Verdachtsmeldung vs. Datenschutz

Mit Inkrafttreten der DSGVO riskieren Unternehmen durch den rechtswidrigen Umgang mit personenbezogenen Daten von Mitarbeitern noch höhere Sanktionen als zuvor. Eine Verarbeitung dieser Daten ist erlaubt, wenn der Zweck der Aufdeckung von Straftaten dient. Die Frage, wann genau dieser Fall vorliegt und wie mit ihm umzugehen ist, sorgt jedoch noch häufig für Unsicherheiten. *Von Alexander Stehr*

Mit Inkrafttreten der Datenschutzgrundverordnung sind datenschutzrechtliche Aspekte und die daraus folgenden verschärften Sanktionen stärker in den Fokus von Unternehmen gerückt. Im Rahmen der Mitarbeitergeschäftskontrolle – einer Pflicht aus MiFID II – erhält die Compliance-Funktion eine Vielzahl an vertraulichen personenbezogenen Daten (bspw. Depotbestand und getätigte Geschäfte). Die Compliance-Funktion muss im Interesse der Effektivität stets die Grundfunktionen „Vorbeugen, Aufdecken, Reagieren" im Blick haben. Das Vorbeugen erfolgt in der Regel durch Schulungen, Workshops und Policies, die den Mitarbeitern die erlaubten und verbotenen Geschäfte aufzeigen; das Aufdecken von nicht erlaubten Mitarbeitergeschäften, die gegen das Insiderhandelsverbot verstoßen, erfolgt durch die besagte Mitarbeitergeschäftskontrolle. Wie das Reagieren zu erfolgen hat, wird durch den Schutz der personenbezogenen Daten des Arbeitnehmers und zusätzlich durch die arbeitsrechtliche Fürsorgepflicht des Arbeitgebers beeinflusst.

Keine unabdingbare STOR-Meldepflicht

Als Reaktion auf ein persönliches Geschäft könnte eine sogenannte Verdachtsmeldung gemäß Art. 16 Abs. 2 Marktmissbrauchsverordnung (MAR) abgegeben werden. Hiernach müssen Institute, die gewerbsmäßig Geschäfte vermitteln oder ausführen, bei begründetem Verdacht auf Insiderhandel unverzüglich die BaFin unterrichten. Getreu dem Motto „Melden macht frei" werden verdächtige Mitarbeitergeschäfte der BaFin per STOR-Meldung angezeigt. Aber der Teufel steckt wie immer im Detail. Nur bei einer ausdrücklichen Regelung, dass verdächtige Mitarbeitergeschäfte der BaFin zu melden sind, kann ein arbeits- oder datenschutzrechtlicher Pflichtverstoß des Arbeitgebers mit Sicherheit ausgeschlossen werden. Doch genau hier liegt das Problem, da es keinen direkten Verweis von der Mitarbeitergeschäftskontrolle (MiFID-II-Pflicht) auf die Meldung von verdächtigen persönlichen Geschäften (MAR-Pflicht) gibt. Beide Verpflichtungen sind in verschiedenen Europäischen Rechtsverordnungen geregelt, die unterschiedliche Zielrichtungen haben: MAR fokussiert auf die Marktintegrität, MiFID II hat primär Anleger-/Kundenschutz im Blick. Daher ist nicht von einer unabdingbaren STOR-Meldepflicht auszugehen.

Zwei mögliche Alternativen

Widmen wir uns nur kurz dem Wortlaut, aus dem sich die Verdachtsmeldung ergibt: „Institute, die gewerbsmäßig Geschäfte vermitteln oder ausführen, müssen bei einem Verdacht eine Meldung abgeben". Hieraus könnte man zwei Alternativen ableiten: Eine Meldepflicht besteht nur bei Geschäften, die das Institut selbst vermittelt oder ausgeführt hat und bei denen erstens ein Verdacht aufgetreten ist oder zweitens bei sämtlichen Geschäften, die dem Institut zur Kenntnis gelangen – unabhängig davon, ob das Institut das Geschäft vermittelt oder ausgeführt hat. Eine eindeutige Meldepflicht lässt sich nicht ableiten. Auch der Sinn und Zweck der Vorschrift lässt keinen eindeutigen Schluss zu: Art. 16 MAR regelt primär die Vorbeugung und Aufdeckung von Marktmissbrauch – die Meldung ist nur eine Folge, die sich zweifelsfrei aus der Aufdeckung ergibt, um einen effektiven Schutz der Marktintegrität zu gewährleisten. Kurz gesagt: Beide Normen regeln unter Berücksichtigung des Schutzzwecks inhaltlich das Gleiche: Vorbeugung und Aufdeckung.

Meldepflicht von Mitarbeitergeschäften gem. Art. 16 MAR ist nicht eindeutig

Jedoch enthält Art. 16 MAR ein Add-On: die Meldepflicht an die BaFin. Nur weil es für Mitarbeitergeschäfte in der MiFID II keine direkte Meldepflicht gibt, kann die Meldepflicht aus der MAR nicht durch eine Analogie zweifelsfrei konstruiert werden. Insgesamt lässt sich in der gebotenen Kürze festhalten: Eine eindeutige Meldepflicht von Mitarbeitergeschäften gem. Art. 16 MAR an die BaFin gibt es nicht.

Sanktionen für Missstände hängen vom Einzelfall ab

Entscheidend muss sein, dass die Compliance-Funktion auf Missstände angemessen reagiert und der betroffene Mitarbeiter bei Verdachtsmomenten ausreichend sanktioniert wird. Die Sanktionen hängen vom Einzelfall ab, etwa von der Intensität des Verdachts oder ob es sich um eine Wiederholungstat handelt. Zumindest wenn sich ein Verdachtsmoment konkretisiert und mit Sicherheit ein verbotenes Insidergeschäft vorliegt, sollte dem Mitarbeiter durch Löschen von IT-Berechtigungen unverzüglich der Zugang zu Insiderinformationen entzogen werden und seine Versetzung in einen weniger informationssensiblen Bereich erfolgen. In einem solchen Fall sollte auch eine STOR-Meldung an die BaFin intensiv geprüft werden. Zusätzlich sind arbeitsvertragliche Reaktionen in Betracht zu ziehen. In jedem Fall ist der Vorgang, insbesondere die eingeleiteten Schritte sowie deren Ergebnisse, nachvollziehbar zu dokumentieren, um eine hinreichende Transparenz gegenüber Aufsichtsbehörden und Prüfern sicherzustellen.

Alexander Stehr ist Volljurist und bei der IKB Deutsche Industriebank AG als Compliance Officer im Bereich WpHG-Compliance tätig.

Der Transparenz verpflichtet

Die regulatorische Belastung auf deutsche Finanzinstitute wächst stetig und steigert die Anforderungen an die Bank-IT. Denn Banken müssen sich mehr denn je auf ihre Daten verlassen können, um der von der Regulatorik geforderten Transparenz Rechnung tragen zu können. *Von Axel Schmale*

Banken müssen aufgrund ständig neuer Regularien, wie etwa der 5. EU-Geldwäscherichtlinie, deutlich mehr Daten vorhalten als noch vor einigen Jahren. Darüber hinaus erfordern Vorschriften wie DSGVO, PSD2 und BCBS 239 eine systemeinheitliche Sicht auf Daten – vor allem auf Geschäftspartnerdaten. Die Menge an Informationen in Konzernfinanzunternehmen kann sich schnell mal auf 20 Millionen und mehr Datensätze summieren – mit unterschiedlichem Überschneidungsgrad je Kundengruppe oder Tochterunternehmen. Zur Herausforderung wird dieser Aspekt beim Thema Betrugsabwehr und wenn Kreditinstitute Geschäftspartner- und Kundendaten für (BaFin-) Reportings ad hoc und in Echtzeit abrufen sollen. Denn stimmt die Datenbasis dabei nicht, sind Reportings nicht belastbar und Compliance-Anforderungen können nicht eingehalten werden.

Der regulatorische Druck in der Finanzbranche wächst

Vor dem Hintergrund der im Juli in Kraft getretenen 5. EU-Geldwäscherichtlinie müssen Finanzinstitute insbesondere bei der Neuanlage von Kunden und Geschäftspartnern mehr Daten erheben, prüfen und revisionssicher festhalten. Somit gilt es auch, IT-Systeme und Applikationen, die diese Daten beherbergen sollen, entsprechend fit zu machen. Dabei geht es vor allem um die Fragen: Welche Regularien erfordern konkret die Erhebung welcher Art von Daten? Welche Informationen müssen den Datensätzen bei der Neukundenanlage im IT-System sofort mitgegeben werden und wo sind eventuell weitere benötigte Informationen zu beschaffen? Beispielsweise müssen geldwäscherechtlich Verpflichtete nun vor Begründung einer neuen Geschäftsbeziehung zwingend Einsicht in das Transparenzregister nehmen. Außerdem sind sie künftig verpflichtet, ihre Geschäftspartner mit Beziehungen zu Hochrisikoländern intensiver zum Unternehmensgegenstand und zu einzelnen Transaktionen zu befragen. Auch müssen sie neue sowie bestehende Geschäftsbeziehungen stärker überwachen. Doch diese Informationen festzuhalten, gestaltet sich durch die in Banken typisch gewachsene heterogene IT-Landschaft und durch Legacy-Systeme schwierig. Und eine konzernweit einheitliche Sicht auf Geschäftspartnerdaten fehlt aus diesem Grund meist völlig. Die Daten liegen somit in unterschiedlichen Systemen, in verschiedenen Formaten, redundant und teilweise veraltet vor. Damit können auch auf den ersten Blick scheinbar profanere Fragen – ob es den neuen Geschäftspartner bereits im System gibt, ob er aus anderen Tochterunternehmen oder Sparten bekannt ist, welche Identifikationsverfahren genutzt wurden und ob der Kunde im Rahmen der DSGVO mit der Datenhaltung einverstanden ist – nicht zweifelsfrei beantwortet werden.

Konzernweite Geschäftspartner-ID

Die Lösung kann eine konzernweite Geschäftspartner-ID sein. Dieser Konzerngeschäftspartner-Datensatz entspricht damit dem sogenannten „Golden Record", also dem „Single Point of Truth" für alle mit einem Kunden verbundenen Kontaktdaten. Über den Golden Record werden die bisher in den unterschiedlichen Systemen erfassten und doppelten Informationen über den jeweiligen Geschäftspartner vereinheitlicht. Außerdem wird sichergestellt, dass die Daten korrekt, aktuell und für alle Sparten einheitlich vorliegen – der Geschäftspartner also eindeutig identifizierbar ist. Alle Berechtigten können so auf den gleichen, qualitätsgesicherten Datensatz zum jeweiligen Geschäftspartner zugreifen. Mögliche Fehler bei Sanktionslistenprüfungen oder bei der Reporting-Erstellung können auf diese Weise ebenfalls minimiert werden.

Vor dem Hintergrund der regulatorisch geforderten, zunehmend strengeren Dokumentationspflichten sollte die durchgängige Eliminierung von Datenqualitätsproblemen daher für alle Banken und Finanzdienstleister oberste Priorität haben. Sie müssen insbesondere die Prozesse der Datengewinnung, des Datenmanagements und des Finanz-Reportings verbessern – und eine professionelle Data Governance etablieren. Nur so sind ein effektives Managen von Geschäftspartnerdaten und die genaue Kenntnis über den Kunden möglich, damit auch die Rechtskonformität.

Axel Schmale ist Account Manager DQ Sales bei Uniserv sowie Branchenexperte für den Finanzsektor und besitzt über 15 Jahre Erfahrung in der IT-Branche.