Hinweisgebersysteme

verfasst von HR Mag. Georg Lechner (Datenschutzbehörde)

Hinweis

Die vorliegende Information stellt eine unverbindliche Darstellung von Hinweisgebersystemen dar. Berechtigungen oder Verpflichtungen können daraus nicht abgeleitet werden.

Grundlagen

Ein Hinweisgebersystem ist eine spezielle Möglichkeit zur Kommunikation innerhalb eines Konzerns, mit deren Hilfe einfache Mitarbeiter (teilweise auch Kunden oder Lieferanten) unter Umgehung der normalen Hierarchie einen Missstand an die Konzernspitze melden können. Dabei werden Telefonhotlines oder Webformulare eingesetzt. Damit soll es möglich sein, Missstände vorbei an untätigen oder möglicherweise korrupten Konzernorganen direkt an die oberste Führungsebene zu melden.

Die Idee von Hinweisgebersystemen oder „Whistleblowing Hotlines“ stammt aus den **USA**. Der Sarbanes-Oxley-Act (Pub. L. No. 107-204, 116 Stat. 745[1]) verpflichtet die Konzerne, besondere Verfahren zur Meldung von wirtschaftlichen Missständen an die Konzernleitung einzurichten. In **Deutschland** gibt es dazu den deutschen Corporate Governance Kodex [2], dessen Beachtung durch § 161 deutsches Aktiengesetz vorgeschrieben ist[3].

Die Artikel 29-Datenschutzgruppe, eine Arbeitsgruppe der europäischen Datenschutzbehörden, hat dazu ein Dokument verfasst („Stellungnahme 1/2006 zur 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“, kurz WP117[4]).

---

[1] Siehe http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf
[2] Siehe http://www.dcgk.de/de/kodex/aktuelle-fassung/praeambel.html
[3] Siehe http://dejure.org/gesetze/AktG/161.html
[4] siehe http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf (deutsch) und http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf (englisch).

Gestaltung in der Praxis

Der Konzern erlässt als rechtliche Grundlage einen „Code of Conduct“ oder „Code of Ethics“, in dem die Mitarbeiter aufgefordert werden, Missstände zu melden. Der Katalog der Missstände kann weit über wirtschaftliche Delikte hinausgehen, was Probleme bei den Rechtsgrundlagen verursachen kann, die auf wirtschaftliche Verstöße zugeschnitten sind. Je konkreter die Liste der möglichen Verstöße ist, desto besser. Unspezifische Missstände („Alles, was dem Ruf des Konzerns schaden könnte“) oder Missstände ohne Bezug zur Tätigkeit („moralische Verstöße“) sind unzulässig. Die Liste der Missstände umfasst typischerweise Korruption und Bestechung, Verstöße gegen Buchführungsvorschriften und Steuerhinterziehung, illegale Praktiken im Zusammenhang mit Banken wie Geldwäsche und Bankenbetrug sowie Fälschung von Finanzunterlagen und Insiderhandel.

In dem Ethikkodex wird auch eine Aufforderung zur Anzeige enthalten sein. Es ist schon vorgekommen, dass in Unterlagen das System als „freiwillig“ bezeichnet wird, aber grundsätzlich werden die Mitarbeiter verpflichtet sein, Missstände anzuzeigen. Eine Anzeige ist daher keine Privatsache, sondern Teil der beruflichen Pflichten und wird daher rechtlich dem Arbeitgeber zugerechnet.

Die Ermittlung und Übermittlung der Daten wird auf das überwiegende berechtigte Interesse (§ 8 Abs. 1 Z 4 DSG 2000) gestützt.

Die Datenschutzbehörde begrenzt das Recht der Konzernmutter auf maßgeblichen Verstößen von leitenden Angestellten.

Der Arbeitgeber hat ein überwiegendes berechtigtes Interesse an der Kenntnis von solchen Verstößen. Ein überwiegendes berechtigtes Interesse der Konzernspitze an der Kenntnis von *allen* Verstößen gegen die konzerninternen Verhaltensregeln wird nicht anzunehmen sein, da dies unverhältnismäßig wäre. Eine sachliche Rechtfertigung für die Übermittlung von Missbrauchsdaten zum Zweck der Aufklärung und Untersuchung von Vorfällen wird nur dann angenommen, wenn dieser Zweck bei der Antragstellerin selbst nicht zweifelsfrei erreicht werden kann: Im Umfang der Meldung von **maßgeblichen Verstößen**, die **Mitarbeitern der**

Antragstellerin in Führungspositionen oder vergleichbar hochgestellten Positionen angelastet werden, anerkennt die Datenschutzbehörde das Bestehen eines überwiegenden berechtigten Interesses an der Übermittlung der Meldungsdaten an die Konzernspitze, da nur auf diese Weise mit hinlänglicher Sicherheit eine objektive und vollständige Aufklärung der erhobenen Vorwürfe zu erwarten ist.

Die Meldung von **Vorfällen, die keine leitenden Angestellten betreffen** ist nicht zulässig, weil in solchen Fällen die Antragstellerin selbst ohne Hilfe der Konzernmutter das Problem bereinigen kann. In dem Fall, dass ein Mitarbeiter von geringerem Einfluss auf die Unternehmensführung einen schwerwiegenden Verstoß verursacht, wäre eine Meldung an die Konzernspitze dann zulässig, wenn die Vorgesetzten ihre Aufsichtspflicht nicht korrekt wahrnehmen und dadurch ihrerseits maßgeblich gegen die Konzernrichtlinien verstoßen (z.B. im Fall der Barings Bank, die 1995 durch unautorisierte Spekulationen eines Terminhändlers in dne Ruin getrieben wurde[5]).

Die Datenschutzbehörde verlangt eine Betriebsvereinbarung oder eine Zustimmung gemäß § 10 AVRAG. Eine AVRAG-Zustimmung ist nicht dasselbe wie eine Zustimmung nach dem DSG 2000.

Verfahren nach dem Datenschutzgesetz 2000

Die üblichen Teilnehmer eines Whistleblower-Systems sind:

- Eine Tochter eines ausländischen Konzerns in Österreich (**datenschutz-rechtlicher Auftraggeber**). Rein innerösterreichische Hinweisgebersysteme sind selten;
- Eine Konzernmutter im Ausland, an welche die Meldungen gehen sollen (**Empfänger der Übermittlung**);
- **Optional:** Ein spezielles Unternehmen, das die Meldungen entgegennimmt (**Dienstleister**). Die meisten US-Konzerne haben dazu einen Vertrag mit

[5] https://de.wikipedia.org/wiki/Barings_Bank

einem spezialisierten amerikanischen Unternehmen. Der Dienstleister gibt die Meldung dann zur Bearbeitung weiter.

Meldung der Datenanwendung

Ein Hinweisgebersystem muss beim Datenverarbeitungsregister gemeldet werden, wie alle Datenanwendungen (§ 17ff DSG 2000).

Die Meldung unterliegt der Vorabkontrolle gemäß § 18 Abs. 2 Z 2 DSG 2000 (strafrechtlich relevante Daten!). Die Tochter in Österreich gilt als Auftraggeber, weil sie die Daten verwendet, die über das System hereinkommen, auch wenn die Meldung an den Dienstleister geht.

Ein (mögliches) Muster einer Meldung ist angeschlossen.

Der Meldung sollten folgende Unterlagen angeschlossen werden;

- Der Ethikkodex des Konzerns und
- Die Betriebsvereinbarung oder die Zustimmung gemäß § 10 AVRAG.

Bei Whistleblower-Fällen, für die keine Genehmigung gemäß § 13 DSG 2000 erforderlich ist (siehe unten), weil keine genehmigungspflichtige Übermittlung gewünscht ist, gibt es nur ein Verfahren beim Datenverarbeitungsregister. In diesem Verfahren können mit Bescheid Auflagen verfügt werden[6]. Es gibt dazu die Möglichkeit zur raschen Erledigung ohne Bescheid gemäß § 19 Abs. 2 DSG 2000, wenn der Auftraggeber bestimmte Auflagen von sich aus zusagt und alle Unterlagen stimmig sind. Ein Satz möglicher Auflagen ist angeschlossen.

Genehmigung für Datenexport

Wenn Daten an die Konzernmutter im Ausland übermittelt werden sollen, muss möglicherweise ein Antrag gemäß § 13 DSG 2000 auf Genehmigung für

[6] Siehe Bescheid K600.320-005/0003-DVR/2012 vom 14. Dezember 2012 http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20121214_K600320_005_0003_DVR_2012_00

Internationalen Datenverkehr gestellt werden. Dies ist der Fall, wenn sich der Empfänger (die Konzernmutter!) in einem Land befindet, das keinen angemessenen Datenschutz hat. Die Übermittlung wird bei der Datenschutzbehörde beantragt. Am Ende steht ein Bescheid[7].

Nicht alle Datenübermittlungen zum Zweck der Korruptionsbekämpfung sind Whistleblower-Hotlines[8].

Rechtsschutz

Falls es Probleme gibt, können Betroffene sich an die Datenschutzbehörde wenden. Diese kann ein Kontroll- und Ombusmannverfahren gemäß § 30 DSG 2000 durchführen. Es besteht auch die Möglichkeit, eine gemeldete Datenanwendung zu prüfen (§ 22a DSG 2000). Bitte beachten Sie, dass Streitfälle auch vor den Gerichten ausgetragen werden können (z.B. Anfechtung einer Kündigung, oder eine Geldforderung wie Abfindung, Schadenersatz etc.).

[7] Siehe Bescheid K178.507/0005-DSK/2012 vom 17. Oktober 2012
http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20121017_K178507_0005_DSK_2012_00

[8] Siehe Bescheid K178.428/0009-DSK/2011 vom 30. September 2011
http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20110930_K178428_0009_DSK_2011_00

Anhang: Mustermeldung

Betroffene Personengruppen:	Datenarten:	Empfängerkreise:
Mitarbeiter der Auftraggeberin, der über die Hotline / das Webformular Missstände meldet:	Personalnummer	01
	Vor- und Familienname	01
	Titel / akademischer Grad	01
	Stellung und Funktion im Unternehmen	01
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	01
	Inhalt der Meldung	01
	Verfahrensablauf, sofern der Melder betroffen ist	01
	Ergriffene Maßnahmen, sofern der Melder betroffen ist	01
Leitende Angestellten der Auftraggeberin, denen ein schwerer Verstoß angelastet wird:	Personalnummer	01
	Vor- und Familienname	01
	Titel / akademischer Grad	01
	Stellung und Funktion im Unternehmen	01
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	01
	Inhalt der Meldung	01
	Verfahrensablauf	01
	Ergriffene Maßnahmen	01
Zeugen oder sonstige Auskunftspersonen:	Vor- und Familienname	01
	Titel / akademischer Grad	01
	Stellung und Funktion im Verfahren (Zeuge, Auskunftsperson, usw.)	01
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	01
	Verfahrensablauf, sofern die Person betroffen ist	01
	Ergriffene Maßnahmen, sofern der Zeuge betroffen ist	01

Übermittlungsempfänger

LfdNr	Bezeichnung	Rechtsgrundlage
01	Konzernmutter (mit Angabe des Landes)…	§ 8 Abs. 1 Z 4 DSG 2000 (überwiegende berechtigte Interessen des Auftraggebers und des Empfängers)

Anhang: Auflagen

Dieser Text gibt die Auflagen für Hinweisgebersysteme wieder. Die Formulierung entspricht einer Zusage von Auflagen gemäß § 19 Abs. 2 DSG 2000:

1. Die Übermittlung von personenbezogenen Daten von Beschuldigten an die Konzernleitung ist nur hinsichtlich leitender Angestellter zulässig, die eines maßgeblichen Verstoßes (oder der Teilnahme daran) gegen die konzernintern verbindlichen Regelungen betreffend [Liste der Verstöße, die angezeigt werden sollen] bezichtigt werden.

2. Die mit der Bearbeitung von Meldungen betraute Stelle ist von den anderen Konzernstellen strikt getrennt und hat nur Personen als Mitarbeiter, die besonders geschult und ausdrücklich verantwortlich für die Vertraulichkeit der gemeldeten Daten sind.

3. Der Auftraggeber lässt anonyme Meldungen zwar zu, fördert sie aber nicht, sondern sichert vielmehr den Meldern volle Vertraulichkeit hinsichtlich ihrer Identität zu, wenn sie diese angeben.

4. Die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen.

5. Die Identität des Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde.

6. Die eingemeldeten Daten werden spätestens 2 Monate nach Beendigung der Untersuchung gelöscht, sofern sie nicht weiter für die Durchführung eines Gerichts- oder Verwaltungsverfahrens oder für weitere disziplinäre oder andere amtliche Verfahren benötigt werden; in diesen Fällen werden die eingemeldeten Daten solange und in dem Umfang gespeichert, soweit dies für die Führung und den Abschluss derartiger Verfahren erforderlich ist.

7. Die Registrierung ist an die Auflage geknüpft, dass die Mitarbeiter arbeitsvertraglich zur Einhaltung der konzernintern verbindlichen Regelungen und zur Meldung an den Arbeitgeber über wahrgenommene Verstöße gegen diese Regelungen verpflichtet wurden.

8. Bei Einsatz eines Dienstleisters zur Führung der Hotline wird weiters folgendes zugesagt:

Der Auftraggeber wird vor Aufnahme der Übermittlungen an die verantwortliche Stelle im Konzern die Behandlung der an die Hotline gemeldeten Daten vertraglich regeln. In dieser Vereinbarung ist festzulegen, dass der Dienstleister als Betreiber der Hotline nur Meldungen mit den in Punkt 1 bezeichneten Inhalten weiterbearbeitet und an die verantwortliche Stelle im Konzern weitergibt, während die restlichen über die Hotline allenfalls eingebrachten Meldungen nur dem Auftraggeber zugänglich gemacht werden. Weiters ist zu vereinbaren, dass der Inhalt von Meldungen nach ihrer Übermittlung an die verantwortliche Stelle im Konzern bzw. nach ihrer Rück-Überlassung an den Auftraggeber beim Dienstleister umgehend gelöscht wird.