarbeitung auch Übermittlungen erfasst sind, stellen Übermittlungen keinen Teil des Begriffes „Verarbeiten“ iSd § 4 Z 9 DSG 2000 dar.

Datenanwendungen welche gemäß des geplanten § 18 Abs 3 DSG-Novelle 2012 aufgrund von Gesetzen oder Verordnungen nicht vorabkontrollpflichtig sind, haben sicher zu stellen, dass die Art der Verwendung iSd § 4 Z 8 DSG 2000 festgelegt wird und geeignete Garantien bei der Verwendung von Daten ergriffen werden.

2.15 § 18 Abs 4 – Vorabkontrolle / Liste gesetzlicher Datenanwendungen

Die geplante Liste der in Gesetzen oder Verordnungen vorgesehenen und gem. § 18 Abs 3 DSG-Novelle 2012 nicht vorabkontrollpflichtigen Datenanwendungen dient sowohl der Information der Betroffenen als auch der Auftraggeber und ist daher zu begrüßen.

Anforderungen an die gemäß § 18 Abs 4 DSG-Novelle 2012 von der Datenschutzkommission zur Verfügung zu stellenden Liste, wie beispielsweise dass diese die Fundstelle der Datenanwendung wiedergeben muss, sollten aus dem Gesetzestext und nicht aus den Erläuterungen hervorgehen.

Dadurch, dass es sich bei Datenanwendungen die gem. § 18 Abs 3 DSG-Novelle 2012 nicht vorabkontrollpflichtig sind um Datenanwendungen handelt die grundsätzlich spezifische Risiken bergen – und somit vorabkontrollpflichtig wären - sollten der Datenschutzkommission analog zu § 30 Abs 3 DSG 2000 entsprechende Kontrollbefugnisse eingeräumt werden.

In der DSG-Novelle 2012 ist klarzustellen, dass die Kontrollbefugnisse, die der Datenschutzkommission gemäß § 30 Abs 3 DSG 2000 zustehen, auch auf Datenanwendungen anzuwenden sind, die gemäß § 18 Abs 3 DSG-Novelle 2012 von der Vorabkontrolle befreit sind.

2.16 § 30 Abs 1a – Datenschutzbeauftragte / Eingaberecht

Bereits unter Punkt 2.4, den Anmerkungen zu § 17a Abs 2 DSG-Novelle 2012, wurde ausgeführt, dass Datenschutzbeauftragten, in Anlehnung an Art 20 Abs 2 DatenschutzRL, die Möglichkeit gegeben werden soll, sich auch bei Zweifeln über die Rechtmäßigkeit von geplanten Datenanwendungen an die Datenschutzkommission wenden zu können.

Datenschutzbeauftragte sollten bereits bei Zweifeln über die Rechtmäßigkeit geplanter Datenanwendungen über ein Eingaberecht an die Datenschutzkommission verfügen.

2.17 § 30 Abs 2a – Überprüfung der Meldepflicht

Dass die Datenschutzkommission Datenanwendungen aufgrund des Verdachts von Datenschutzbeauftragten, dass diese Datenanwendungen datenschutzrechtliche Vorschriften verletzen, überprüfen können soll, ist zu begrüßen.

Bei der geplanten Änderung wird jedoch übersehen, dass Datenanwendungen die der Kontrolle durch Datenschutzbeauftragte unterliegen gem. § 17 Abs 2 Z 7 DSG - Novelle 2012 nicht meldepflichtig sind. Die Bestimmungen des § 30 Abs 2a DSG-Novelle 2012 würde somit auf diese Datenwendungen keine Anwendung finden.

§ 30 Abs 2a DSG-Novelle 2012 ist insofern zu konkretisieren, als dass dieser auch auf Datenanwendungen anzuwenden ist, die der Kontrolle durch Datenschutzbeauftragte unterliegen und somit nicht meldepflichtig sind.

Die §§ 22 und 22a DSG-Novelle 2012 sind entsprechend zu überarbeiten, sodass diese auch auf Datenanwendungen zutreffen die der Kontrolle durch Datenschutzbeauftragte unterliegen und daher nicht meldepflichtig sind.

Um die Überprüfung von Datenanwendungen, welche aufgrund der Bestellung von Datenschutzbeauftragten nicht meldepflichtig sind, praktisch zu ermöglichen, wird auf die Ausführungen zu Punkt 2.6, den Anmerkungen zu § 17a Abs 4 DSG-Novelle 2012 hingewiesen.

2.18 § 30 Abs 4a – Unterstützung der Datenschutzkommission

§ 30 Abs 4a DSG-Novelle 2012 stellt klar, dass Bezirksverwaltungsbehörden oder Landespolizeidirektionen verpflichtet sind, auf Ersuchen der Datenschutzkommission deren Befugnisse wahrzunehmen.

Die Unterstützung der Datenschutzkommission durch Bezirksverwaltungsbehörden oder Landespolizeidirektionen wird begrüßt.

2.19 § 38 Abs 3 – Stellungnahme durch die Datenschutzkommission

Es spricht grundsätzlich nichts dagegen, dass die Datenschutzkommission zukünftig auch vor der Erlassung von Gesetzen, die wesentliche Fragen des Datenschutzes betreffen, anzuhören ist. In Verbindung mit dem geplanten § 18 Abs 3 DSG-Novelle 2012 kann dies dazu beitragen, die Rechte der Betroffenen besser zu wahren und spätere Vorabkontrollen von Datenanwendungen zu vermeiden.

Es muss allerdings darauf hingewiesen werden, dass es bereits jetzt gemäß § 41 DSG 2000 Aufgabe des Datenschutzrates ist, „Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind“ (§ 41 Abs 2 Z 2 DSG 2000).

Des Weiteren muss ausdrücklich darauf hingewiesen werden, dass die Datenschutzkommission bereits in Hinblick auf die Erfüllung ihre derzeit bestehenden Aufgaben deutlich unterbesetzt ist. Zusätzliche Aufgaben könnten daher zu einer weiteren Überlastung der Datenschutzkommission und somit insgesamt dazu beitragen, dass Betroffenenrechte nicht ausreichend gewahrt werden.

Gleichzeitig wurde bereits die Auflösung der Datenschutzkommission beschlossen, wobei unklar ist welche Kontrollstelle die Aufgaben der Datenschutzkommission zukünftig übernehmen soll.

Anstatt einer Behörde, die es in weniger als eineinhalb Jahren nicht mehr geben wird, neue Aufgaben und Pflichten zuzuteilen, sollte die DSG-Novelle 2012 dazu genutzt werden die Aufgaben und Kompetenzen einer neuen Kontrollstelle zu regeln, die sowohl aufgrund der DatenschutzRL als auch aufgrund der Datenschutz-Grundverordnung vorgesehen ist.

Die DSG-Novelle 2012 hat die Schaffung einer unabhängigen, kompetenten, finanziell und personell ausreichend ausgestatteten Kontrollstelle vorzusehen.

2.20 § 50a Abs 7 – Videoüberwachung / Bewertung von Betroffenen

Neben dem Verbot, Daten von Videoüberwachungen mit anderen Bilddaten abzugleichen oder diese nach sensiblen Daten zu durchsuchen, soll zukünftig auch die Ermittlung von sensiblen Daten sowie das Durchsuchen nach bzw. die Ermittlung von Daten die zur Bewertung von Personen geeignet sind unzulässig sein.

Dass Videodaten nicht nach Daten, die dazu geeignet sind die Persönlichkeit der Betroffenen zu bewerten, durchsucht werden dürfen bzw. dass derartige Daten nicht aus Daten von Videoüberwachungen ermittelt werden dürfen, ist zu begrüßen.

2.21 §§ 50b Abs 2, 50c Abs 1 – Videoüberwachung / Vorabkontrolle

Videoüberwachungen greifen besonders stark in die Rechte Betroffener ein, da diese einen ständigen Überwachungsdruck erzeugen. Videoüberwachungen stellen somit ein spezifisches Risiko für die Rechte und Freiheiten der Betroffenen dar.

Zwar ist in § 50a Abs 2 DSG 2000 ausdrücklich vorgesehen, dass Videoüberwachungen dem Verhältnismäßigkeitsgrundsatz des § 7 Abs 3 DSG 2000 gerecht werden müssen. Vor allem aufgrund der teilweise geringen Kosten, die für die Installation und den Betrieb von Videoüberwachungen anfallen, sind Auftraggeber aber nicht in der Lage eine objektive Interessensabwägung vorzunehmen. Sofern Videoüberwachungen nicht mehr der Vorabkontrolle unterliegen, besteht daher die dringende Gefahr, dass es zu einem uferlosen Anstieg von Videoüberwachungen unter Missachtung der Bestimmungen des Datenschutzgesetzes und somit unter Verletzung von Betroffenenrechten kommen wird.

Aufgrund des ständigen Überwachungsdrucks, der von Videoüberwachungen ausgeht, sind auch Betroffene regelmäßig nicht dazu in der Lage, objektiv zu beurteilen, ob eine Videoüberwachung dem Verhältnismäßigkeitsgrundsatz gerecht wird – ihrer Meinung nach werden Videoüberwachungen in jedem Fall unverhältnismäßig in ihr Grundrecht auf Datenschutz eingreifen.

Derzeit können sich Betroffene von Videoüberwachungen darauf verlassen, dass eine unabhängige Kontrollstelle – die Datenschutzkommission – den Betrieb einer Videoüberwachung ausnahmsweise genehmigt hat, nachdem diese zu dem Schluss gekommen ist, dass Eingriffe in das Grundrecht auf Datenschutz, durch den Betrieb der Videoüberwachung, nur im erforderlichen Ausmaß und mit dem gelindesten zur Verfügung stehenden Mittel erfolgen.

Fällt diese Kontrollfunktion weg, führt dies dazu, dass Betroffene grundsätzlich davon ausgehen werden, dass Videoüberwachungen nicht dem Verhältnismäßigkeitsgrundsatz entsprechen. Dies wird zu einer Vielzahl von Eingaben führen, welche neben der Datenschutzkommission auch für die Betreiber der Videoüberwachung einen, im Vergleich zur Vorabkontrolle, unverhältnismäßigen Aufwand verursachen werden.

Ausschließlich eine unabhängige Kontrollstelle – wie die Datenschutzkommission oder Datenschutzbeauftragte – sind in der Lage objektiv zu beurteilen ob der Betrieb von Videoüberwachungen iSd § 7 Abs 3 DSG 2000 verhältnismäßig ist.

Videoüberwachungen müssen daher auch weiter unbedingt der Vorabkontrolle unterliegen.

Insbesondere für Videoüberwachungen deren aufgezeichnete Daten für einen 72 Stunden übersteigenden Zeitraum aufbewahrt werden sollen ist die Vorabkontrolle beizubehalten.

2.22 § 50c Abs 2 – Analoge Videoüberwachungen

Dass zukünftig auch analoge Videoüberwachungen zu melden sind ist zu begrüßen. Die technische Ausgestaltung einer Videoüberwachung ist schließlich unbedeutend für deren Eignung Betroffenenrechte zu beeinträchtigen.

§ 50c Abs 2 DSG-Novelle 2012 hat festzuhalten, dass zukünftig auch analoge Videoüberwachungen der Vorabkontrolle unterliegen.

2.23 § 52 Abs 2 Z 10 – Strafbestimmung / Behinderung von Datenschutzbeauftragten

§ 52 Abs 2 Z 10 DSG 2000 stellt es unter Strafe, falls Auftraggeber Datenschutzbeauftragte an der Erfüllung ihrer Pflichten vorsätzlich hindern. Klarstellend sollte es ebenfalls strafbar sein, wenn Auftraggeber Datenschutzbeauftragten nicht die gesetzlich vorgesehene Fort- und Weiterbildung ermöglichen.

In § 52 Abs 2 DSG-Novelle 2012 ist festzuhalten, dass es für Auftraggeber strafbar ist, wenn diese dem Datenschutzbeauftragten, die in § 17a Abs 8 DSG-Novelle 2012 vorgesehene, Fort- und Weiterbildung nicht ermöglichen.

2.24 § 52 Abs 2 – Strafbestimmung / Abberufung von Datenschutzbeauftragten

Neben den geplanten die Datenschutzbeauftragten betreffenden Strafbestimmungen wird vermisst, dass einerseits Auftraggeber die Pflicht haben müssen Datenschutzbeauftragte von ihrer Funktion zu entheben sobald diese ihre Aufgabe nicht mehr erfüllen können, andererseits sollte es auch für Datenschutzbeauftragte verpflichtend sein ihre Funktion zurück zu legen, wenn diese selbst zur Ansicht gelangen, dass sie ihre Pflichten nicht mehr ordentlich erfüllen können.

§ 52 Abs 2 DSG-Novelle 2012 hat es vorzusehen, dass es für Auftraggeber strafbar ist, wenn diese bestellte Datenschutzbeauftragte nicht von ihrer Funktion entheben, sobald diese den Voraussetzungen zur Erfüllung ihrer Pflichten nicht mehr gerecht werden.

In § 52 Abs 2 DSG-Novelle 2012 ist vorzusehen, dass es für Datenschutzbeauftragte strafbar ist, wenn diese ihre Funktion nicht freiwillig zurücklegen, sobald sie ihre Pflichten nicht mehr erfüllen können.

Es wird auf die Ausführungen unter Punkt 2.8, den Anmerkungen zu § 17a Abs 10 DSG-Novelle 2012, verwiesen.

2.25 § 61 Abs 9 und Abs 10 – Automatische Registrierung

Gemäß § 61 Abs 9 bzw. Abs 10 DSGVO-Novelle 2012 sollen bereits gemeldete aber noch nicht registrierte, Datenanwendungen, die aufgrund der Bestimmungen der DSGVO-Novelle 2012 nicht der Vorabkontrolle unterliegen automatisch registriert werden. Dies soll auch für bereits eingebrachte Meldungen von Datenanwendungen zutreffen die nach den derzeitigen Bestimmungen vorabkontrollpflichtig sind.

In diesem Zusammenhang muss abermals deutlich auf die Ausführungen zu den Punkten 2.9, 2.10, 2.13, 2.21 und 2.22 betreffend die Bedeutung und Notwendigkeit der Vorabkontrolle hingewiesen werden. Unabhängig davon, dass dringend davon abgeraten wird die genannten Änderungen an den Bestimmungen betreffend die Vorabkontrolle vorzunehmen, birgt die automatische Registrierung von Datenanwendungen ein nicht abzuschätzendes Risiko für die Betroffenen.

Von der geplanten, automatischen Registrierung bereits gemeldeter, aber noch nicht von der Datenschutzkommission, in Hinblick auf die Verletzung von Betroffenenrechten vorabgeprüfter Datenanwendungen, ist dringend abzuraten.

3. FAZIT

Das Ziel der DSG-Novelle 2012, die Datenschutzkommission durch einen Abbau von Bürokratie zu entlasten, erfüllt der vorliegende Entwurf nur zum Teil.

So ist die Etablierung von Datenschutzbeauftragten beispielsweise zu begrüßen. Schließlich sind fachkundige, unabhängige Datenschutzbeauftragte bestens dazu geeignet gewisse Aufsichts- und Kontrollfunktionen der Datenschutzkommission in Hinblick auf ihren Auftraggeber zu übernehmen.

Von der de facto Abschaffung der Vorabkontrolle muss aber unbedingt abgesehen werden. Bürokratie- und Verwaltungsabbau darf nicht ohne Rücksicht auf Verluste auf Kosten der Betroffenenrechte vorgenommen werden. Die Abschaffung der Vorabkontrolle würde Betroffene schutzlos der Willkür von Auftraggebern aussetzen und dem Verstoß gegen grundlegende Datenschutzrechte Tür und Tor öffnen.

Zu bedauern ist, dass der vorliegende Entwurf keine Bestimmungen bezüglich einer, die Datenschutzkommission ablösenden, Kontrollstelle enthält obwohl dies in Anbetracht derer Auflösung dringend an Zeit wäre.

Ebenfalls bedauerlich ist, dass es der Entwurf verabsäumt auf aktuelle Entwicklungen im Datenschutzbereich einzugehen. So finden sich im Entwurf keine Bestimmungen in Bezug auf Online-Dienste oder die Möglichkeit von Verbandsklagen. Auch etablierte Mängel am bestehenden Datenschutzgesetz, wie „indirekt personenbezogene Daten“ oder Datenschutz für juristische Personen bleiben unberührt. Die Chance, dass Österreich der geplanten Datenschutz-Grundverordnung zuvorkommt und eine europäische Vorreiterrolle in Bezug auf die Wahrung von Grundrechten einnimmt bleibt somit vertan.

Nichtsdestotrotz erwartet sich ARGE DATEN, dass der vorliegende Entwurf unter Beachtung der vorgebrachten Verbesserungen rasch überarbeitet und anschließend konsequent umgesetzt wird. Keinesfalls darf die Umsetzung der geplanten Maßnahmen erneut zwei Jahre in Anspruch nehmen, wie dies bei der DSG-Novelle 2008 der Fall war.

An Herrn
Sektionschef Mag. Dr. Gerhard Hesse
Bundeskanzleramt
Sektion V - Verfassungsdienst

Ballhausplatz 2
1014 Wien

Wien, 28. August 2012

Betreff: Zeichen: BKA-810.026/0001-V/3/2012
Stellungnahme der ARGE DATEN zum
Entwurf eines Bundesgesetzes, mit dem das Datenschutzgesetz 2000 geändert
werden soll.

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme

Alle Stellungnahmen werden unter <ftp://ftp.freenet.at/privacy/gesetze> veröffentlicht.