

An alle Bundesministerien

An die  
Verbindungsstelle der  
Bundesländer

An den  
Österreichischen Gemeindebund

An den  
Österreichischen Städtebund

An die  
Gewerkschaft Öffentlicher Dienst

Betrifft: **Fragebogen des Datenschutzrates**  
hinsichtlich „Whistleblowing“

Der **Datenschutzrat** hat in 208. Sitzung am 29. Juni 2011 **einstimmig** beschlossen, zu „Whistleblowing“ eine Reihe von Fragen an öffentliche und private Institutionen, so auch an Sie zu richten, um deren Beantwortung wir Sie ersuchen:

Anlass für dieses Schreiben und des Fragebogens sind europaweite Diskussionen zur Zulässigkeit von Whistleblowing und die Frage, ob für den privaten und öffentlichen Bereich ein Handlungsbedarf des Gesetzgebers besteht.

### **I. Allgemeines:**

Der Begriff „Whistleblowing“ leitet sich vom „Whistleblower“ ab, der als eine Art „Hinweisgeber“ Missstände, illegales Handeln (z.B. Korruption) oder allgemeine

Gefahren, von denen er beispielsweise an seinem Arbeitsplatz erfährt, an die Öffentlichkeit bringt.

Das Übereinkommens der Vereinten Nationen gegen Korruption, BGBl. III Nr. 47/2006, enthält in Artikel 33 eine Bestimmung über den Schutz von Personen die Angaben machen. Wobei jeder Vertragsstaat zu erwägen hat, in seiner innerstaatlichen Rechtsordnung geeignete Maßnahmen vorzusehen, um Personen, die den zuständigen Behörden in redlicher Absicht und mit hinreichender Begründung Sachverhalte betreffend in Übereinstimmung mit diesem Übereinkommen umschriebenen Straftaten mitteilen, vor ungerechtfertigter Behandlung zu schützen.

Sowohl in Großbritannien (Public Interest Disclosure Act – PIDA), als auch in den USA (Whistleblower Protection Act, Sarbanes-Oxley Act – SOX) werden Whistleblower zum Teil bereits gesetzlich geschützt. So sieht SOX etwa in Section 301 verpflichtend die Einrichtung von Verfahren für die vertrauliche, anonyme Beschwerde durch Mitarbeiter in Bezug auf fragwürdige Rechnungslegungs- oder Prüfungsangelegenheiten vor. Der Vorteil des Whistleblowerschutzes steht bei SOX einem Arbeitnehmer dann zu, wenn er das vorgegebene Verfahren – so vor allem die Einschaltung der jeweils zuständigen Stellen – einhält.

Auch in Deutschland wurde in dem im Jahr 2009 in Kraft getretenen Beamtenstatusgesetz eine Durchbrechung des Verschwiegenheitsgrundsatzes für Beamte im Zusammenhang mit der Meldung von Korruptionsstraftaten eingeführt.

Ein Entwurf zum § 612a dt. Bürgerliches Gesetzbuch (BGB) sah zudem in Deutschland ein Anzeigerecht für Arbeitnehmer für den Fall vor, dass der Arbeitnehmer auf Grund konkreter Anhaltspunkte der Auffassung war, dass im Betrieb oder bei einer betrieblichen Tätigkeit gesetzliche Pflichten verletzt werden. Nach dem Entwurf konnte er sich an den Arbeitgeber oder eine zur innerbetrieblichen Klärung zuständige Stelle wenden und Abhilfe verlangen. Kommt der Arbeitgeber dem Verlangen nach Abhilfe nicht oder nicht ausreichend nach, hat der Arbeitnehmer das Recht, sich an eine zuständige außerbetriebliche Stelle zu wenden. Ein vorheriges Verlangen nach Abhilfe ist nicht erforderlich, wenn dies dem Arbeitnehmer

nicht zumutbar ist. Unzumutbar ist ein solches Verlangen stets, wenn der Arbeitnehmer aufgrund konkreter Anhaltspunkte der Auffassung ist, dass aus dem Betrieb eine unmittelbare Gefahr für Leben oder Gesundheit von Menschen oder für die Umwelt droht, der Arbeitgeber oder ein anderer Arbeitnehmer eine Straftat begangen hat, eine Straftat geplant ist, durch deren Nichtanzeige er sich selbst der Strafverfolgung aussetzen würde, oder eine innerbetriebliche Abhilfe nicht oder nicht ausreichend erfolgen wird.

Der Entwurf des § 612a BGB stieß auf breite Kritik: Auf der einen Seite wurde dadurch eine massive Gefährdung des Betriebsfriedens befürchtet, auf der anderen Seite stellte die Beweislast, die danach immer noch beim Whistleblower liegen würde, und die Anonymitätssicherung ein Problem dar.

Der **Datenschutzrat** hat in seiner 191. Sitzung am 16. November 2009 erstmals eine Grundsatzdebatte zum Thema „Whistleblowing“ geführt. Im Zuge dieser Grundsatzdebatte wurde auch die Regierungsvorlage zum Umweltinformationsgesetz vom Datenschutzrat behandelt. Im Fokus der Diskussion stand hierbei insbesondere § 9b des Umweltinformationsgesetzes („Informantenschutz“), der in Abs. 2 vorsah, dass eine Behörde bei der Ausübung ihrer Zuständigkeiten niemanden bestrafen, verfolgen oder belästigen darf, weil er ihr konkrete Anhaltspunkte für einen Verstoß gegen die Verordnung über begleitende Regelungen im Zusammenhang mit der Schaffung eines Europäischen Schadstofffreisetzungs- und -verbringungsregisters (E-PRTR Begleitverordnung, EPRTR-BV) anzeigt.

In der Folge wurde mit einem Abänderungsantrag (AA-92 24. GP) § 9b der RV dahingehend abgeändert, dass eine Behörde bei der Ausübung ihrer Zuständigkeiten niemanden wegen einer Anzeige, mit welcher ihr konkrete Anhaltspunkte für einen Verstoß gegen die E-PRTR-Begleitverordnung oder die EG-PRTR-V mitgeteilt werden, bestrafen, verfolgen oder belästigen darf.

### **Stellungnahme der Art. 29 Datenschutzgruppe**

Die Art. 29-Datenschutzgruppe hat sich in ihrer **Stellungnahme 1/2006 (WP 117)** mit der Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung

mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität sowie insbesondere mit den Grundlagen und Fragen der Zulässigkeit von Whistleblowing beschäftigt.

Die Art. 29-Datenschutzgruppe stellte fest, dass vorhandene Regelungen und Leitlinien über Verfahren zur Meldung von Missständen darauf ausgelegt sind, der Person („dem Hinweisgeber“), die diese Verfahren nutzt, besonderen Schutz zu gewähren, sie aber an keiner Stelle den Schutz der beschuldigten Person besonders erwähnen, insbesondere hinsichtlich der Verarbeitung seiner/ihrer personenbezogenen Daten. Eine Person hat jedoch Anspruch auf die Rechte, die ihr nach der Datenschutz-Richtlinie 95/46/EG und den entsprechenden einzelstaatlichen Rechtsvorschriften zustehen, auch wenn sie eines Verstoßes beschuldigt wird.

Im Ergebnis kam die Art. 29-Datenschutzgruppe zu dem Schluss, dass Verfahren zur Meldung von Missständen ein sinnvoller Mechanismus sein können, um ein Unternehmen oder eine Organisation bei der Überwachung der Einhaltung von Regeln und Vorschriften im Zusammenhang mit der Unternehmensführung zu unterstützen, sie wies jedoch darauf hin, dass die Einrichtung von Verfahren zur Meldung von Missständen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und Bekämpfung von Korruption und Banken- und Finanzkriminalität im Einklang mit den Grundsätzen des Datenschutzes gemäß der Datenschutz-Richtlinie 95/46/EG erfolgen muss. **Es sei wesentlich, dass bei der Umsetzung eines Verfahrens zur Meldung von Missständen das grundlegende Recht auf den Schutz personenbezogener Daten, sowohl des Hinweisgebers als auch der beschuldigten Person, während des gesamten Meldeverfahrens gewährleistet wird.**

Die Art. 29-Datenschutzgruppe wies auch darauf hin, dass die Datenschutzgrundsätze nach der Datenschutz-Richtlinie 95/46/EG vollständig auf die Verfahren zur Meldung von Missständen angewandt werden müssen, insbesondere hinsichtlich der Rechte der beschuldigten Person auf Mitteilung, Zugang, Berichtigung und Löschung von Daten. In Anbetracht der unterschiedlichen Interessen erkannte die Gruppe jedoch an, dass die Ausübung dieser Rechte in ganz bestimmten Fällen beschränkt werden kann, um ein Gleichgewicht zwischen dem Recht auf Schutz der

Privatsphäre und den Interessen des Systems herzustellen. Derartige Beschränkungen sollten jedoch restriktiv gehandhabt und nur in dem Maß angewandt werden, das erforderlich ist, um die Ziele des Systems zu erreichen.

### **Parlamentarische Entwicklungen**

Am 21.10.2009 wurden drei Entschließungsanträge (824/A(E), 825/A(E) und 827/A(E)) mit der Forderung nach einem verstärkten (gesetzlich verankerten) Schutz von „Whistleblowern“ von der grünen Parlamentsfraktion im Parlament eingebracht. Insbesondere wurden eine Neuregelung des Arbeitsverfassungsgesetzes, des Beamtendienstrechts-Gesetzes 1979 sowie die Vorlage eines Gesetzesvorschlages für die Einrichtung einer „Ombudsstelle“ für die Entgegennahme von Informationen über straf- und verwaltungsstrafrechtliche Missstände von öffentlichem Interesse gefordert. Diese Anträge wurden im Nationalrat noch nicht geschäftsordnungsmäßig erledigt.

### **Initiativen der Länder**

Zu dem „Entwurf eines GRECO-Umsetzungsberichtes“ haben die Länder – über Ersuchen des BMJ – eine gemeinsame Länderstellungnahme (dem BMJ) vorgelegt; in dieser gemeinsamen Länderstellungnahme heißt es ua.:

„Der wirksamste ‚Whistleblower Schutz‘ besteht einerseits in der Möglichkeit, auch anonyme Anzeigen und Meldungen erstatten zu können. Wie von den Ländern in der ersten gemeinsamen Länderstellungnahme ausgeführt, wird diesen anonymen Meldungen auch nachgegangen. Andererseits ist nach Ansicht der Länder nochmals darauf hinzuweisen, dass das österreichische Rechtssystem namentlich bekannte Anzeigenleger bereits jetzt vor ungerechtfertigter Diskriminierung schützt. Dies gilt selbstverständlich auch für Beamte und Vertragsbedienstete, die ihrer gegenüber ihren Vorgesetzten bestehenden Meldepflicht von strafbaren Handlungen nachkommen.

**Die Länder vertreten zu dieser Empfehlung weiters die Ansicht, dass – vorbehaltlich der Regelungsautonomie der Länder für ihren Bereich – zunächst die Maßnahmen des Bundes zum Whistleblower Schutz abgewartet werden.“**

### **Aktuelle Entscheidungen der Datenschutzkommission**

Die Datenschutzkommission (DSK) hatte sich ua. in ihrer Entscheidung **K178.274/0010-DSK/2008** vom 05.12.2008 mit Aspekten des Whistleblowings auseinanderzusetzen. Dabei hat sie die Genehmigung erteilt, dass aus der beim DVR gemeldeten Datenanwendung (Bezeichnung: „Internes Verfahren zur Erfassung von Meldungen über mutmaßliche Missstände im Unternehmen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität“) Daten an die G\*\*\*\* Inc., USA, übermittelt werden. Hierbei werden einerseits Daten von Mitarbeitern (Entscheidungsträger) übermittelt, über die im Wege der im Auftrag der G\*\*\*\* Inc. (USA) betriebenen Hotline ein schwerer Verstoß gegen Regeln des „Code of Business Conduct des G\*\*\*\*-Konzerns“ betreffend die Bereiche Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität gemeldet wird. Andererseits werden Daten von Mitarbeitern übermittelt, die im Wege der genannten Hotline Meldung über Missstände erstatten haben und hierbei ihre Identität angegeben haben.

**Die Genehmigung wurde unter der Auflage erteilt, dass im internen Verfahren für die Behandlung von Missbrauchsmeldungen folgende Maßnahmen garantiert sind:**

1. G\*\*\*\* **lässt anonyme Meldungen zwar zu**, fördert sie aber nicht, sondern sichert vielmehr den **Meldern volle Vertraulichkeit** hinsichtlich ihrer Identität zu, wenn sie diese angeben.
2. Die mit der **Bearbeitung von Meldungen** betrauten Stellen sind von den anderen **Konzernstellen strikt getrennt** und haben nur Personen als Mitarbeiter, die besonders geschult und ausdrücklich verantwortlich für die Vertraulichkeit der gemeldeten Daten sind.
3. Die **Beschuldigten** haben **grundsätzlich Zugang zu Anschuldigungen**.
4. Die **Identität des Meldenden** wird nur dann **offengelegt**, wenn sich nachträglich herausstellt, dass die **Anschuldigung bewusst falsch erhoben wurde**.
5. Die eingemeldeten Daten werden spätestens **2 Monate nach Beendigung der Untersuchung gelöscht**.

Die Genehmigung wurde von der DSK weiters unter der aufschiebenden Bedingung erteilt, dass die Antragstellerin vor Aufnahme der Übermittlungen an die G\*\*\*\* Inc. (USA) die Genehmigung der Datenschutzkommission zur Überlassung der Daten eingeholt hat, die an die Betreiberin der Hotline, S\*\*\*\* Inc. (USA) im Wege der Hotline von Mitarbeitern der Antragstellerin gemeldet werden.

Auch in den Entscheidungen **K178.301/0003-DSK/2009** vom 25.2.2009 und **K178.305/0004-DSK/2009** vom 24.7.2009 hat die DSK unter ähnlichen Voraussetzungen die Genehmigung für die Datenübermittlung im Rahmen eines internen Verfahrens zur Meldung von mutmaßlichen Missständen erteilt.

Mit Bescheid vom 20.1.2010, **K600.074/0002-DVR/2010**, hat die DSK zudem die Registrierung für eine „Ethik-Hotline“ unter Erteilung von Auflagen und unter der aufschiebenden Bedingung verfügt, dass die Antragstellerin vor Aufnahme der Übermittlungen in die USA die Behandlung der an die Hotline gemeldeten Daten entsprechend vertraglich geregelt hat.

## **II. Fragestellungen zum Whistleblowing:**

Die Regelungen in den USA, Großbritannien und Deutschland sowie die in der Literatur geäußerten Rechtsansichten verfolgen im Umgang mit Whistleblowing zum Teil unterschiedliche Ansätze.

Festgehalten wird, dass sich aufgrund der unterschiedlichen Problemstellungen für den öffentlichen und den privaten Bereich unterschiedliche Ansätze ergeben, wobei es im öffentlichen Bereich schon eine gesetzliche Regelung zu Whistleblowing im Rahmen der Korruptionsbekämpfung gibt (Bundesgesetz über die Einrichtung und Organisation des Bundesamts zur Korruptionsprävention und Korruptionsbekämpfung BGBl I Nr 72/2009).

Zu dieser Frage wurde auch ein ausführliches Gespräch mit dem Leiter der Korruptionsstaatsanwaltschaft Mag. Walter Geyer geführt, der auf die Notwendigkeit einer derartigen gesetzlichen Regelung verwies. Weiters war er der Meinung, dass es jedenfalls außerhalb der Behörde, auf die sich die mitgeteilten Vorwürfe beziehen, eine Anlaufstelle für Whistle-Blower geben sollte. Entscheidend wäre hierbei auch die

Gewährleistung der Anonymität und die Möglichkeit der Kontaktaufnahme mit den Informanten.

Bedenklich sei in diesem Zusammenhang, dass in den letzten Monaten Mitarbeiter in Betrieben von der Firmenleitung (z.B. Hypo-Alpe-Adria) aufgefordert wurden, Missstände aufzuzeigen, ohne dass entsprechende Betriebsvereinbarungen oder Regelungen vorlagen.

In Österreich wurde ein Verein „Whistleblowing Austria“ gegründet. Zweck des Vereins ist, die Schaffung einer gesetzlichen Grundlage für Whistleblowing in Österreich in Anlehnung an den Entwurf einer Whistleblower Gesetzgebung von Transparency International zu unterstützen. Darüberhinaus möchte er die Umsetzung von in internationalen Verträgen normierten Whistleblowing Regelungen (z.B. Artikel 33 des Übereinkommens der Vereinten Nationen gegen Korruption, BGBl. III Nr. 47/2006) in Österreich fördern sowie die Ratifizierung solcher Verträge unterstützen. Ein weiterer Auftrag sei, gesellschaftliche Anerkennung für Whistleblowing und Zivilcourage gegen alle Arten von Missständen und Fehlverhalten zu fördern sowie das Bewusstsein für die Richtigkeit und Nützlichkeit von Whistleblowing in einer modernen, transparenten und demokratischen Gesellschaft zu schärfen. Die Beratung von Whistleblowern soll in rechtlicher und psychologischer Sicht sowie in deren Umgang mit den Medien erleichtert werden. Das Instrument des Whistleblowings soll in Staat, Wirtschaft, Wissenschaft und Gesellschaft, u.a. im Wege von Forschung und Lehre bekanntgemacht werden. Auch der Kontakt zu Gesellschaften und Organisationen mit ähnlichen Zielsetzungen wie Whistleblowing Austria sowie zu Gesellschaften zur Förderung von Maßnahmen gegen die Korruption (z.B. Transparency International oder UNCAC Coalition) im In- und Ausland soll zwecks Informationsaustausch und Zusammenarbeit gepflegt werden.

Nicht übersehen werden darf, dass auch schon von den Medien Whistle-Blower-Plattformen eingerichtet wurden, auf denen vertrauliche Dokumente und Hinweise veröffentlicht werden können (z.B. Kurier-Plattform Austrolix). Meistens sind diese Webportale mit einem elektronischen Postfach ausgestattet, welches den Hinweis gibt, dass unter Wahrung der vollkommenen Anonymität Dokumente hochgeladen werden können.



In der Zwischenzeit wurde eine Kronzeugenregelung in der StPO beschlossen (§ 209a StPO BGBl I Nr 108/2010). Eine gesetzliche Whistleblowing-Regelung sollte als Ergänzung dieser Kronzeugenregelung verstanden werden.

§ 209a StPO enthält konkret eine Kronzeugenregelung zum Rücktritt von der Verfolgung wegen einer Zusammenarbeit mit der Staatsanwaltschaft. Demnach kann die Staatsanwaltschaft unter bestimmten Voraussetzungen von der Verfolgung einer Straftat zurücktreten, wenn ihr der Beschuldigte freiwillig sein Wissen über Tatsachen offenbart, die noch nicht Gegenstand eines gegen ihn geführten Ermittlungsverfahrens sind und deren Kenntnis wesentlich dazu beiträgt,

1. die Aufklärung einer der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengerichts oder der Korruptionsstaatsanwaltschaft oder eines Wirtschaftskompetenzzentrums unterliegenden Straftat entscheidend zu fördern,
2. eine Person auszuforschen, die in einer kriminellen Vereinigung, kriminellen Organisation oder terroristischen Organisation führend tätig war, oder
3. dem Verfall oder dem erweiterten Verfall unterliegende Vermögenswerte in einem 500 000 Euro übersteigenden Wert sicherzustellen.

Im Zusammenhang mit Whistleblowing treten daher für den **Datenschutzrat** insbesondere folgende Fragestellungen auf, um deren Beantwortung wir Sie ersuchen:

**1) Welche gesellschaftspolitischen Vor- und Nachteile sehen Sie in einer Regelung von Whistleblowing? Wie beurteilen Sie Whistleblowing-Plattformen von Medienunternehmen?**

Es wurden von Medienunternehmen Whistleblower-Plattformen eingerichtet, auf denen vertrauliche Dokumente und Hinweise veröffentlicht werden (z.B. Kurier-Plattform Austrolix). Dies sind meistens Webportale mit einem elektronischen Postfach, welches erlaubt, unter Wahrung der vollkommenen Anonymität Dokumente hochzuladen.

**2) Gibt es im Rahmen ihres Wirkungsbereiches bereits Regelungen bzw. vergleichbare Mitteilungsverpflichtungen, die „Whistleblower“ (d.s. Hinweisgeber) beim Aufdecken von Missständen hinreichend schützen oder sind Sie der Meinung, dass es zusätzlicher Regelungen – auf betrieblicher oder auf gesetzlicher Ebene – bedarf (Leitlinien über Verfahren zur Meldung von Missständen)?**

**3) Wenn ja, soll dabei nur „internes Whistleblowing“ oder auch „externes Whistleblowing“ geregelt werden?**

Demzufolge wird bei internen und externen Whistleblowing unterschieden, ob Hinweise nur intern innerhalb des Betriebes, der Dienststelle oder Organisation oder aber auch extern gegenüber den zuständigen Behörden, Dritten, oder auch gegenüber der Presse gegeben werden.

**4) Gibt es in ihrem Wirkungsbereich Kronzeugenregelungen bzw. sind Sie der Meinung, dass es solcher Regelungen im öffentlichen Bereich bedarf?**

**5) Welche Erfahrungswerte liegen Ihnen konkret hinsichtlich „Whistleblowing“ im öffentlichen Bereich bereits vor?**

**6) Sind Ihnen spezielle Erlässe hinsichtlich „Whistleblowing“ bekannt?**

Wenn ja, was wird inhaltlich in diesen Erlässen geregelt und wurden dabei die Bestimmungen der EG-Datenschutzrichtlinie 95/46/EG jeweils berücksichtigt?

**7) Welche Personen sollen als „Whistleblower“ geschützt werden?**

Die grundsätzliche Fragestellung lautet, welche Personen sollen als Whistleblower geschützt werden, bzw. welche Personen sollen berechtigt sein, Missstände zu melden.

Sollen auch anonyme Anzeigen zugelassen werden?

**8) Für welche Bereiche soll ein „Whistleblowerschutz“ eingerichtet werden?**

In den genannten Entscheidungen der DSK wurde Whistleblowing auf die Bereiche Rechnungslegung, interne Rechnungslegungskontrolle, Fragen der Wirtschaftsprüfung, sowie die Bekämpfung von Korruption, Banken- und

Finanzkriminalität eingeschränkt. Auch der Sarbanes-Oxley Act (SOX) konzentriert sich auf Meldungen in Rechnungslegungs- oder Prüfungsangelegenheiten.

Das dt. Beamtenstatusgesetz erfasst hingegen nur Meldungen zu Korruptionsstraftatbeständen. Die Regelung des Informantenschutzes in § 9b des österreichischen Umweltinformationsgesetzes bietet einen Whistleblowerschutz nur bei der Meldung von Verstößen gegen die E-PRTR-Begleitverordnung oder die EG-PRTR-V.

Im Bereich der Korruptionsbekämpfung gibt es in Österreich bereits einen Whistleblowerschutz.

**Es stellt sich daher die Frage, welche Bereiche von einem Whistleblowerschutz umfasst sein sollen?**

Sollten auch ganz allgemein Informationen über vermutete Rechtsverletzungen oder Gefährdungen öffentlicher Interessen dem Whistleblowerschutz unterliegen?

**9) An welche Anlaufstellen soll bzw. muss sich der „Whistleblower“ mit seiner Beschwerde wenden?**

Soll es interne und/oder externe Meldestellen geben?

Soll es eine eigene Whistleblower Meldestelle für den öffentlichen und den privaten Bereich geben und wenn ja, wo sollen diese angesiedelt sein?

Wenn ja, für welche Bereiche soll Whistleblowing im öffentlichen und privaten Bereich zulässig sein?

**10) Soll der „Whistleblower“ vor strafrechtlichen Sanktionen und/oder vor zivilrechtlichen bzw. dienstrechtlichen Rechtsfolgen geschützt werden?**

In diesem Zusammenhang stellt sich auch die Frage, ab welchem Zeitpunkt vom Dienstgeber disziplinarrechtliche bzw. strafrechtliche Maßnahmen gegenüber dem Angezeigten gesetzt werden müssen bzw. dürfen.

Fraglich ist aber auch, ob der Whistleblower rechtlichen Schutz genießen soll, wenn sich nachträglich – allenfalls auch nach Ermittlungen durch eine Behörde – herausstellt, dass die angezeigten Missstände in Wirklichkeit gar nicht vorliegen.

**11) Welche Rechte hat die Person, die von einem „Whistleblower“ angezeigt wurde?**

In diesem Zusammenhang stellt sich die Frage, wie eine Abwägung hinsichtlich der berechtigten Grundrechtsschutzinteressen des Angezeigten und des Hinweisgebers erfolgt. Anhand welcher Kriterien sollen die Schutzinteressen des Angezeigten und des Hinweisgebers bewertet werden?

Welche Maßnahmen sind notwendig um die Schutzinteressen des Hinweisgebers und des Angezeigten umzusetzen?

Welche Handlungen sind notwendig, um angezeigte Personen vor materiellen und immateriellen Schäden zu schützen?

Im Rahmen eines vom Whistleblower angezeigten Missstandes stellt sich auch die Frage, ab welchem Zeitpunkt der Angezeigte Zugang zu den angezeigten Daten erhalten soll.

Soweit sich die Anschuldigungen jedoch als haltlos erweisen, stellt sich auch diesfalls die Frage, ob bzw. unter welchen Voraussetzungen dem Angezeigten die Daten des Whistleblowers für eine allfällige straf- oder zivilrechtliche Verfolgung ausgehändigt werden müssen.

## **12) Besondere Sicherheitsmaßnahmen?**

Welche besonderen Sicherheitsmaßnahmen sind über jene in §14 Abs. 2 DSG 2000 genannten Datensicherheitsmaßnahmen hinaus notwendig, um einen besonderen Schutz für den Zeitraum der genauen Prüfung der getätigten Anschuldigungen zu gewährleisten? Wie eng sollte der Kreis der informierten Personen sein?

## **13) Zu welchem Zeitpunkt und in welcher Form soll die Löschung der angezeigten Daten erfolgen?**

In diesem Zusammenhang stellt sich auch die Frage, wie die Datenqualität gemäß § 27 DSG 2000 sichergestellt werden kann, bzw. wie lange die Daten in diesem Zusammenhang aufgehoben werden sollen.

Der **Datenschutzrat** beabsichtigt, die eingegangenen Stellungnahmen zusammenzufassen und im Herbst dieses Jahres eine Generaldebatte unter Mitwirkung aller zuständigen Stellen (Gebietskörperschaften) und

Interessensvertretungen durchzuführen. Sollten Sie weitere Probleme sehen, ersuchen wir Sie, dies in ihrer Stellungnahme zu berücksichtigen.

In diesem Sinne dürfen wir Sie ersuchen, die gegenständlichen Fragen bis zum 30. September 2011 zu beantworten.

Für allfällige Rückfragen steht Ihnen aus der Geschäftsstelle des Datenschutzrates Frau MR Mag. Birgit Hrovat-Wesener ([birgit.hrovat-wesener@bka.gv.at](mailto:birgit.hrovat-wesener@bka.gv.at) oder Tel. 01 – 53 115/2526) gerne zur Verfügung.

8. Juni 2011  
Für den Datenschutzrat:  
Der Vorsitzende:  
MAIER

**Elektronisch gefertigt**