

Whistleblowing und Datenschutz

Wenn Geheimhaltungs- und Offenlegungsinteressen aufeinanderprallen



Dr. Friedrich Popp
Rechtsanwalt
bei Debevoise & Plimpton

In kaum einem anderen Zusammenhang prallen Geheimhaltungs- und Offenlegungsinteressen so heftig aufeinander wie beim Whistleblowing: Der Hinweisgeber auf einen Missstand wie etwa Korruption strebt zur Vermeidung von Repressalien zumeist nach Geheimhaltung seiner Identität. Hingegen sind vielleicht zu Unrecht Verdächtige oder aber in der Meldung angeführte weitere Personen zur Verfolgung von Unterlassungs- und Ersatzansprüchen an genau dieser Identität und am konkreten Inhalt der Meldung interessiert. Offenlegung oder Geheimhaltung – beide berühren das Vertrauen in die Integrität eines Hinweisgebersystems und damit das Unternehmensinteresse an einem effizienten Instrument zur Aufdeckung von Missständen.

Die Frage nach dem rechtsrichtigen Umgang des Unternehmens mit den verschiedenen, auch gegenläufigen Interessen erfährt durch die bevorstehende Verabschiedung eines Hinweisgeberschutzgesetzes zusätzliche Brisanz: Dieses soll die Vertraulichkeit des Hinweisgebers wahren und ihn bei Verwendung gesetzlich definierter Kanäle vor Repressalien schützen. Weil viele Missstände menschengemacht sind, lassen sie sich mit identifizierbaren Personen in Verbindung bringen. Personen-

bezogene Daten kommen aber auch dann ins Spiel, wenn sich der Hinweisgeber identifiziert oder ihn der Hinweis identifizierbar macht. Entgegennahme und Auswertung personenbezogener Daten in Meldungen, insbesondere die Untersuchung des Sachverhalts durch datenschutzrechtlich Verantwortliche, ist Verarbeitung im Sinne der Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG).

Der Hinweis auf mögliches Fehlverhalten bringt für den Verdächtigen das Risiko immaterieller und materieller Schäden wie etwa Rufschädigung, Rechtsverteidigungskosten oder Arbeitsplatzverlust; solchen Risiken können auch in einer Meldung bloß erwähnte Personen ausgesetzt sein. Die Offenlegung der Identität des Hinweisgebers birgt aber auch für diesen das Risiko von Nachteilen, etwa in Form von Kündigung oder Mobbing. Sämtliche dieser Risiken sind datenschutzrechtlich relevant und die Entscheidung des Betreibers eines Hinweisgebersystems für oder gegen eine Offenlegung kann diesen auch Ansprüchen nach DS-GVO oder BDSG aussetzen. Wie also mit einer Offenlegung umgehen?

Der aktuell im Bundestag in Umsetzung der EU-Whistleblower-Richtlinie diskutierte Entwurf eines Hin-

weisgeberschutzgesetzes (HinSchG) soll Menschen schützen, die im Zusammenhang mit ihrer beruflichen Tätigkeit etwa als Arbeitnehmer Informationen über Verstöße erlangt haben und diese nach den gesetzlichen Vorgaben melden oder offenlegen. Meldefähig sind Verstöße gegen in der Richtlinie aufgezählte EU-Rechtsmaterien wie etwa Geldwäsche oder Datenschutz. Darüber hinaus sollen sämtliche strafbewehrte sowie bestimmte bußgeldbewehrte Verstöße gegen nationales Recht in den Schutzbereich einbezogen werden. Der Hinweisgeber kann zwischen einer internen und einer externen Meldestelle frei wählen. Der Weg an die Öffentlichkeit durch Offenlegung ist ihm aber nur in engen Grenzen erlaubt, etwa nach ergebnisloser externer Meldung.

In der Regel werden Beschäftigungsgeber mit mindestens 50 Beschäftigten zu Einrichtung und Betrieb sicherer Meldekanäle verpflichtet. Die zentral beim Bundesamt für Justiz zu errichtende externe Meldestelle wird die Sonderzuständigkeiten der Bundesanstalt für Finanzdienstleistungsaufsicht oder des Bundeskartellamts unberührt lassen. Interne und externe Meldestellen prüfen die eingehenden Meldungen und ergreifen angemessene Folgemaßnahmen. Anonyme Meldungen sollen, was nicht

In Umsetzung der EU-Whistleblower-Richtlinie wird das Hinweisgeberschutzgesetz diskutiert

unumstritten ist, gegenüber nicht-anonymen Meldungen nur nachrangig bearbeitet werden müssen. Ein Kernstück des Gesetzes ist der Vertraulichkeitsschutz: Sämtliche Meldestellen haben die Vertraulichkeit der Identität des Hinweisgebers, des Verdächtigen und der sonstigen in der Meldung genannten Personen zu wahren. Verstöße gegen wesentliche Vorgaben des HinSchG, insbesondere die rechtswidrige Offenlegung der Identität des Hinweisgebers, werden als Ordnungswidrigkeiten mit einer Geldbuße geahndet und verpflichten das Unternehmen zu Schadensersatz. Sofern der Hinweisgeber zum Zeitpunkt der Meldung hinreichenden Grund zur Annahme hatte, dass die von ihm gemeldeten oder offengelegten Informationen der Wahrheit entsprechen, er also redlich ist, wird er vor Repressalien geschützt. Aber auch der Schutz des Hinweisgebers ist nicht uneingeschränkt: Vielmehr ist er im Falle einer vorsätzlichen oder grob fahrlässigen Falschmeldung zum Ersatz des dadurch eingetretenen Schadens verpflichtet; daneben kommt auch eine strafrechtliche Verantwortlichkeit in Betracht.

Unter datenschutzrechtlichen Gesichtspunkten stellt der Entwurf klar, dass Meldestellen zur Verarbeitung personenbezogener Daten zur Erfüllung ihrer Aufgaben befugt sind. Die Dokumentation zu Meldungen soll zwei Jahre nach Abschluss des Verfahrens zu löschen sein. Wie aber ist mit den in der DS-GVO verankerten und auf Offenlegung gerichteten Betroffenenrechten auf Information und Auskunft umzugehen? Soll etwa der Verdächtige über die Bearbeitung des ihn betreffenden Hinweises informiert werden müssen oder im Wege des Auskunftsanspruchs die Identität des Hinweisgebers erfahren können? In dieser Hinsicht erläutert der Entwurf lediglich, dass die Ausübung der Betroffenenrechte das Vertraulichkeitsgebot nicht konterkarieren darf und diesem Anliegen mit dem Instrumentarium des BDSG bereits Rechnung getragen sei. Ist dem wirklich so?

Ein Urteil des Bundesgerichtshofs vom 22. Februar 2022 (VI ZR 14/21) veranschaulicht die bei Erfüllung

Der Hinweisgeber kann zwischen einer internen und einer externen Meldestelle frei wählen

eines Auskunftsanspruchs nach DS-GVO vorzunehmende Interessenabwägung: Der Vermieter von Wohnungen in einem Mehrparteienhaus erhielt von einem Mieter den Hinweis über starke Geruchsbelästigung und Ungeziefer im Treppenhaus, die von einer bestimmten Wohnung eines anderen Mieters ausgehen sollten. Auf den Vorwurf angesprochen, erkundigte sich der andere Mieter nach dem Informanten. Der Vermieter verweigerte diese Auskunft sowohl unter Hinweis auf die Datenschutzinteressen des Hinweisgebers als auch die eigenen Interessen an einer sachgerechten und effektiven Aufgabenerfüllung einer Hausverwaltung, darunter auch die Erhaltung der Ordnung und des Friedens in der Hausgemeinschaft. Der andere Mieter erhob nun gegen den Vermieter Klage auf Auskunft über die Herkunft der Daten, Schmerzensgeld und Rechtsanwaltskosten.

Ausgangspunkt des BGH ist, dass nur die Informationen über die Herkunft der Daten die betroffene Person in die Lage versetzt, mögliche Rechte auch gegen die Person geltend zu machen, von der die (möglicherweise unrichtigen oder zu Unrecht weitergegebenen) Daten herrühren. Ein Auskunftsanspruch kann nur dann nicht bestehen, wenn die Interessen des Hinweisgebers an der Nichtweitergabe seiner Daten oder berücksichtigungsfähige Interessen des Vermieters überwiegen. Das Erfordernis einer Interessenabwägung folgt aber nicht nur aus dem BDSG, sondern auch aus der DS-GVO.

Die Einwände des Verantwortlichen, Hinweisgebern Vertraulichkeit zugesichert zu haben, Hinweisgeber seien generell schutzbedürftig oder auf Hinweise zur Beseitigung von Missständen angewiesen zu sein, führen jeweils für sich genommen noch nicht zur zulässigen Auskunftsverweigerung. Insoweit bezieht sich der BGH auch auf das lesenswerte Urteil des LAG Baden-Württemberg vom 17. März 2021 (21 Sa 43/20). Das Geheimhaltungsinteresse des Hinweisgebers hat regelmäßig etwa dann zurückzutreten, wenn dieser wider besseres Wissen oder leichtfertig unrichtige Angaben gemacht hat. Ver-

schulden des Hinweisgebers soll aber nur ein Element der Betrachtung sein, weil Unterlassungsansprüche gegen unrichtige Tatsachenbehauptungen auch verschuldensunabhängig mit Unterlassungsklage bekämpft werden können. Die Richtigkeit des Hinweises ist ein weiteres maßgebliches Element: Die Erwartung der Vertraulichkeit des Hinweisgebers soll jedenfalls dann nicht für eine Geheimhaltung genügen, wenn die Beschwerde auf unrichtigen Tatsachenbehauptungen beruht. Die Darlegungs- und Beweislast für die Interessenabwägung im Einzelfall trägt der Verantwortliche: Er hat die konkreten Tatsachen zu benennen, die das überwiegende Interesse des Hinweisgebers an seiner Geheimhaltung begründen sollen.

Das Geheimhaltungsinteresse der Hausverwaltung behandelt das Gericht nur kurz: Sofern der Hinweis sachlich unrichtig ist steht der Hausverwaltung eine Verweigerung der Auskunft unter Hinweis auf Hausordnung oder Hausfrieden nicht zu, weil sie dem Verdächtigen so die Unterlassungsansprüche gegen den Hinweisgeber nehmen könnte. Eine Gefahr, dass sich niemand mehr an die Hausverwaltung wenden würde, sieht das Gericht hingegen nicht: Eine Hausverwaltung kann auch anonymen Hinweisen nachgehen.

Whistleblowing und Datenschutz stehen seit jeher in einem delikaten Wechselverhältnis und im Widerstreit zwischen Geheimhaltungs- und Offenlegungsinteressen verweist der Entwurf des HinSchG auf die allgemeinen datenschutzrechtlichen Regeln. Die Interpretation dieser Regeln durch den BGH, der unter bestimmten Umständen auch eine verschuldensunabhängige Aufdeckung der Hinweisgeberidentität als zulässig erachtet, steht in einem Spannungsverhältnis zu dem im HinSchG angedachten Schutz des redlichen Informanten. Letztlich wird sich also der Betreiber eines Hinweisgebersystems im Anwendungsbereich des HinSchG zur Vermeidung von Ordnungswidrigkeit und Schadensersatz bei seiner Interessenabwägung auch von den spezialgesetzlichen Wertungen des HinSchG leiten lassen.