Transparency International Deutschland e.V.
Innenministerium des Landes Baden-Württemberg

2. Erfahrungsaustausch der Vertrauensanwälte, Ombudsleute und Antikorruptionsbeauftragten des Bundes und der Länder

26. Februar 2013 in der Landesvertretung von Baden-Württemberg in Berlin

Die Anforderungen des Datenschutzes bei der Einführung von Hinweisgebersystemen in Unternehmen

Rechtsanwalt und Fachanwalt für Strafrecht Dr. Rainer Frank, Berlin

1.
Hinweisgebersysteme sind datenschutzrelevant, weil regelmäßig (wenn auch nicht immer und ausschließlich) personenbezogene Daten erhoben, gespeichert, übermittelt, verarbeitet und genutzt werden. Deshalb gelten die Regelungen des BDSG.

§ 43 BDSG enthält diverse Bußgeldtatbestände, § 44 BDSG sogar einen Straftatbestand.

2.
Um den Bestimmungen des BDSG Rechnung zu tragen, ist ein Rahmen von Regelungen zu schaffen, der den Bogen von der Datenerhebung im Hinweisgebersystem bis zur Löschung personenbezogener Daten nach Vorgangsbearbeitung im Hinweisgebersystem und beim Auftraggeber spannt. Das kann eine *Geschäftsordnung Hinweisgebersystem* oder eine *Verfahrensanweisung Datenschutz im Hinweisgebersystem* sein.

3.
In Anlehnung an die Empfehlungen der Art. 29 Arbeitsgruppe der EU-Kommission 2006 und das Gesetzesziel der §§ 28 und 32 BDSG (2009) ist eine sachliche Eingrenzung des Hinweisgebersystems auf Kernthemen erforderlich. *„Hinweise auf Straftaten, insbesondere aus den Bereichen Korruption und Wirtschaftsstrafrecht, des Wirtschaftsordnungswidrigkeitenrechts einschließlich Versuchs- und Vorbereitungshandlungen sowie Hinweise auf sonstige strafbare Rechtsverstöße und schwerwiegende Ordnungswidrigkeiten“*.

Im industriellen Bereich erfolgt üblicherweise eine ausdrückliche Nennung von *„Straftaten und Ordnungswidrigkeiten in den Bereichen Arbeitsschutz und Umweltschutz“*.

Für zulässig halte ich auch: *„Hinweise auf Verstöße gegen das Allgemeine Gleichstellungsgesetz, wenn der berichtete Sachverhalt so schwer wiegt, dass er Anlass zur fristlosen Kündigung eines Arbeitsverhältnisses aus wichtigem Grund geben könnte“.*

Die Entgegennahme von Hinweisen auf Verstöße gegen arbeitsrechtliche Pflichten, die nicht zugleich in den ausdrücklich bezeichneten Regelungsbereich fallen, ist ausdrücklich vom Hinweisgebersystem auszuschließen.

4.
Das Hinweisgebersystem muss eine Eingangsprüfung gewährleisten. Es dürfen nur solche Hinweise erfasst und übermittelt werden, welche den definierten Themenkreis betreffen.

5.
In Anlehnung an die Empfehlungen der Art. 29 Arbeitsgruppe der EU-Kommission 2006 ist sicherzustellen, dass ein Hinweisgeber auf die vorhandenen Wege der direkten und offenen Kommunikation hingewiesen wird, bevor im Rahmen der Vertraulichkeit des Hinweisgebersystems ein Hinweis entgegengenommen wird.

6.
Aus § 32 Abs. 1 Satz 2 BDSG (und im Übrigen aus Verhältnismäßigkeitserwägungen) leite ich ab, dass ein Hinweisgebersystem eine Eingangsprüfung mit Blick auf einen qualifizierten Anfangsverdacht vorsehen muss. Bloße Beschuldigungen ins Blaue hinein dürfen nicht übermittelt werden. Hinweise auf verjährte Sachverhalte dürfen nicht übermittelt werden. Übermittelt werden dürfen nur Hinweise, die einen auf Tatsachen gegründeten Anfangsverdacht eines verfolgbaren Rechtsverstoßes begründen. Hilfreicher Maßstab ist § 152 Abs. 2 StPO.

7.
Ein Hinweisgebersystem muss Vertraulichkeit hinsichtlich der Identität des Hinweisgebers gewährleisten. Vertraulichkeit heißt nicht Anonymität.

Vertraulichkeit in diesem Sinne kann keine unternehmensinterne Person zusagen. Dienstliche Handlungspflicht und strafprozessuale Zeugenpflicht stehen entgegen. Ausschließlich externe Rechtsanwälte – Ombudsanwälte – können Vertraulichkeit gewährleisten (Zeugnisverweigerungsrecht und –pflicht sowie Beschlagnahmefreiheit.

8.
Eine Geschäftsordnung oder ein Datenschutzkonzept Hinweisgebersystem muss den Vorgang der Datenübermittlung an den Auftraggeber definieren (ausschließlicher Empfänger, Art der Datenübermittlung).

9.
Das Verfahren nach Eingang eines Hinweises beim Auftraggeber ist zu regeln. Meine und die Erfahrung anderer Ombudsanwälte ist: Die Probleme beginnen bei Eingang eines Hinweises. Ursache sind regelmäßig fehlende Regelungen über die Hinweisbearbeitung.

Der Datenschutz gebietet Prüfungen mit Blick auf die Zweckbindung und die Verhältnismäßigkeit bei jeder Speicherung, Übermittlung, Verarbeitung oder Nutzung von Daten aus dem Hinweisgebersystem. An den entscheidenden Punkten sollen Abwägungsprozess und Abwägungsergebnis in angemessener Form dokumentiert werden. Beispiel: Übermittlung von Daten an die interne Revision zur Prüfung.

10.
Im Datenschutzrecht gibt es de lege lata kein Konzernprivileg. Die Datenübermittlung zwischen Konzerngesellschaften bedarf einer ausdrücklichen rechtlichen Grundlage. Eine solche kann sich ergeben aus Betriebsvereinbarungen zum Hinweisgebersystem. Sie kann sich als Auftragsdatenverarbeitung im Sinne des § 11 BDSG darstellen. Dann bleibt die betroffene Konzerngesellschaft aber in der datenschutzrechtlichen (Mit-)Verantwortung, § 3 Abs. 7, § 11 BDSG.

11.
§ 33 BDSG regelt Benachrichtigungspflichten gegenüber Betroffenen. § 34 BDSG begründet Auskunftsansprüche. §§ 33, 34 BDSG gelten auch für Daten aus Hinweisgebersystemen. Eine Geschäftsordnung oder ein Datenschutzkonzept muss Regelungen über die Benachrichtigung des Betroffenen von über ihn erhobenen und gespeicherten Personendaten enthalten.

Die Benachrichtigung des Betroffenen soll durch den Auftraggeber und nicht durch das Hinweisgebersystem/den Ombudsanwalt erfolgen. Das setzt voraus, dass bestimmt ist, dass vom Hinweisgebersystem erfasste Informationen vollständig (mit Ausnahme gegebenenfalls der Identität des Hinweisgebers) an den Auftraggeber übermittelt werden. Das wiederum verlangt, dass eine Teilfreigabe zur Weiterleitung durch den Hinweisgeber nicht zugelassen werden darf.

Die Identität des Hinweisgebers wird durch § 33 Abs. 2 Nr. 3, 34 Abs. 7 BDSG gewährleistet: *„Eine Pflicht zur Benachrichtigung besteht nicht, wenn die Daten (…) ihrem Wesen nach namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen“.* Das kann nicht gelten, wenn der dringende Verdacht einer vorsätzlichen Falschbeschuldigung (Denunziation) besteht.

12.
Es ist sicherzustellen, dass im Rahmen des Hinweisgebersystems personenbezogene Daten gelöscht werden, wenn der mit der Erhebung und Übermittlung verfolgte Zweck erfüllt ist. Der Rechtsgedanke der §§ 28, 32 BDSG (2009) ist zu berücksichtigen. Grundsätzlich müssen die Daten nach Ende einer Vorgangsbearbeitung gelöscht werden.

Nach § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Eine Aufbewahrung zu Präventionsgründen ist nur in sehr engem zeitlichen Rahmen zulässig (wenige Monate).

Die Aufbewahrungspflicht des Rechtsanwalts stellt eine vorrangige Regelung im Sinne des § 35 Abs. 3 Nr. 1 BDSG dar.

13.
Weitere Speicherung beim externen anwaltlichen Ombudsmann: Der Berliner Datenschutzbeauftragte wünscht, dass die im Rahmen der anwaltlichen Aufbewahrungspflicht von Handakten erfolgende weitere Speicherung personenbezogener Daten folgenden Grundsätzen folgt:

- Übertragung analoge Daten in digitale Daten und Vernichtung der analogen Daten.
- Speicherung digitaler Daten in einem gesonderten Datenraum mit Zugriff ausschließlich für den beauftragten Rechtsanwalt.
- Kennzeichnung der Datensperrung für andere Zwecke.
- Klare Regelungen, dass nach (kurzen) Fristen dem Auftraggeber keine Auskünfte aus Hinweisgebervorgängen mehr erteilt werden dürfen.

14.
Weitere Speicherung beim Auftraggeber: Die Geschäftsordnung oder das Datenschutzkonzept muss exakte Regelungen für Löschung, Speicherung, Sperrung der beim Auftraggeber gespeicherten Daten enthalten.

Referent:
Rechtsanwalt und Fachanwalt für Strafrecht Dr. Rainer Frank
Fachanwälte für Strafrecht am Potsdamer Platz
Dr. Frank Dr. Auffermann Halbritter Dr. Horrer
Potsdamer Platz 8, 10117 Berlin
www.fs-pp.de