Round Table: Anforderungen des neuen Gesetzes

Hinweisgeberschutz

Vor einem Jahr haben wir in ähnlicher Runde bereits über den deutschen Hinweisgeberschutz gesprochen. Nun ist er Gesetz geworden und wir haben noch einmal vier Experten an einen Tisch gebracht, um zu berichten, wie das Gesetz aufgenommen wurde und wie wir nun im Arbeitsalltag damit verfahren. Dieser Beitrag ist ein Auszug des Gesprächs mit Dr. Jan Tibor Lelley, Fachanwalt für Arbeitsrecht und Partner bei Buse in Frankfurt, Dr. Frank Schemmel, Senior Director International Privacy & Compliance DataCo GmbH (DataGuard) in München, Dr. Ariane Loof, Rechtsanwältin für Datenschutzrecht, Arbeitsrecht und IT-Recht und Partnerin bei ADVANT Beiten in Berlin, und Kai Leisering, Managing Director Corporate Compliance bei der EQS Group in Berlin. Ein Zusammenschnitt der Aufzeichnung ist unter www.arbeit-und-arbeitsrecht.de/events/das-neue-hinweisgeberschutzgesetz.html abrufbar.

Welche Definition des Begriffs Whistleblowing bzw. Hinweisgeber legen Sie zugrunde?

Leisering: Ein Hinweisgeber ist eine Person, die über einen reputationsgefährdenden Sachverhalt der Meinung ist, dass dieser berichtenswert ist und sich andernfalls damit plagen würde.

Lelley: Ich würde aus der juristischen Sicht ein bisschen zurückrudern. Bei der Reputation ist aus der juristischen Brille die Schwierigkeit, was justiziabel ist. Ich würde immer gerne auf die gesetzliche Definition verweisen. In § 1 Abs. 1 HinSchG ist die hinweisgebende Person definiert. Da geht es um Verstöße, die aufgedeckt oder gemeldet werden. Verstöße sind rechtlich relevante Vorgänge, rechtswidrige Vorgänge. Reputationsverlust kann schmerzhaft sein, auch für Unternehmen, ist möglicherweise aber nicht unbedingt auch etwas Rechtswidriges.

Schemmel: In § 1 Abs. 1 steht auch „im Zusammenhang ihrer beruflichen Tätigkeit", also wir Compliance-Experten würden den Begriff weiter verstehen. Es kann natürlich sein, dass jemand, z. B. weil er in den Medien unterwegs ist, von Umständen Kenntnis erlangt. Diese Personen fallen nicht unter den Anwendungsbereich unseres HinSchG, sind aber trotzdem Whistleblower.

Loof: Die Art von Verstößen, die gemeldet werden können, ist zunächst erstmal in der EU-Richtlinie geregelt, dann aber auch in den nationalen Gesetzen. Diese sind in den EU-Mitgliedstaaten auch unterschiedlich. Darüber hinaus legen die Unternehmen im Code of Conduct und Code of Business Ethics selbst fest, welche Verstöße sie darüber hinaus melden lassen und bearbeiten werden, die über die Hinweisgebersysteme eingehen.

Der rechtliche Ausgangspunkt war bereits die Richtlinie vom 23.10.2019, die Umsetzung in den Mitgliedstaaten war bis zum 17.12.2021 vorgesehen. Was regelt die Richtlinie und warum hat die Umsetzung in Deutschland so lange auf sich warten lassen?

Loof: Die Richtlinie gibt im Wesentlichen vor, wann welche Unternehmen Meldekanäle und Meldestellen einrichten müssen, interne Meldeverfahren für private Unternehmen, externe Meldestellen, die der Staat einrichten muss. Sie regelt auch den Hinweisgeber- und Identitätsschutz für die meldenden Personen sowie die Umsetzung in nationales Recht. In Deutschland hat es nach meiner Kenntnis länger gedauert, weil zuletzt um die Einbeziehung der Beamten in das HinSchG gestritten wurde.

Lelley: Ich habe diesen Gegensatz immer als eigenartig empfunden, da die Arbeitgeberseite sich lange gesträubt hat gegen eine Gesetzgebung zum Hinweisgeberschutz. Dessen Notwendigkeit wurde lange Zeit auch von den zuständigen Verbänden in Abrede gestellt. Genauso lange gibt es aber einschlägige Stellungnahmen von internationalen Organisationen, wie z. B. der Internationalen Handelskammer, die immer schon die Notwendigkeit von Whistleblowing im Interesse der Unternehmen betont haben. Von Arbeitgeberseite wurde immer auf die Arbeitsgerichte, die Rechtsprechung und das Schikaneverbot aus § 612a BGB verwiesen. Mein Eindruck war, dass sich diese „Grabenkämpfe" fortgesetzt haben ins parlamentarische Verfahren und ein Hinderungsgrund waren.

Schemmel: Neben dieser Beamtenfrage hat es sich auch an den verpflichtenden anonymen Meldungen aufgehangen. Wir Compliance-Experten würden das so niedrigschwellig wie möglich ausgestalten, damit man Hinweise intern bekommt und nicht extern gemeldet wird. Die Befürchtung der Politik war, dass das zum Denunziantentum führt und Falschmeldungen eingehen. Nun ist es ein politischer Kompromiss geworden, mit dem wir als Praktiker leben müssen. Allerdings ist es nichts Halbes und nichts Ganzes. Wir finden dazu jetzt im Gesetz eine Sollte-Vorschrift. Muss man jetzt oder soll man nur?

Leisering: Ich kann das nur bestätigen. Es ist tatsächlich genau das Drama zwischen Theorie und Praxis, was zu diesen Grabenkämpfen geführt hat. In der Theorie ist das Thema sehr weit erschlossen. Es gibt einschlägige Studien, Umfragen, Untersuchungen der großen Wirtschaftsprüfungsgesellschaften, die alle bestätigen, dass das totalen Sinn macht. Denn die Unternehmen erlangen dadurch Wissen, was sie einerseits reputativ schützt und andererseits auch vor größeren Schäden bewahren kann. Insofern haben viele der großen Konzerne sehr früh begonnen, solche Stellen einzurichten und jetzt jahrelange Erfahrungen mit der Sinnhaftigkeit solcher Whistleblowing-Systeme. Was wir jetzt in Deutschland haben, ist eher ein Kompromiss, der gerade noch politisch durchsetzbar war, obwohl er der Praxis nicht einhundertprozentig entspricht. Dass wir Sonderregelungen für die Beamten treffen, ist eigentlich unsäglich, denn diese stehen auch auf Arbeitnehmerseite und kritische Themenstellungen treten nun einmal im Arbeitnehmerkontext auf.

Wie sahen die Regelungen in Europa vor der EU-Richtlinie aus? Und wie ist das Ganze in Großbritannien und den USA geregelt?

Loof: Die EU ist hier Vorreiter. Ich erwarte, dass, wie es damals mit der DSGVO auch geschah, in anderen Staaten alles entsprechend nachgezogen wird und ähnliche Regelungen erlassen werden. Aber bisher sind im EMEA-Raum die EU-Mitgliedstaaten – aktuell noch bis auf Polen – und Serbien die einzigen, die dieses Recht haben.

Lelley: In Nordamerika gibt es eine Whistleblowing-Gesetzgebung, die Jahrzehnte alt ist. Das ist ein völlig etablierter Teil der Wirtschaftspolitik, der sich auf börsennotierte Unternehmen, aber auch auf alle möglichen anderen Branchen und Wirtschaftsbereiche bezieht. Diese Erfahrung zeigt, dass die Umsetzung keine Schwierigkeit darstellen muss. Das sind erfolgreiche Länder, die sowas schon viele Jahre machen. Zu uns ist das Ganze herübergeschwappt. Wir kennen diese Gesetzgebung aus den USA, die mittelbar auf deutsche Unternehmen übertragen wurde, indem durch eine Beziehung zu einer amerikanischen Konzernmutter das entsprechende System auch im deutschen Unternehmen eingeführt werden musste. Dabei ist es seit vielen Jahren internationaler Standard, dass es ein System gibt, welches anonyme Meldungen ermöglicht und dass die meldende Person Schutz genießt.

Schemmel: Im angloamerikanischen Raum herrscht ein anderes Mindset vor. Deren Systeme richten sich mit einer Incentivierung an die Hinweisgeber. Es gibt Prämien für Personen, die Missstände melden. Der Whistleblower, der meldet und einen Missstand aufzeigt, wird dort als positiver Beitrag gesehen, während man hier oft über den Nestbeschmutzer diskutiert.

Wie war der Umgang mit dem Thema in Deutschland, bevor es diese Vorstöße aus der Gesetzgebung gab?

Leisering: Die Unternehmen stehen in einem Dilemma. Sie haben einerseits das nationale Recht in all den Ländern, in denen sie tätig sind, aber auf der anderen Seite natürlich auch eine Unternehmenskultur, typischerweise einen Code of Conduct, welche für das gesamte Unternehmen gelten. Jetzt kann man natürlich nicht sagen, ein Mitarbeiter von Siemens in Deutschland unterliegt dann einem anderen Compliance-Regelwerk als ein Mitarbeiter von Siemens in Südamerika oder Asien. Insofern ist für die Unternehmen typischerweise erst einmal das strengste anwendbare Recht dasjenige, wonach sie ihren Compliance Scope definieren müssen. Und da bestanden die angloamerikanischen Regelungen sehr früh. Es hat sich der Best-Practice-Ansatz herausgebildet, dass selbstverständlich Anonymität gewährt werden muss, dass eine Multilingualität abgedeckt werden muss, sodass hinweisgebende Personen eine möglichst niedrige Hemmschwelle haben, um zu melden.

Wie ist der Anwendungsbereich des jetzigen Gesetzes geregelt?

Lelley: Hinsichtlich des persönlichen Anwendungsbereichs sprechen wir über Hinweise, die abgegeben werden von Personen, über Verstöße, also rechtswidrige Vorgänge, die immer in einem arbeitsrechtlichen Kontext bestehen.
Beim sachlichen Anwendungsbereich ist der deutsche Gesetzgeber – aus meiner Sicht zu Recht – über die Vorgaben der EU-Richtlinie hinausgegangen.
Es gilt aber auch: Jede Meldung, die nicht in den Anwendungsbereich fällt (Stichwort Reputationsschaden), unterliegt nicht mehr dem Schutz des HinSchG.

Schemmel: Das ist ganz wichtig, weil man in der Praxis oft auf die Annahme trifft, dass Sachverhalte, die nicht unter den Anwendungsbereich des HinSchG fallen, nicht gemeldet werden dürfen oder nicht verfolgt werden müssen. Die Intention des Gesetzes ist, wie der Name schon sagt, der Hinweisgeberschutz. Wenn ein gemeldeter Sachverhalt unter den sachlichen Anwendungsbereich fällt, ist der Hinweisgeber geschützt. Das heißt aber für Unternehmen nicht, dass sie Meldungen, die nicht unter diesen Anwendungsbereich fallen, nicht trotzdem prüfen und ggf. verfolgen sollten.

Können sich Arbeitgeber auch gegen den Hinweisgeberschutz entscheiden?

Loof: Sie können sich nicht dagegen entscheiden. Es gibt eine Pflicht. Ab 50 Beschäftigten sind Unternehmen verpflichtet, interne Meldekanäle einzurichten. Der zweite Schwellenwert, 250 Mitarbeiter, ist relevant für die Art der Ausgestaltung, also ob gemeinsam mit anderen Unternehmen oder eigene Meldestellen eingerichtet werden. Die Hinweisgeber sind, auch wenn man freiwillig ein Hinweisgebersystem zur Verfügung stellt, geschützt, auch vor Vergeltungsmaßnahmen. Alle Unternehmen, die ich in der Beratung habe, haben die Verstöße, die gemeldet werden können, auch geregelt, meistens im Code of Conduct, welcher auch vorsieht, dass jede Diskriminierung untereinander im Arbeitsverhältnis durch Vorgesetzte oder Kollegen sowie jeder Angriff auf die Persönlichkeitsrechte gemeldet werden kann. Dort finden sich also sehr viel detailliertere Beschreibungen als in der Aufzählung im HinSchG.

Lelley: Manche Unternehmen denken, das Gesetz macht es uns leicht, weil es immer von Beschäftigungsgebern, nicht Arbeitgebern spricht. Es ist natürlich klar, dass das daher kommt, weil es eben auch für den öffentlichen Dienst gelten soll. In der Privatwirtschaft könnte man sich hier die Frage stellen: Ist es das Unternehmen oder nur der Betrieb? Wenn man davon ausgeht, dass es der Betrieb ist, werden die Schwellenwerte vielleicht doch nicht erreicht.
Ich halte das für falsch. Der Anknüpfungspunkt für den Schwellwert ist das Unternehmen.

Leisering: Ich glaube, was wir mitunter verkennen, ist, ein solches Gesetz – und das auch noch einmal auf europäischer Ebene – tut auch etwas mit der Gesellschaft. Mitarbeitende gehen natürlich davon aus, dass Unternehmen sich ganzheitlich rechtskonform verhalten, das heißt solche Meldestellen, eben weil es ein Gesetz gibt, anbieten. Dementsprechend gehen Mitarbeitende künftig mehr und mehr davon aus, diese Meldestellen nutzen zu können, wenn es sie gibt. Ich glaube, das wird gesamtgesellschaftlich psychologisch dazu führen, dass es viel selbstverständlicher wird, eine solche Meldung abzugeben.

Schauen wir uns einmal die Problematik der internen und externen Meldungen genauer an. Wie sind die Regelungen im Gesetz dazu ausgefallen?

Schemmel: Bis 17.12.2023 gibt es noch diese Übergangsfrist. Unternehmen mit 250 Beschäftigten müssen einen internen Meldekanal einrichten, Behörden auch. Für Kommunen gibt es einen Schwellenwert von 10.000 Einwohnern. Ab 17.12. fällt dann dieser 250-Mitarbeiter-Schwellenwert und dann sind es nur noch 50. Externe Meldekanäle mussten schon parallel eingerichtet werden. Bei der BaFin waren, wenn es sich um Korruptionstatbestände gehandelt hat, beim Bundeskartellamt, wenn es sich um kartellrechtliche Sachverhalte gehandelt hat, früher schon Meldungen möglich. Es gibt jetzt noch eine weitere externe Meldestelle für alles, was nicht kartellrechtlichen oder Bezug zur Finanzindustrie hat, beim Bundesamt für Justiz.
Durch die Einrichtung der externen Meldestellen kann ein Hinweisgeber entscheiden, ob er intern bei seinem Arbeitgeber meldet oder bei dieser externen Meldestelle. Unabhängig davon genießt er den Schutz des Gesetzes, insbesondere vor Repressalien und Schikanen. Er darf jedoch nicht an die Medien gehen. Es war im politischen Diskurs auch ganz wichtig, dass man den Unternehmen die Möglichkeit gibt, den Verstoß erst mal selber zu ermitteln und zu beheben. Nur wenn das Unternehmen den Verstoß nicht selbst oder nicht in ausreichendem Maße ermittelt, kann ein Hinweisgeber auch eine öffentliche Meldung abgeben.
Das Gesetz sagt aber, die Unternehmen sollen Anreize schaffen, um interne Meldungen zu generieren, weil sie von den Verstößen betroffen sind und sie aufklären sollen und viel näher am Sachverhalt sind als ein Bundesamt für Justiz.

Leisering: Ein ganz wesentlicher Punkt ist, dass wir eine viel größere Durchsetzung sehen werden.
Am Ende des Tages ist die hinweisgebende Person gefragt, was sie denn melden will. Ist das ein zivilrechtlicher Verstoß? Ist das ein strafrechtliches Thema? Insofern ist unsere Empfehlung immer breiter an das Thema heranzugehen, sodass die Mitarbeitenden nicht durch unzählige Kanäle surfen müssen und fragen müssen, wo ihre Meldung hingehört.

Lassen Sie uns noch einmal über die nationalen Grenzen blicken. Welche Regelungen haben andere Länder getroffen?

Loof: Die EMEA-Staaten, Türkei, Ukraine und Nordafrika haben keine Gesetze. Gleichwohl haben die internationalen Konzerne alle schon lange Hinweisgebersysteme, die sie allen Mitarbeitern im Konzern weltweit zur Verfügung stellen und die sich am strengsten Recht orientieren. Die Regelungen darüber, was gemeldet werden kann, finden sich für die Mitarbeiter im Code of Conduct, für die Business-partner im Code of Business Ethics. Diese werden jetzt angepasst. Die häufigste Frage ist die, ob weiter das globale oder regionale System verwendet werden kann. Die Antwort darauf fällt auch in den Mitglied-staaten ganz unterschiedlich aus, obwohl die Richtlinie dazu relativ eindeutig ist.

Bei jeder Meldung werden personenbezogene Daten verarbeitet. Welche Anforderungen ergeben sich hierbei durch das Gesetz für Arbeitgeber?

Schemmel: Es sollte immer eine sog. Datenschutz-Folgenabschätzung durchgeführt werden. Das ist eine Risikoevaluierung. Am Anfang gilt es, das eingesetzte System, die Prozesse und Datenflüsse zu beschreiben. Die Krux ist, dass Unternehmen sich irgendein System einkaufen, von dem sie nicht wissen, wie die Prozesse und Datenflüsse aussehen. Das erfordert aber diese Datenschutz-Folgenabschätzung, dort werden sodann mögliche Datenschutzrisiken identifiziert, bewertet und risikominimierende Maßnahmen abgeleitet. Schließlich nimmt der Datenschutzbeauftragte Stellung. Dieser darf die Datenschutz-Folgenabschätzung nicht selbst durchführen.
Zu den umzusetzenden Maßnahmen gehört vor allem ein Rollen- und Berechtigungskonzept. Dieses regelt den Zugriff auf Meldungen. Das Gesetz selber beinhaltet ein Vertraulichkeitsgebot bzw. einen Identitätsschutz. Danach dürfen nur mit der Meldung betraute Personen die Informationen aus der Meldung bearbeiten, wenn eine Meldung nicht anonym erfolgt bzw. sich aus anderen Umständen heraus ergibt, wer der Hinweisgeber ist.
Weitere wichtige Themen sind Anonymisierung, Verschlüsselung, Archivierungs- und Löschfristen. Das Gesetz macht in § 11 Abs. 5 Vorgaben zur Dokumentation. Diese soll nämlich drei Jahre lang vorgehalten werden, wobei unklar ist, was das auslösende Moment ist.
Hinzu kommen die üblichen Fragen im Datenschutz: Wer sind die datenschutzrechtlich Verantwortlichen? Gibt es Auftragsverarbeiter, also Dienstleister, die Daten auf Weisung des Verantwortlichen verarbeiten? Was ist die Rechtsgrundlage für die Verarbeitung? Wir können uns glücklich schätzen, weil das deutsche Gesetz in § 10 einen spezial-gesetzlichen Erlaubnistatbestand enthält für die Verarbeitung personenbezogener Daten im Zusammenhang mit eingehenden Meldungen.

Loof: Ich möchte die Pflicht zur Information und Auskunftserteilung ergänzen. Wenn ein Hinweis eingeht, kommt bei den Unternehmen oft als Erstes die Frage auf: Muss ich die Betroffenen jetzt informieren? Das möchten sie gerade nicht, weil sie die Ermittlungen erst beginnen und nicht darüber unterrichten möchten, solange die Gefahr des Wegschaffens der Beweismittel und der Einflussnahme besteht. Da sieht das Bundesdatenschutzgesetz Ausnahmen vor für den Fall, dass etwas geheim gehalten werden muss. In diesem Fall darf die Information so lange ausgesetzt werden und das Auskunftsersuchen muss so lange nicht erfüllt werden, außer man erhebt die Daten bei den Betroffenen selbst. Das ist in den anderen Mitgliedstaaten leider nicht so.

Lelley: Meine persönliche Voraussage aus arbeits-rechtlicher Sicht ist, dass das Spannungsfeld HinSchG und Datenschutz einer der Hauptkampfplätze in der Zukunft sein wird. Aus Arbeitgebersicht ist die angesprochene Löschfrist, vor allem im Zusammen-spiel mit der Beweislastumkehr, teils schwer nachvollziehbar. Sie sollen das, was sie ermittelt haben, nach drei Jahren löschen. Wie verteidigen sie sich dann hinterher, wenn sie beschuldigt werden, eine Repressalie verhängt zu haben?

Loof: Ich sehe diese drei Jahre Aufbewahrungsfrist auch nicht im Einklang mit Art. 17 DSGVO, der ganz andere Grundsätze dafür aufstellt, wie lange Daten aufbewahrt werden dürfen, nämlich solange sie erforderlich sind für den Zweck und danach für die Dauer der gesetzlichen Aufbewahrungsfrist.

Zum Verbot von Repressalien gibt es eine Regelung samt Beweislastumkehr. Was hat es damit auf sich?

Lelley: Das Repressalienverbot ist geregelt im § 36 HinSchG. Das ist ganz traditionell gesehen eines der Kernelemente des Hinweisgeberschutzes. Der Begriff Repressalien ist dabei sehr weit und umfasst nicht nur Kündigungen, sondern alle möglichen „Unannehm-lichkeiten", die eine hinweisgebende Person in einem Arbeitsverhältnis aufgrund solcher Hinweise treffen können. Diese sind eben gesetzlich verboten.
Zudem gibt es eine Beweislastumkehr, die sich wie folgt zusammenfassen lässt: Die Beschäftigungs-geberin muss, wenn es zu Repressalien kommt, beweisen, dass diese nicht aufgrund des erteilten Hinweises erfolgt sind. Das heißt, es besteht eine ganz hohe Hürde, die Unternehmen überwinden müssen und die gleichzeitig auch einen sehr hohen Schutz für Hinweisgeber gesetzlich verankert.

Schauen wir uns einmal einige Best-Practice-Beispiele an. Angenommen, ein Mitarbeiter meldet anonym einen Compliance-Verstoß durch seinen Vorgesetzten an die interne Meldestelle. Was passiert mit dieser Meldung?

Leisering: Das hängt sicherlich stark von dem Unternehmensumfeld ab. Sprechen wir über ein eher kleines Unternehmen, sprechen wir über ein größeres Unternehmen? Ist die interne Meldestelle vielleicht extern besetzt? Auch das sind ja Konstellationen, die wir in der Praxis finden. Insofern kann man nicht per se von demselben Ablauf ausgehen. In den eher größeren Unternehmenskonstellationen gibt es

typischerweise Verfahrensbeschreibungen, nach denen sich die entsprechenden Abteilungen richten müssen. Mitunter wird die Revision miteinbezogen, um erst einmal zu schauen, ob eine Meldung plausibel ist und wie das Unternehmen damit umgeht. Die Grenzen in der Praxis sind immer diejenigen, die die Realität betreffen. Wenn es also eine eher kleine Abteilung ist, ist es schwierig, die hinweisgebende Person zu schützen bzw. ihre Anonymität zu wahren.
Zudem kann auch Anlass bestehen, unabhängige Prüfungen durchzuführen und den Sachverhalt noch einmal durch eine andere Brille zu checken. Das kann immer eine Möglichkeit sein, die hinweisgebende Person zu schützen und erst einmal den Fokus von dieser reinen Behauptung wegzuziehen in einen neutralen Sachverhalt.

Schemmel: Das Gesetz gibt die Verfahrensbeschreibung im Groben auch vor. Das Unternehmen muss dem Hinweisgeber innerhalb von sieben Tagen eine Eingangsbestätigung geben. Dann hat es drei Monate Zeit, um die Plausibilität zu prüfen. In der Praxis sind die Hinweise natürlich nicht bereits schön zusammengefasst. Deswegen ist es auch wichtig, wie man so ein Hinweisgebersystem ausgestaltet. Insbesondere bei anonymen Meldungen ist man, wenn man kein System nutzt, wo man mit dem Hinweisgeber kommunizieren kann, abgeschnitten, weil häufig Nachfragen erforderlich sind, um den Sachverhalt genau zu eruieren und dann einen Plausibilitätscheck zu machen.
Hinzu kommen Problematiken wie grenzüberschreitende Sachverhalte, wo ggf. auch andere Unternehmenseinheiten involviert werden müssen. Zudem sind Folgemaßnahmen abzuleiten und nach drei Monaten dem Hinweisgeber kundzutun.
Unternehmen sind gut beraten, das alles in einer Whistleblowing Policy schon vorher festzulegen, damit, wenn ein Hinweis eingeht, alles in geordneten Bahnen abläuft.

Wie ist die Herangehensweise, wenn die zuständige Stelle feststellt, dass es sich um eine Falschmeldung handelt?

Schemmel: Auskunft zu diesem Ergebnis muss ich der hinweisgebenden Person trotzdem geben.
Die erfolgt häufig synchron mit der datenschutzrechtlichen Information. Wichtig ist eine genaue Prüfung, damit größtmögliche Sicherheit besteht, dass es sich um eine Falschmeldung handelt.
Schwierigkeiten haben insbesondere kleinere Unternehmen, die sich fragen, wie sie die Meldestelle einrichten und wer dafür verantwortlich ist. Hier gibt es keine Compliance-Abteilung. Der Erwägungsgrund 56 der Hinweisgeber-Richtlinie und auch die deutsche Gesetzesbegründung sieht für diesen Fall den Rückgriff auf Funktionen vor, die es in dem Unternehmen schon gibt, bspw. den Datenschutzbeauftragten. Unternehmen mit mehr als 20 Mitarbeitern müssen in Deutschland grundsätzlich einen solchen benennen. Davon würde ich abraten.
Man hat dabei das Problem mit Interessenskonflikten. Der Datenschutzbeauftragte muss weisungsfrei sein, die Meldestelle auch. Üblicherweise sehen wir bei kleinen Unternehmen, dass das die HR-Abteilung macht, denn eine Personalabteilung hat üblicherweise jedes Unternehmen. Für Verstöße, die diese Abteilung selber betreffen, ist dann noch einmal eine Person außerhalb davon zuständig.

Leisering: Unser Rat wäre immer ein professionelles System einzusetzen, was sich auch stetig an sich ändernden Rechtsnormen orientiert und dem Unternehmen damit eben auch dauerhaft die Sicherheit gewährleistet, dass man eine solide Lösung hat, die mit den Anforderungen des Unternehmens wächst.

Welche Möglichkeiten haben Arbeitgeber, auf eine absichtlich abgegebene Falschmeldung zu reagieren?

Lelley: Eine absichtlich abgegebene Falschmeldung würde arbeitsrechtlich sehr wahrscheinlich als ein schwerwiegender Verstoß gewertet. Diese Falschmeldung betrifft auch Kollegen, die falsch beschuldigt werden, möglicherweise sogar in einer gewissen Öffentlichkeit. Mögliche Maßnahmen sind dann klassisch die Abmahnung, Kündigung – außerordentlich oder ordentlich. Ich kann mir nur ganz wenige Situationen vorstellen, in welchen man es bei arbeitsrechtlichen Maßnahmen belassen könnte, die unterhalb der Schwelle einer Abmahnung liegen.
Ich kann mir sogar nur ganz schwer vorstellen, dass es bei einer Abmahnung sein Bewenden haben könnte. Immer vorausgesetzt, es ist wirklich ein Hinweis, der sich als Falschmeldung herausstellt, der auch das Vertrauen in das System erschüttert.

Wie sieht gutes Krisenmanagement aus, unabhängig davon, ob es sich um eine Falschmeldung handelt? Wie viel proaktive öffentliche Aufarbeitung ist seitens der Unternehmen sinnvoll?

Lelley: Die beste Aufarbeitung ist immer die, die gar nicht notwendig ist. Das HinSchG legt sehr viel Wert auf Vertraulichkeit. Wenn ein Unternehmen Krisenmanagement betreiben muss, ist schon einiges schiefgelaufen. Das ist aus meiner Perspektive wirklich der GAU, wenn das die Aufmerksamkeit der Öffentlichkeit erregt. Das geht weit über Hinweisgeberschutz hinaus. Da geht es schon um Reputationsschutz.

Leisering: Es gibt ja sozusagen auch ein Krisenmanagement im Kleinen. Die großen Konzerne gehen doch inzwischen in wachsendem Maße dazu über, zu publizieren: Wie viele Hinweise haben wir im Jahr bekommen? In welchen Rechtsgebieten waren die? Was haben wir dagegen unternommen? Das schafft ein Stück weit Vertrauenskultur. Wenn man offen mit dem Sachverhalt umgeht, ihn professionell aufarbeitet und seine Ableitungen daraus zieht und dann aber eben auch kommuniziert, schürt das Vertrauen und ist sozusagen die Vorstufe zur Krisenbewältigung.

Vielen Dank für das Gespräch!

Das Interview führten Andreas Krabel und Anne Politz.