bratschi
wiederkehr
& buob

Investigations Newsletter Mai 2017

Inhaltsverzeichnis

1. Einleitung

Die Verletzung von gesetzlichen Bestimmungen, regulatorischer Standards und ethischer Anforderungen, also Compliance- und Governanceverletzungen können für Ihr Unternehmen zu teils massiven Kosten führen. Regelmässig sind diese Kosten höher, wenn Sie in Unkenntnis der eigenen Schwachstellen und konkreten Fehler in Ihrem Unternehmen Ziel einer (externen) Straf- oder Administrativuntersuchung werden. Denn ohne das umfassende Wissen über die eigenen Schwachstellen und Fehler lässt sich keine Strategie für den Umgang mit diesen entwickeln. Sie können auf die Untersuchungsergebnisse von Straf- und Administrativbehörden nur reagieren. Die frühzeitige interne Untersuchung von vermuteten Compliance- und Governanceverletzungen belässt Ihrem Unternehmen dagegen das Heft in der Hand. Sie kennen das Ausmass der Verletzungen, Sie können den möglichen Schaden einschätzen und die notwendigen Schritte einleiten. Mandatieren Sie für Ihre Untersuchung unsere Anwaltskanzlei, sind die Untersuchungsergebnisse erst noch vom Anwaltsgeheimnis geschützt und Sie können nicht verpflichtet werden, diese den Straf- und Untersuchungsbehörden offen zu legen.[1]

Mögliche Auslöser für interne Untersuchungen sind Hinweise von Kunden in Reklamationsschreiben, Anspruchsschreiben von Anwälten, die geschädigte Kunden oder Mitarbeiter vertreten, Auskunftsersuchen von Straf- oder Administrativuntersuchungsbehörden wie der Eidgenössischen Finanzmarktaufsicht (FINMA) oder der Wettbewerbskommission (WEKO), Berichte der internen Revision, Mitteilungen und Vorwürfe in der Presse und in den Medien sowie Vorfälle, welche über eine interne oder externe Whistleblowing-Stelle gemeldet werden. In den genannten Fällen sollten Sie beurteilen, ob es sich um eine leicht einzugrenzende Angelegenheit handelt, welche kein Potential für Weiterungen hat oder ob die Durchführung einer internen Untersuchung notwendig ist. Berücksichtigen Sie dabei die Interessenslage Ihres Unternehmens und aller weiteren Beteiligten, z.B. betroffene Kunden oder Dritte. Hierbei drängt sich – insbesondere unter dem Aspekt der Sorgfaltspflicht der Verwaltungsräte und Geschäftsführer nach Art. 717 Abs. 1 OR – auch eine Risikoeinschätzung hinsichtlich der involvierten Personen, der möglichen materiellen und immateriellen Schäden, der Relevanz für die Geschäftsleitung sowie der Öffentlichkeitswirkung auf. Bei mutmasslich schwerwiegenden oder systematischen Missständen kommen Sie oftmals nicht darum herum, eine interne Untersuchung einzuleiten, selbst wenn nur blosse Behauptungen und keine weiteren Anzeichen für das Vorhandensein des gemeldeten Missstandes vorliegen, weil an die Öffentlichkeit gelangte Vorwürfe – auch wenn sie unbegründet sind – eine Öffentlichkeitswirkung und damit verbunden Reputationsschäden für Ihr Unternehmen nach sich ziehen können. Eine interne Untersuchung, in der Regel bestehend aus einer Auswertung von Dokumenten und Befragungen von Mitarbeitenden, dient zur Sachverhaltsermittlung, Minimierung materieller und immaterieller Schäden, Sicherstellung von gerichtsverwertbaren Beweisen, Berichterstattung an die Geschäftsleitung, an den Verwaltungsrat und unter Umständen an eine allfällige Aufsichtsbehörde sowie zur Erarbeitung und Umsetzung von Massnahmen zur Verhinderung einer Wiederholung der aufgedeckten Missstände.

[1] Eine Einschränkung gilt jedoch für Untersuchungen im Zusammenhang mit Geldwäschereiüberwachungsaufgaben. In einem nicht publizierten Urteil vom 20. September 2016 (BGer 1B_85/2016) gelangte das Bundesgericht für die Auslagerung von Geldwäschereiüberwachungsaufgaben einer Bank an externe Anwaltskanzleien im Rahmen einer internen Untersuchung zum Ergebnis, dass für diese Tätigkeit das Anwaltsgeheimnis nicht gilt.

Typischerweise werden interne Untersuchungen bei Verdacht auf Rechtsverletzungen in den Bereichen Kartell- und Wettbewerbsrecht, Finanzmarktrecht und Geldwäscherei, Steuerrecht, Strafrecht, Umweltrecht und Datenschutz durchgeführt. Selbstverständlich können auch arbeitsrechtliche Verstösse (z.B. Nichteinhaltung von Weisungen der Arbeitgeberin, sexuelle Belästigungen, Mobbing oder Verletzungen des Gesundheitsschutzes) Gegenstand einer internen Untersuchung sein. Das Arbeitsrecht spielt vor allem aber eine wichtige Rolle bei der korrekten Durchführung einer internen Untersuchung.

Bei der Durchführung der internen Untersuchung gibt es im Gegensatz zu straf- und behördlichen Untersuchungen keine Zwangsmittel und in der Regel keine Verfahrensbestimmungen, dennoch gilt es aber zu beachten, dass durch die interne Untersuchung verschiedene Rechte Dritter (Geschäftsgeheimnisse, Bankgeheimnis, Datenschutz, etc.) und von Arbeitnehmern betroffen sein können. Zudem ist bei internationalen Sachverhalten Art. 271 StGB (Verbotene Handlungen für einen fremden Staat) und Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) Beachtung zu schenken.

Unsere Kanzlei verfügt über die Spezialisten in den verschiedenen genannten Rechtsgebieten und sie hat die notwendige Erfahrung im Umgang mit den betroffenen Rechten und Pflichten.

2. Anwendungsfälle

2.1 Kartell- und Wettbewerbsrecht

2.1.1 Szenarien

Es kann verschiedene Gründe geben, weshalb es aus der Sicht des Unternehmens angebracht erscheint, eine interne Untersuchung mit Blick auf mögliche kartellrechtliche Risiken durchzuführen.

Szenario 1: Das Sekretariat der WEKO hat bereits in verschiedenen Kantonen der Schweiz (Aargau, Bern, St. Gallen [See-Gaster], Schwyz [March-Höfe]) Hausdurchsuchungen bei Bauunternehmen durchgeführt oder entsprechende Verfahren sind noch im Gang (Graubünden, Zürich). Als Verwaltungsrat eines Bauunternehmens in einem anderen Kanton, der (noch) nicht von Untersuchungen betroffen ist, möchte man durch einen externen Rechtsanwalt abgeklärt haben, ob im eigenen Unternehmen alles rechtens abgewickelt wurde oder ob, und wenn ja, in welchem Ausmass, möglicherweise kartellrechtliche Risiken bestehen.

Szenario 2: Man weiss im Unternehmen, dass es zu kartellrechtlichen Verfehlungen gekommen ist. Eine interne Untersuchung unter der Leitung eines externen Anwalts soll den Sachverhalt aufarbeiten und sämtliche Beweismittel zusammenstellen, weil man bei der Behörde eine Selbstanzeige machen möchte, um in den Genuss der Bonusregel zu kommen.

2.1.2 Vorgehensweise

Erstens ist es bei einer kartellrechtlichen internen Untersuchung i von entscheidender Bedeutung, dass sie vom Verwaltungsrat und der Geschäftsleitung vorbehaltlos unterstützt und dies intern auch entsprechend kommuniziert wird.

Zweitens ist eine kartellrechtliche Risikoanalyse durchzuführen:

- Besteht die Gefahr von horizontalen Absprachen? Zum Beispiel bei Arbeitsgemeinschaften, Einkaufsgemeinschaften, Spezialisierungs- oder Forschungskooperationen, Teilnahme an Verbandsaktivitäten, Austausch von marktsensitiven Informationen, Einsitznahme in Verwaltungsräten von Konkurrenten, Joint-Ventures zwischen Wettbewerbern, Teilnahme an Submissionen, direkten oder indirekten Preisabsprachen, Preisempfehlungen, Gebiets- oder Kundenzuteilungen, Boykotte, Austausch von Offerten oder „schwarze“ Kundenlisten?
- In vertikaler Hinsicht gilt es abzuklären, ob z.B. Preisbindungen zweiter Hand vorliegen (feste Wiederverkaufspreise oder Mindestpreise bei Distributoren), ein absoluter Gebietsschutz (kein passiver Verkauf möglich) vereinbart oder Verkauf via Internet untersagt wurde oder in einem selektiven Vertriebssystem nebst qualitativen auch quantitative Kriterien vorgegeben wurden.
- Für den Fall, dass die Möglichkeit besteht, in gewissen Märkten marktbeherrschend zu sein, ist sicherzustellen, dass keiner der Missbrauchstatbestände vorliegt, wie z.B. die Verweigerung von Geschäftsbeziehungen, die Diskriminierung von Handelspartnern, die Erzwingung unangemessener Preise oder Geschäftsbedingungen oder die gezielte Unterbietung derselben oder Koppelungsgeschäfte.

Drittens sind ausgehend von der Risikobeurteilung die zu interviewenden Personen festzulegen und vor den Interviews durch den externen Anwalt entsprechend von der Unternehmensführung zu instruieren, voll zu kooperieren und die Tatsachen und allfällige Beweismittel auf den Tisch zu legen.

Viertens sind physische Dokumente, wie Protokolle, Verträge, Korrespondenz, Ablagen und elektronische Dokumente, wie E-Mails und elektronische Ablagen zu sichten und je nach Bedarf mit Spezialisten nach festgelegten Stichwörtern oder Namen forensisch zu untersuchen und bei Unklarheiten oder Fragen mit den Involvierten zu klären.

Fünftens wird alles in einem Bericht festgehalten und mit der Geschäftsleitung und mindestens dem Verwaltungsratspräsidenten besprochen sowie allfällige weitere Schritte festgelegt.

2.1.3 Besonderheiten

In der Schweiz beträgt die Sanktion in Form einer Busse maximal 10 Prozent des in den letzten drei Geschäftsjähren in der Schweiz erzielten Umsatzes des Unternehmens.

Die Bonusregelung sieht vor, dass der vollständige Erlass der Sanktionen nur einem einzigen Unternehmen – demjenigen, das zuerst meldet – gewährt wird. Die weiteren Unternehmen können je nach Wichtigkeit des Beitrages zum Verfahrenserfolg noch in den Genuss von einer maximalen Bussenreduktion von 50 Prozent kommen.

Christian Wind
Dr. iur. HSG, LL.M., EMBA IMD,
Rechtsanwalt, Partner
Co-Leiter Compliance und Investigations
Co-Leiter Wettbewerb, Medien und Immaterialgüter
Telefon +41 58 258 10 00
christian.wind@bratschi-law.ch

2.2 Finanzmarktrecht und Geldwäscherei

2.2.1 Ausgangslage

Im Finanzdienstleistungsbereich sind die von der FINMA überwachten Finanzintermediäre durch eine veritable „Regulierungswut“ oder Überregulierung gefordert und bei schlanken Unternehmensstrukturen allenfalls gar überfordert. Nicht genug, dass die Regulierungssubstanz zusehends und in bislang ungebremsten Tempo – das Finanzmarktinfrastrukturgesetz (FinfraG), das Finanzdienstleistungsgesetz (FIDLEG) und das Finanzinstitutsgesetz (FINIG) lassen grüssen – dichter wird, hinzukommen etliche Bereiche und Themen, in und zu welchen die Erwartungen der FINMA gar zum Teil weit über das materiell-rechtlich Festgeschriebene hinausgehen. Mark Branson, Direktor der FINMA, hat zum Beispiel im April 2016 anlässlich der jährlichen FINMA-Medienkonferenz sinngemäss gefordert, dass Meldungen bei Geldwäschereiverdacht erstattet werden müssen, auch wenn die gesetzlichen Voraussetzungen der Meldepflicht noch nicht erreicht sind.

Ein organisatorisch auch nur leicht ungenügend aufgestellter Finanzintermediär, Altlasten oder zu risikoreiche Aktivitäten können für jeden Finanzintermediär massive Konsequenzen nach sich ziehen, wie verschieden Fälle in den vergangenen Monaten gezeigt haben (z.B. massive Sanktionen gegen verschiedene Banken im 1MDB-Skandal). Es ist daher angezeigt, vorausschauend und proaktiv Risiken im Bereich der Finanzmarktregulierung und der Geldwäscherei zu adressieren und wirksam und umfassend einzugrenzen. Reaktive Massnahmen nach «Unfällen» können zudem gegen behördliche Untersuchungen vorbeugen, wenn Verfehlungen intern rechtzeitig erkannt und bereinigt werden können. Ist man zu spät, gerät der Finanzintermediär in die unerbittliche Maschinerie des Finanzmarktaufsichts-Enforcement der FINMA

2.2.2 FINMA-Enforcement

Die FINMA erteilt nicht nur Bewilligungen und beaufsichtigt Finanzintermediäre. Ein Schwerpunkt ihrer Tätigkeit ist die Durchsetzung von Aufsichtsrecht mit eigenen Verfahren gegen Institute oder Personen durch den Geschäftsbereich Enforcement. In diesem sind heute über 80 Mitarbeitende tätig. Vorabklärungen und daran anschliessend Enforcementverfahren leitet die FINMA bei Hinweisen ein, dass Aufsichtsrecht verletzt sein könnte. Ergeben diese Verfahren tatsächlich schwere Verletzungen des Aufsichtsrechts, erlässt die FINMA eine Verfügung und ordnet Massnahmen zur Wiederherstellung des ordnungsgemässen Zustands an. Diese Massnahmen können gravierend sein und haben teilweise auch repressiven Charakter (Berufsverbot, Publikation, Gewinneinziehung, Bewilligungsentzug, Liquidation). Die Verfügungen der FINMA können beim Bundesverwaltungsgericht und in dritter Instanz beim Bundesgericht angefochten werden.

Die Verfahren können sich auch gegen Marktteilnehmer richten, welche für ihre Tätigkeit eine Bewilligung bräuchten, aber ohne solche tätig sind. Die Enforcementverfahren gegen unerlaubt tätige Unternehmen führen in der Regel zur Liquidation und zum Konkurs. Im Bereich Marktaufsicht kann die FINMA zudem bei Verdacht auf Missbräuche (Ausnützen von Insiderinformationen, Marktmanipulation, unkorrektes Offenlegen von Beteiligungen) auch gegen Marktteilnehmer vorgehen, welche nicht ihrer Aufsicht unterstehen.

Für ihre Untersuchungen setzt die FINMA auch Untersuchungsbeauftragte (Prüfgesellschaften, Treuhandfirmen, spezialisierte Compliance-Berater, Anwaltskanzleien) ein, welche vor Ort in den Unternehmen den Sachverhalt abklären, mit forensischen Mitteln und auch mit Befragungen.

2.2.3 Vorbeugung

Es stellt sich damit die Frage, wie sich Finanzintermediäre aufstellen und rüsten können, um das Risiko eines FINMA-Enforcements auszuschliessen oder möglichst tief zu halten. Es ist auf drei Ebenen anzusetzen.

Erste unabdingbare Grundlage zur Vorsorge und Sicherstellung von Compliance sind erstens ein internes Regulativ, welches den aufsichtsrechtlichen Anforderungen genügt. Allein die Erarbeitung und der Unterhalt eines solchen stellen Herausforderungen dar, welche Ressourcen binden und Kosten verursachen. Allerdings zeichnet sich zusehends ab, dass es, wie erwähnt, unter Umständen nicht mehr genügt, über ein Regelwerk zu verfügen, welches die gesetzlichen Anforderungen abbildet. Die Finanzintermediäre sind gehalten auch Auflagen umzusetzen, welche von der FINMA darüber hinaus eingefordert werden. Diese betreffen neben rein regulatorischen Aspekten auch organisatorische, operationelle und personelle Themen auf allen Stufen des Unternehmens. Das interne Regelwerk hat ferner nicht nur auf dem Papier konform zu sein, auch seine Umsetzung muss bezüglich Wirksamkeit zu konformen Ergebnissen führen (design and operational effectiveness).

Zweitens sind interne Kontroll- und Prüfprozesse vorzusehen, welche die Einhaltung der Regularien und eine zeitnahe Aufdeckung von trotzdem auftretenden Verwerfungen sicherstellen.

Kommt es, drittens, eben trotzdem zu Vorfällen sind diese rasch zu adressieren, intern mit Beizug von externen Spezialisten zu untersuchen und zu bereinigen, so dass der gesetzliche Zustand ohne behördliche Interventionen wieder hergestellt werden kann. Der Beizug von Experten von ausserhalb der Organisation gewährleistet eine neutrale Sicht und eine unabhängige Untersuchung. Die Vorteile einer selber angeordneten Untersuchung gegenüber einem von der FINMA eingesetzten Untersuchungsbeauftragten sind offensichtlich. Initiative und Handlungshoheit liegen noch in der Hand des Unternehmens. Unter Umständen kann sich aber auch wenn bereits ein FINMA-Untersuchungsbeauftragter im Hause ist aufdrängen, parallel dazu eigene Abklärungen durchführen zu lassen.

Ziel der Vorkehrungen auf allen drei Ebenen muss sein, dass der Finanzintermediär die Einhaltung der tatsächlichen Erwartungen der Behörden vollumfänglich gewährleistet und auf Vorfälle rechtzeitig und adäquat reagieren kann. Mit dem Fachwissen und der Erfahrung von Spezialisten unserer Kanzlei im Finanzmarktrecht, auch aufgrund früherer Tätigkeiten bei den Behörden (u.a FINMA und Meldestelle für Geldwäscherei) ist Bratschi Wiederkehr & Buob in der Lage, Finanzintermediäre und Marktteilnehmer entsprechend zu beraten und zu unterstützen sowie interne Untersuchungen durchzuführen.

2.2.4 Szenarien

2.2.4.1 Aufsichtsrecht

Szenario 1: Bei der Besprechung des Jahresergebnisses im Verwaltungsrat fällt auf, dass der Erfolg des Handelsgeschäfts im Vergleich zu den Vorjahren aussergewöhnlich und überproportional zum guten Ergebnis der Bank beigetragen hat. Auch wenn dies zwar einerseits erfreulich ist, aber andererseits eben auch auffällig, sollte der Verwaltungsrat dies kritisch hinterfragen. Es kann allenfalls angezeigt sein, die Handelsaktivitäten durch einen unabhängigen Dritten mit Fachwissen im Effektenhandel analysieren zu lassen. Ein allfälliger Missstand liesse sich dadurch vor dem Eingreifen der Behörden beheben und mit Massnahmen kann verhindert werden, dass Vorfälle vergleichbarer Art inskünftig nicht mehr vorkommen können.

Szenario 2: Die Bank finanziert im Firmenkundengeschäft ein an der Börse kotiertes mittelgrosses Unternehmen mit Krediten. Gleichzeitig übernimmt die Bank eine massgebliche Beteiligung am Unternehmen. Aufgrund der Besprechung des Kreditdossiers an der Geschäftsleitungssitzung der Bank erfährt das für den Handel verantwortliche Mitglied der Geschäftsleitung, dass sich die Situation des Unternehmens massiv verschlechtert hat. Wie sich einige Zeit später herausstellt, hat die Bank damit begonnen, den Aktienanteil am Unternehmen schrittweise über die Börse zu verkaufen. Dem für die Verwaltung des Nostro-Bestands verantwortlichen Mitarbeitenden, dem für ihn zuständigen Mitglied der Geschäftsleitung, dem Compliance-Officer oder gar der Bank selber drohen, ins Visier der FINMA und der Strafverfolgungsbehörde zu geraten. Es stellt sich die Frage, ob die Massnahmen und Vorkehren der Bank für den Umgang mit Interessenkonflikten und privilegierten Informationen die erforderlichen Wirkungen erzielen konnten oder vielmehr, weshalb nicht. Die rechtzeitige Überprüfung durch einen unabhängigen und erfahrenen Dritten lässt entsprechende Risiken rechtzeitig erkennen und reduzieren.

Szenario 3: Ein Unternehmen vermittelt Finanztransaktionen zwischen ausländischen professionellen Gegenparteien und ist dabei äusserst erfolgreich. Die Tätigkeit ist aufsichtsrechtlich nicht bewilligungspflichtig. Mit dem Erfolg weitet das Unternehmen seine Geschäftstätigkeit aus und bietet weitere Dienstleistungen an, ohne zu erkennen, dass dies gegebenenfalls zu einer von den Finanzmarktgesetzen regulierten Tätigkeit und damit zu einer Unterstellungspflicht führt. Es drohen ein Enforcementverfahren der FINMA und die Anordnung der Liquidation. Eine rechtzeitige Analyse der neuen Geschäftstätigkeit stellt sicher, dass mit der FINMA vor einem Eingreifen die Thematik einer Bewilligung aufgenommen und ein entsprechendes Gesuch gestellt werden kann.

2.2.4.2 Geldwäscherei

Szenario 4: Aufgrund einer ausländischen Medienmitteilung ist der Finanzintermediär verpflichtet, der Meldestelle für Geldwäscherei eine Verdachtsmeldung zu erstatten. Im Rahmen der Erarbeitung der einzureichenden Dokumente stellt sich heraus, dass der Finanzintermediär über geldwäschereirelevante Altlasten verfügt, was eine aufsichtsrechtliche und strafrechtliche Lawine ins Rollen bringen könnte. Ein unabhängiger Dritter, der die notwendige Erfahrung mitbringt, kann die Bereinigung von Altlasten effizient und unbelastet von internen Zwängen vorantreiben, durchfüh-

ren und überwachen. Unsere Kanzlei kann Finanzintermediäre durch einzelfallgerechte und massgeschneiderte Vorkehren so vor drohenden Ermittlungen schützen und behördlichen Untersuchungen zuvorkommen.

Szenario 5: Der Finanzintermediär führt eine Transaktion aus, die – wie sich nachträglich erweist – den objektiven Tatbestand der strafrechtlichen Geldwäschereibestimmung erfüllt hat. Der Mitarbeitende, die Complianceverantwortlichen oder der Finanzintermediär selber könnten in den Fokus der Strafverfolgungsbehörde geraten. Zur Eindämmung dieses Risikos gilt es, die Umsetzung der organisatorischen Massnahmen, die sich aus dem Geldwäschereigesetz (GwG) ergeben, umfassend auf ihre Wirksamkeit hin zu überprüfen. Wird dies durch einen unabhängigen und erfahrenen Dritten gemacht, können die Risiken substantiell vermindert werden. Zudem wird sich der Finanzintermediär im Einzelnen aussichtsreich auf die getroffenen Massnahmen berufen können.

Marcel Aellen
Dr. iur., Rechtsanwalt, Partner
Telefon +41 58 258 16 00
marcel.aellen@bratschi-law.ch

Arnaud Beuret
MLaw, LL.M.
Telefon +41 58 258 16 00
arnaud.beuret@bratschi-law.ch

2.3 Steuerrecht

Gemeinsam mit fast 100 Staaten, darunter alle wichtigen Finanzzentren, hat sich die Schweiz verpflichtet, den automatischen Informationsaustausch (AIA) zu implementieren. Mit Hilfe dieses neuen globalen Standards soll die grenzüberschreitende Steuerhinterziehung verhindert werden. Der Standard sieht vor, dass Staaten, die den AIA untereinander vereinbart haben, gegenseitig Informationen über Finanzkonten austauschen. Damit erfolgte der letzte Schritt in Richtung internationale Steuertransparenz. Seit dem 1. Januar 2017 werden in der Schweiz nun Daten erhoben, die im Rahmen des AIA ab dem Jahr 2018 erstmals an ausländische Steuerbehörden gemeldet werden (vgl. dazu bereits den BWB Compliance Newsletter, Juni 2015).

Unabhängig von diesem neu implementierten Instrument haben ausländische Steuerbehörden jedoch bereits heute mit einer sog. Gruppenanfrage die Möglichkeit, Daten von Steuerpflichtigen für die Zeit vor dem 1. Januar 2017 bzw. ab dem 1. März 2013 anzufordern. Bei einer Gruppenanfrage müssen schweizerische Banken auf Anfrage eines ausländischen Fiskus Informationen über Gruppen erteilen, die ein bestimmtes Verhalten gezeigt oder bestimmte Transaktionen getätigt haben, d.h. bestimmte vorher angefragte Identifikationsmerkmale erfüllen. Das Instrument der Gruppenanfrage hat in letzter Zeit insbesondere aufgrund eines im letzten Herbst ergangenen Bundesgerichtsentscheides eine neue Dimension erreicht, welche es – insbesondere hinsichtlich allfälliger derzeit noch nicht deklarierter Vermögenswerte – zu berücksichtigen gilt.

So versuchte die niederländische Steuerverwaltung erfolgreich nach Abschluss des niederländischen Offenlegungsprogramms mittels Gruppenanfragen an die Namen derjenigen Personen zu gelangen, die ihren Steuerpflichten nicht nachgekommen sind und auch nicht am Offenlegungsprogramm teilgenommen haben. Zu diesem Zweck reichten die Niederlande bereits im Juni 2015 ein entsprechendes Amtshilfeersuchen betreffend namentlich nicht genannte UBS-Kunden ein. Davon erfasst wurden diejenigen in den Niederlande domizilierten Kunden der UBS, die im Zeitraum vom 1. Februar 2013 bis 31. Dezember 2014 ein Schweizer Konto bei eben dieser Bank hatten und darüber hinaus (i) von der UBS ein Schreiben erhalten haben, in dem ihnen mitgeteilt wurde, dass die Kontobeziehung gekündigt werde, wenn sie ihre Steuerkonformität nicht nachweisen und (ii) der entsprechende Nachweis gegenüber der UBS in der Folge ausblieb.

Im vergangenen Herbst hat das Bundesgericht das niederländische Amtshilfeersuchen überraschend gutgeheissen. Die Anforderungen an derartige Amtshilfegesuche wurden vom Gericht genauer definiert, wobei insbesondere festgehalten wurde, dass nicht erforderlich sei, dass Gruppenanfragen den Namen der betroffenen Personen ausdrücklich nennen. Vielmehr genüge es bereits, wenn die Anfrage ausreichende Informationen zur Identifikation der betroffenen Person enthalte. Obwohl das Bundesgericht in seinem Urteil festhält, dass sich der Entscheid nur auf den konkreten Fall des Doppelbesteuerungsabkommens (DBA) mit den Niederlanden beziehe und nicht auch auf Abkommen mit anderen Ländern, ist das Urteil wohl so zu interpretieren, dass die Eidgenössische Steuerverwaltung (EStV) ausländische Gruppenanfragen ohne Namensnennung – gestützt auf Amtshilfeabkommen, die eine Amtshilfe basierend auf Gruppenersuchen zulassen – fortan bewilligen darf. Aufgrund dieser erleichterten Anforderungen an die Steuertransparenz besteht die Gefahr, dass das Instrument der Amtshilfe für eigentlich verbotene „fishing expeditions“ ohne klare Verdachtsgrundlage verwendet wird.

Unbestritten ist, dass das Instrument der Gruppenanfrage eine neue Dimension erreicht hat. Aufgrund des Umstandes, dass viele in der Schweiz ansässige Banken auf Anraten der FINMA die Weissgeldstrategie durch Versand solcher Schreiben betreffend Steuerehrlichkeit proaktiv angegangen sind, dürfte in naher Zukunft mit weiteren Gruppenanfragen seitens ausländischer Steuerbehörden unter Verwendung desselben Musters zu rechnen sein. So haben die Niederlande ein zweites Amtshilfegesuch für Kunden der Credit Suisse gestellt, deren Daten bereits ausgeliefert wurden. Weiter sind bei der Eidgenössischen Steuerverwaltung (EStV) derzeit vergleichbare Amtshilfegesuche von Spanien und Frankreich anhängig. Diese weitreichenden länderspezifischen Anfragen sollten auf Stufe der betroffenen Banken zu internen Untersuchungen führen, die innert Kürze abgewickelt werden sollten. Banken, welche derzeit noch über nicht deklarierte Vermögenswerte verfügen bzw. keine entsprechenden Nachweise ihrer Kunden betreffend Steuerkonformität erhalten haben, ist eine erneute Kontaktierung ebendieser Kunden unter Hinweis auf die aktuellen Entwicklungen anzuraten.

Als Rechtsvertreter des in den Niederlanden ansässigen UBS-Kontoinhabers haben wir im Rahmen des Rechtsverfahrens bis vor das Bundesgericht wesentliche Erkenntnisse gewonnen, welche Bratschi Wiederkehr & Buob für betroffene Banken zum idealen Partner für eine interne Untersuchung machen. In Kürze können wir aus unserer Erfahrung bereits die folgenden Empfehlungen zusammenfassen:

- Der frühzeitige Beizug von externen Beratern zwecks Begleitung und Abwicklung des Verfahrens vereinfacht den Prozess.
- Das Coaching betroffener Kontoinhaber (Einrichtung einer Hotline, Empfehlung von Rechtsvertretern, etc.) wird am Markt positiv aufgenommen.
- Der professionelle Austausch mit der Eidgenössischen Steuerverwaltung fördert den Informationsfluss und vermeidet Missverständnisse.
- Das Vorbereiten eines Notfallplanes (Medienmitteilung, Task Force Team, Definition des internen Prozesses etc.) mit externen Beratern zur Vermeidung eines Überraschungseffektes ist zu empfehlen.

Während künftig die Steuertransparenz durch den automatischen Informationsaustausch (AIA) sichergestellt wird, ist – unter Berücksichtigung der vorstehend ausgeführten neusten Entwicklungen im Bereich der Gruppenanfragen – Personen mit derzeit noch nicht deklarierten Vermögenswerten dringend eine Offenlegung zu empfehlen. Dies gilt insbesondere auch vor dem Hintergrund, dass in einigen Staaten derzeit (noch) attraktive Offenlegungsprogramme genutzt werden können.

Michael Alexis Barrot
Lic. iur., LL.M., dipl. Steuerexperte,
Rechtsanwalt, Partner
Leiter Steuern
Telefon +41 58 258 10 00
michael.barrot@bratschi-law.ch

Tabea Lorenz
M.A. HSG in Law and Economics
Telefon +41 58 258 10 00
tabea.lorenz@bratschi-law.ch

2.4 Strafrecht

Wirtschaftskriminalität ist ein vielschichtiges Phänomen, welches nicht nur die Strafverfolgungsbehörden und die Gerichte beschäftigt, sondern in erster Linie auch die Unternehmen selber. Interne Untersuchungen können nicht nur helfen, Fälle der Wirtschaftskriminalität aufzuklären, sondern sollten solche im Idealfall präventiv verhindern.

2.4.1 Szenarien

Szenario 1: Ein Kaderangestellter eines KMU nützt jahrelang interne Schwachstellen in der Buchhaltung seines Arbeitgebers aus. Er erstellt fingierte Rechnungen, um sich selber Zahlungen in der Höhe von mehreren hunderttausend Franken zuzuschanzen. Die Straftaten fallen erst auf, nach dem der Angestellte das Unternehmen bereits verlassen und einen Grossteil des deliktisch erlangten Geldes verspielt hatte.

Szenario 2: Ausländische Kunden eines mittelgrossen Schweizer Finanzintermediärs waschen regelmässig hohe Geldbeträge über ihre Kontobeziehung beim Finanzintermediär. Auf dem Rechtshilfeweg gelangt der Finanzintermediär in den Fokus der Strafverfolgungsbehörden, welche zum Schluss kommen, dass das Unternehmen Mitschuld an der Geldwäscherei trägt. Weil der Finanzintermediär intern mangelhaft organisiert wird, kann die Tat nicht einem bestimmten Angestellten zugerechnet werden. Als Folge davon wird der Finanzintermediär mit einer Busse bis zu CHF 5 Millionen bestraft.

2.4.2 Präventive interne Untersuchung

Wirtschaftskriminalität kann alle Wirtschaftsteilnehmer treffen. Deshalb sollte jedes Unternehmen unabhängig von seiner Grösse oder Branche auf den Ernstfall vorbereitet sein. Eine interne Untersuchung kann dazu beitragen, potentielle Straftaten im Voraus zu erkennen und entsprechende Massnahmen zu deren Verhinderung zu treffen.

In dieser präventiven internen Untersuchung wird das Unternehmen in einem ersten Schritt mit dem Ziel durchleuchtet, organisatorische, rechtliche und tatsächliche Schwachstellen zu identifizieren. Eine externe Analyse hat dabei den Vorteil, dass sie ohne Betriebsblindheit neutral und unabhängig aufdeckt, welche Praktiken und Verhaltensweisen des Unternehmens besonders kritisch sind. Die Schwachstellen des Unternehmens müssen nicht immer in tiefgreifenden organisatorischen Strukturen liegen. Interne Untersuchungen zeigen oftmals, dass einfache Sicherungsmechanismen fehlen, welche es Mitarbeitern ermöglichen, im Unternehmen Straftaten zu verüben. Zu denken ist an fehlendes Vieraugenprinzip im Zusammenhang mit Geldzahlungen, Einzel- statt Kollektivunterschriftsberechtigungen, unklare Kompetenzzuweisungen, mangelhafte Selektionsprozesse von neuen Mitarbeitern in sensitiven Bereichen, Sicherheitslücken in der IT oder bei den Zutrittsberechtigungen.

Nach der internen Untersuchung und der Analyse der Schwachstellen müssen die identifizierten Schwachstellen durch geeignete Massnahmen beseitigt werden. Dabei geht es insbesondere darum, die Organisation und die Reglemente des Unternehmens so anzupassen, dass strafrechtliche Delikte verhindert werden können. Dazu gehört, die neu definierten Regeln und Prozesse sorgfältig zu dokumentieren.

Die präventive interne Untersuchung und die Implementierung von neuen Regeln und Prozessen erfolgen nicht zum Selbstzweck. Sollte nämlich trotzdem eine Straftat im Unternehmen verübt werden, hilft eine klare Dokumentation einerseits der Identifikation des oder der Verantwortlichen. Andererseits hilft die präventive interne Untersuchung und Dokumentation dem Unternehmen, in einem Straffall darzulegen, dass es alle zumutbaren Vorkehrungen zur Verhinderung von Straftaten getroffen hat. Hätte der Finanzintermediär im oben stehenden zweiten Szenario belegen können, dass er alle erforderlichen und zumutbaren organisatorischen Vorkehren getroffen hat, um die Geldwäscherei zu verhindern, würde er nicht bestraft werden.

2.4.3 Reaktive interne Untersuchung

Neben der präventiven Funktion dienen interne Untersuchungen auch der reaktiven Aufarbeitung von Straftaten im Unternehmen. Wird in einem Unternehmen eine Straftat entdeckt, sind meistens zahlreiche Fragen offen. Mit Bezug auf das oben genannte erste Szenario wäre zu fragen: «Wer war an der Straftat beteiligt, nur ein Mitarbeiter oder hatte dieser Mitwisser und Gehilfen? Wie hoch ist der gesamte Deliktsbetrag? Gibt es neben den bisher erkannten fehlenden Geldern weitere Straftaten (Urkundenfälschung, etc.)? Welchen Einfluss hat die Straftat auf die Reputation des Unternehmens? Müssen (Aufsichts-)Behörden informiert werden?»

Besonders in dieser Anfangsphase rechtfertigt sich der Einbezug eines externen Rechtsanwaltes. Einerseits sollten die intern involvierten Personen aufgrund der unklaren Ausgangslage (mögliche Mittäter, Schadenssumme, etc.) auf ein absolutes Minimum beschränkt werden. Andererseits stellen sich vielfältige rechtliche Fragen (Strafanzeige, arbeits- und aufsichtsrechtliche Konsequenzen, mögliche Zeugenbefragungen und Beweismittelbeschaffung, finanzielle Gefährdung des Unternehmens bis hin zu einer Überschuldung, Reputation, etc.), welche zusammen mit einem Spezialisten abgeklärt werden müssen, bevor weitere Schritte eingeleitet werden.

Nach dem ersten Entscheid über das Einleiten der notwendigen Schritte, sollte das Unternehmen anhand einer internen Untersuchung das gesamte Ausmass des Straffalles aufklären lassen. Dazu gehört nicht nur die Identifikation des oder der Täter, sondern auch die Feststellung der Schadenssumme und die Auswirkungen auf die Beziehungen zu Dritten (z.B. Beeinträchtigung von Kundenvermögen). Die interne Aufarbeitung sollte ebenso festhalten, welche Massnahmen im Unternehmen zu implementieren sind, um in Zukunft solche Wirtschaftsdelikte wirksam zu verhindern. Wiederum macht es Sinn, dass ein externer Dienstleister diese interne Untersuchung durchführt. Als (aussenstehende) Anwaltskanzlei verfügen wir dazu nicht nur über das notwendige Spezialistenwissen, sondern wir sind auch unabhängig und unsere Arbeitsprodukte unterstehen dem Anwaltsgeheimnis.

Thomas Iseli
Dr. iur., LL.M., Rechtsanwalt
Telefon +41 58 258 10 00
thomas.iseli@bratschi-law.ch

2.5 Datenschutz

Die moderne Informationstechnologie bietet laufend neue Möglichkeiten zur Datenbearbeitung. Angefangen beim mobilen, globalen Datenzugriff der Mitarbeitenden über das Outsourcing der Datenverarbeitung bis zur Nutzung von internetbasierten «Application as a Servcie»-Anwendungen oder dem «Internet der Dinge». Dabei werden Personendaten, die dem Datenschutzgesetz unterliegen, ins Ausland übermittelt, dort bearbeitet und gespeichert.

Mit der Europäischen Datenschutzgrundverordnung (EU DSGVO) und der Revision des Eidgenössischen Datenschutzgesetzes (E-DSG) werden in Zukunft die Vorschriften über die Verarbeitung von Personendaten deutlich verschärft und es werden den Unternehmen zahlreiche neue Pflichten auferlegt sowie diverse Tatbestände neu unter Strafe gestellt. In der EU sind Geldstrafen bis EUR 20 Mio. möglich, in der Schweiz sind Strafen bis CHF 500‘000.00 geplant.

2.5.1 Datenschutz Compliance

Unternehmen sind angehalten, die Bearbeitung ihrer Daten in Prozessen und Regelwerken zu dokumentieren. Die neuen Gesetze sehen Dokumentationspflichten über deren Bearbeitung von Personendaten vor. Unter anderem dient das neue Instrument der Datenschutz-Folgeabschätzung (DSFA) dem Unternehmen zu Folgendem: (i) Zur Erfüllung der Dokumentationspflicht des Unternehmens; (ii) als Nachweis über die Pflicht oder den Verzicht zur Durchführung einer DSFA; (iii) als Nachweis über die Risikobeurteilung der Datenbearbeitung und (iv) als Informationsgrundlage für die Aufsichtsbehörden bei verbleibenden hohen Risiken.

Die Datenschutz-Folgeabschätzung (DSFA) beurteilt die Risiken in Bezug auf die Konformität mit der Datenschutzgesetzgebung bei der Verarbeitung von Personendaten. Ist eine Datenschutz-Folgeabschätzung gesetzlich vorgeschrieben und zeigt diese ein verbleibendes hohes Risiko, muss zudem die Datenschutzaufsichtsbehörde konsultiert werden.

Die allgemeinen Mindestvorgaben für eine DSFA sind gemäss Art. 35 Abs. 7 DSGVO:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschliesslich der vom Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die zur Bewältigung der Risiken geplanten Abhilfemassnahmen, einschliesslich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Die Durchführungsverantwortung für eine DSFA liegt beim verantwortlichen Daten-Controller (zum Beispiel Process-Owner). Eine Unterlassung kann zu einer Bestrafung des Unternehmens führen.

2.5.2 Szenarien

Zwei typische Szenarien aus unserer Beratungspraxis sind Fälle von Datendiebstahl durch Mitarbeitende oder die neuen Informationspflichten im Rahmen von Datenschutzverstössen im Unternehmen, die sogenannte „Data Breach Notification".

Szenario 1: Ein Mitarbeiter verlässt freiwillig oder auch unfreiwillig das Unternehmen und wechselt zu einem Mitbewerber. Dabei nimmt er die Kundendaten oder Geschäftsgeheimnisse zum neuen Arbeitgeber mit.

Datendiebstahl ist für die meisten Unternehmen schwer fassbar, es bestehen meistens nur Vermutungen, es fehlen aber die konkreten Beweise. Was soll ein Unternehmen bei solchen Verdachtsmomenten tun?

Das Unternehmen sollte schon bei der Einstellung von Mitarbeitenden seine Firmendaten schützen und Präventions- und Schutzmassnahmen vorsehen und diese auch an die Mitarbeitenden kommunizieren:

- Regeln für die Informationssicherheit und für die Nutzung der Informatiksysteme, insbesondere beim Einsatz von privaten Geräten (Bring your own device);
- Einsatz von Systemüberwachungssoftware sowie datenschutzkonforme Regelungen für Tracking- und Überwachungsmassnahmen bei Datenzugriffen;
- Persönliche Datenzugriffe (regelmässige Änderung von Passwörtern und keine Weitergabe von Passwörtern unter Kollegen);
- Eingeschränkte Zugriffe für vertrauliche Daten;
- Verschlüsselung des Datenverkehrs und der Datenablage;
- Geheimhaltungsverpflichtungen in Arbeitsverträgen.

Besteht ein Verdacht auf Datendiebstahl gilt es rasch zu handeln und eine sorgfältige Beweissicherung vorzunehmen. Dabei gilt es, den Täter zu identifizieren sowie den Nachweis über erfolgte Datei-Downloads und Dateizugriffe oder Datenänderungen sowie sämtliche betroffenen und relevanten Daten zu ermitteln. Dabei sind die technischen Untersuchungen eng mit dem rechtlich zulässigen Rahmen abzustimmen, damit die Beweise in einem späteren Gerichtsverfahren verwertet werden können. Mit geeigneten Massnahmen ist eine Datenweitergabe vom Täter an Dritte möglichst rasch zu unterbinden.

Dem Unternehmen stehen grundsätzlich alle zivil- und strafrechtlichen Schritte gegen den Täter offen. Diese sind aber sorgfältig abzuschätzen, oftmals ist der Weg über einen Vergleich mit dem potentiellen Täter effektiver als eine Strafanzeige. Vor jeder Strafanzeige muss genau geprüft werden, welche Risiken dies für das Unternehmen beinhaltet. Dabei ist zu berücksichtigen, dass die Strafverfolgungsbehörden eine Straftat nach ihren eigenen Planungen untersuchen und der Antragsteller keine Kontrolle über das Strafverfahren hat. Ein Strafverfahren kann relativ geräuschlos ablaufen oder aber auch grosse mediale Aufmerksamkeit erlangen. Spätestens im Rahmen eines Gerichtsverfahrens wird der Sachverhalt öffentlich. Zudem stossen Strafverfolgungsbehörden bei internationalen Sachverhalten rasch an faktische und rechtliche Grenzen. Zudem gilt es auch immer den Reputationsschaden im Auge zu behalten.

Neben Schadenersatzansprüchen gegen den Täter, stehen auch Rechtstitel aus dem Urheberrecht gegen das allenfalls verwendende Unternehmen zur Verfügung. Im Strafrecht geht es um die Unbefugte Datenbeschaffung (Art. 143 StGB), Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB)[2] oder um die Verletzung von Fabrikations- und Geschäftsgeheimnissen (Art. 162 StGB). Es sind auch weitere Tatbestände und Kombinationen denkbar. Unter anderem kann sich auch die Frage stellen, ob sich das Unternehmen, resp. die Verantwortlichen bei einem solchen Vorfall ebenfalls strafbar gemacht haben, weil sie ihre Sorgfaltspflichten verletzt haben.

Szenario 2: Ihr Unternehmen ist von einem Datendiebstahl oder einem Datensicherheitsverstoss betroffen und missachtet die neuen Informationspflichten im Rahmen von Datenschutzverstössen im Unternehmen, die sogenannte „Data Breach Notification".

«Ein Data-Breach ist ein Verstoss, gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten Unberechtigten vermutlich oder erwiesenermaßen bekannt werden. Ursachen dafür sind vielfältig und können beispielsweise in einem Hackerangriff, dem Verlust eines USB-Sticks oder Notebooks, dem Diebstahl eines Smartphones oder in einem unbefugten Weitergeben durch Mitarbeiter sein. Dabei spielt es keine Rolle ob dies bewusst oder unbewusst erfolgt.»

In einzelnen Ländern bestehen Pflichten zur Information der betroffenen Datensubjekte sowie der Aufsichtsbehörden. Mit der DSGVO wird das ab nächstem Jahr in allen EU Ländern Pflicht und mit der Revision des Datenschutzgesetzes in Zukunft auch in der Schweiz. Die DSGVO schreibt bei einer solchen Verletzung eine Information der Datenschutz-Aufsichtsbehörde innert 72 Stunden ab Kenntnisnahme der Datenschutzverletzung vor. Als Mindestanforderung bei der Meldung an die Aufsichtsbehörde ist eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze vorzunehmen. Es sind die wahrscheinlichen Folgen der Verletzung von personenbezogenen Daten zu dokumentieren und es ist eine Beschreibung der ergriffenen oder vorgeschlagenen Massnahmen des Unternehmens und gegebenenfalls Massnahmen zur Abmilderung der möglichen Auswirkungen darzustellen.

Ergibt die durchzuführende Risikoabwägung, dass durch die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht, sind diese nach Art. 34 DSGVO ebenfalls zu benachrichtigen. Dabei sind die betroffenen Personen über die betroffenen Daten sowie die Auswirkungen auf ihre Person zu informieren. Eine solche Information ist einerseits mit hohen Reputationsrisiken verbunden und andererseits mit einem enormen Organisations- und Kostenaufwand.

Eine Verletzung der Vorschriften über die «Data Breach Notification» führt zu Sanktionen und Bussen durch die Aufsichtsbehörden. Unternehmen sind daher angehalten, Prozesse für den Fall eines «Data Breaches» vorzubereiten und einen Verantwortlichen zu bezeichnen. Im Eintretensfall

[2] Das Eindringen in ein fremdes Computersystem kann ebenfalls durch heimliches Umleiten von fremden E-Mails auf eine E-Mail-Adresse des Täters geschehen (BGE 130 III 28 E. 4.2).

muss das Unternehmen rasch ermitteln können, was genau passiert ist und formal seine rechtlichen Informationspflichten einhalten. Dies erfolgt am besten in einem Team aus IT-Technikern, Kommunikationsfachleuten und juristischem Know-How.

Markus Näf
Master of Law, Rechtsanwalt
Telefon +41 58 258 10 00
markus.naef@bratschi-law.ch

3. Whistleblowing-System als Informationsquelle

Eine interne Untersuchung setzt voraus, dass das Unternehmen Anhaltspunkte zu einem möglichen Fehlverhalten hat. Durch ein funktionsfähiges Whistleblowing-System, in welches die Mitarbeitenden Vertrauen haben, können dieselben mutmassliches Fehlverhalten kanalisiert melden und das Unternehmen kann diese Hinweise prüfen sowie, falls erforderlich, eine interne Untersuchung einleiten. Durch interne Hinweise auf mögliches Fehlverhalten kann ein Unternehmen auf die Mitarbeitenden als eine der wichtigsten Informationsquellen für den eine interne Untersuchung initiierende Anfangsverdacht zurückgreifen. Aber nicht nur deshalb, sondern auch aus den folgenden Gründen ist ein Whistleblowing-System für Unternehmen ein äusserst wichtiges Compliance-Instrument:

- über kanalisierte Meldestrukturen kann im Sinne eines Frühwarnsystems eine Risikokommunikation stattfinden, so dass gemeldete Sachverhalte identifiziert und falls erforderlich angemessene Massnahmen eingeleitet werden können (Risikokommunikationsfunktion);
- es können Verstösse gegen Gesetze oder unternehmensinterne Regeln aufgedeckt werden, um im Anschluss daran interne Prozesse, Weisungen und Kontrollen auf ihre Wirksamkeit hin zu überprüfen und gegebenenfalls anzupassen (Aufdeckungsfunktion);
- im Sinne einer «Compliance Defence» kann unter Umständen eine Unternehmensverantwortlichkeit nach Art. 102 Abs. 2 StGB vermieden werden (Haftungsvermeidungsfunktion);
- bei einer Berücksichtigung von produktions- und sicherheitsrelevanten Ereignissen sowie bewusst missachteten Qualitätsdefiziten als mögliche Meldegegenstände kann ein bestehendes Qualitätsmanagement-System ergänzt werden (Qualitätssicherungsfunktion).

Ein Whistleblowing-System muss nichts Kompliziertes sein, sollte aber folgende Elemente beinhalten, damit es funktionsfähig ist:

- interne Meldungen über mutmassliches Fehlverhalten sollten sowohl von den Mitarbeitenden als auch vom Unternehmen als erwünschte Risikokommunikation, die im Interessen des Unternehmens erfolgt, wahrgenommen werden;
- es sollten interne und/oder externe Meldestrukturen (z.B. Anwaltskanzlei) bezeichnet und gegenüber den Arbeitnehmenden regelmässig als zuständige Meldestellen kommuniziert werden;
- das Meldeverfahren sowie die darauffolgende Bearbeitung der Meldung sollten zusammen mit den Rechten und Pflichten der Mitarbeitenden in einem Whistleblowing-Reglement festgehalten werden;
- eingehende Meldungen müssen zeitnah und sorgfältig überprüft werden, damit falls erforderlich auf ein Fehlverhalten mit angemessenen Massnahmen reagiert werden kann;
- es sollten angemessene Massnahmen zum Schutz von meldenden Mitarbeitenden und von einer Meldung betroffenen Mitarbeitenden bestehen.

Die konkrete Ausgestaltung eines Whistleblowing-Systems ist unternehmensindividuell und abhängig von der Unternehmensgrösse und -organisation. Bratschi Wiederkehr & Buob hat Erfahrung beim Aufbau eines funktionstüchtigen Whistleblowing-Systems und übernimmt bereits für mehrere Unternehmen die Funktion der externen Meldestelle.

Stefan Rieder
Dr. iur. HSG, LL.M., Rechtsanwalt
Telefon +41 58 258 14 00
stefan.rieder@bratschi-law.ch

4. Durchführung der internen Untersuchung

4.1 Beachtung des Arbeitsrechts

4.1.1 Untersuchungspflicht

Die Arbeitgeberin ist nicht nur berechtigt, eine interne Untersuchung durchzuführen, je nach Art und Schwere der Meldung kann sogar eine Pflicht zur Durchführung einer internen Untersuchung vorliegen. Eine Untersuchungspflicht kann sich auch aus der Fürsorgepflicht der Arbeitgeberin nach Art. 328 OR ergeben. Die Fürsorgepflicht beinhaltet die Pflicht der Arbeitgeberin, die Persönlichkeit der Mitarbeitenden zu achten und zu schützen. Bei Anhaltspunkten zu einem mutmasslichen Fehlverhalten stehen typischerweise auch einzelne oder mehrere Mitarbeitende in Verdacht. Die Arbeitgeberin sollte deshalb einen Verdacht angemessen verifizieren, da andernfalls eine ausgesprochene Kündigung ohne vorgängige Sachabklärung missbräuchlich sein kann. Die Gerichte betrachten eine Kündigung jedenfalls als missbräuchlich, wenn die Arbeitgeberin ohne Durchführung einer internen Untersuchung an ihrem Verdacht festhält, obwohl der beschuldigte Mitarbeitende die Vorwürfe ausdrücklich bestritten und eine Konkretisierung der Vorwürfe verlangt hat.

4.1.2 Untersuchungsgrenzen

Die Arbeitgeberin muss aufgrund ihrer Fürsorgepflicht nach Art. 328 OR auch bei einer internen Untersuchung die Persönlichkeit des Mitarbeitenden schützen und im Rahmen der zulässigen Datenbearbeitung im Arbeitsverhältnis die allgemeinen datenschutzgesetzlichen Bearbeitungsgrundsätze berücksichtigen. Untersuchungsmassnahmen sind deshalb zurückhaltend sowie schonend durchzuführen und dürfen nicht schikanös sein. Die Arbeitgeberin kann auch bei schwachen Verdachtsmomenten ein berechtigtes Interesse an einer internen Untersuchung haben, allerdings bedeutet dies nicht automatisch, dass sie diesen schwachen Verdachtsmomenten intensiv und systematisch nachgehen darf. Eine Verletzung der Fürsorgepflicht liegt etwa vor, wenn von einer internen Untersuchung betroffene Mitarbeitende gegenüber Vorgesetzten oder anderen Arbeitnehmenden diskreditiert werden.

Aus der Fürsorgepflicht nach Art. 328 OR lassen sich zudem verschiedene weitere Pflichten der Arbeitgeberin ableiten. Die interne Untersuchung sowie allfällige Vorwürfe gegenüber Arbeitnehmenden müssen von der Arbeitgeberin vertraulich behandelt werden, d.h. die Informationen dürfen nach dem «need to know-Prinzip» nur Personen zur Verfügung stehen, die diese aufgrund ihrer Aufgabe im Rahmen der internen Untersuchung oder aufgrund ihrer Funktion im Unternehmen (z.B. Verwaltungsrat, Geschäftsführer, General Counsel) erhalten müssen. Ansonsten werden betroffene Arbeitnehmende unnötig gegenüber anderen Arbeitnehmenden diskreditiert.

Von einer internen Untersuchung betroffene Arbeitnehmende haben zudem einen legitimen Anspruch, sich gegen die ihnen zur Last gelegten Vorwürfe verteidigen zu können. Die Arbeitgeberin sollte betroffene Arbeitnehmende über die interne Untersuchung und die Vorwürfe in Kenntnis setzen, wobei bei überwiegenden Interessen der Arbeitgeberin auch eine zeitlich beschränkte heimliche Untersuchung zulässig ist. Eine heimliche Untersuchung ist z.B. in einer Anfangsphase einer Untersuchung erforderlich und gerechtfertigt, damit die Untersuchung und Beweissicherung nicht vereitelt werden können. Sobald eine solche Vereitelungsgefahr aber nicht mehr besteht, muss

der von der Untersuchung betroffene Arbeitnehmende über die Untersuchung und die ihm zur Last gelegten Vorwürfe informiert werden.

4.1.3 Befragung von Mitarbeitenden

Bei einer internen Untersuchung werden regelmässig Mitarbeitende befragt und diese sind verpflichtet, der Arbeitgeberin wahrheitsgemäss und vollständig Auskunft zu erteilen. Eine treuwidrige Behinderung der Sachverhaltsaufklärung durch einen Mitarbeitenden kann eine fristlose Kündigung nach Art. 337 OR rechtfertigen. Bei der Befragung von Mitarbeitenden sollte beachtet werden, dass solche Befragungen geeignet sind, die Beweiskraft späterer Einvernahmen in einer Strafuntersuchung zu schwächen, weil bei Mehrfachbefragungen in Kombination mit suggestiver Einflussnahme eine gewisse Gefahr der Aussageverfälschung besteht. Die Befragungen sind deshalb nicht nur sorgfältig zu planen, sondern es muss auch dem Ablauf der Befragung und der Fragetechnik eine grosse Bedeutung beigemessen werden. Zudem sollten die Befragungen protokolliert werden, wobei dies aufgrund der Fürsorgepflicht der Arbeitgeberin dem befragten Mitarbeitenden vorgängig mitzuteilen ist.

Auch bei Befragungen von Mitarbeitenden muss die Arbeitgeberin ihre Fürsorgepflicht beachten, namentlich auch dann, wenn die Arbeitgeberin Dritte (z.B. einen Rechtsanwalt) mit der Befragung beauftragt hat. Dem ist insbesondere bei der Anordnung, der Art der Durchführung, der Form der Fragestellungen und der Protokollierung Rechnung zu tragen. Die Arbeitgeberin darf bei der Befragung z.B. nicht durch eine Anwesenheit von Anwälten ungebührlichen Druck auf den befragten Mitarbeitenden ausüben. Bei Befragungen kann der befragte Mitarbeitende infolge der Drucksituation ein berechtigtes Interesse an der Begleitung eines Rechtsbeistandes haben, selbst wenn dem Mitarbeitenden kein strafbares Verhalten vorgeworfen wird. Die Arbeitgeberin hat dieses Interesse grundsätzlich infolge ihrer Fürsorgepflicht zu berücksichtigen und die Begleitung durch einen Rechtsbeistand hinzunehmen.

4.1.4 Arbeitsrechtliche Sanktionen

Nach Abschluss der internen Untersuchung geht es in arbeitsrechtlicher Hinsicht auch darum, arbeitsrechtliche Sanktionen (Verwarnung, ordentliche oder fristlose Kündigung) sowie gegebenenfalls die Geltendmachung von Schadenersatzansprüchen (z.B. Verrechnung mit Lohnansprüchen) einzuleiten, wobei insbesondere bei einer fristlosen Kündigung zu beachten ist, dass diese rechtlich korrekt erfolgt (Vorliegen eines wichtigen Grundes und umgehende Reaktion nach Kenntnis des wichtigen Grundes). Allenfalls kann es auch Sinn machen, das Arbeitsverhältnis mit einem fehlbaren Mitarbeitenden durch eine Aufhebungsvereinbarung einvernehmlich auszulösen.

Stefan Rieder
Dr. iur. HSG, LL.M., Rechtsanwalt
Telefon +41 58 258 14 00
stefan.rieder@bratschi-law.ch

4.2 Beachtung von Geschäftsgeheimnissen

4.2.1 Regelung von Geschäftsgeheimnissen

Bei internen Untersuchungen ist einerseits darauf zu achten, dass die Pflicht zur Geheimhaltung von Geschäftsgeheimnissen gegenüber Dritten nicht verletzt wird. Anderseits muss das Unternehmen bei Befragungen von Arbeitnehmenden im Rahmen einer internen Untersuchung darauf achten, dass sich diese nicht wegen Verstössen der Pflicht zur Wahrung von Geschäftsgeheimnissen strafbar machen. Der Schutz von Geschäftsgeheimnissen hat in der Schweiz lange Tradition, ist allerdings nur fragmentarisch geregelt. So ist beispielsweise das Verleiten zum Verrat oder zur Auskundschaftung von Fabrikations- oder Geschäftsgeheimnissen nach Bundesgesetz gegen den unlauteren Wettbewerb unter Strafe gestellt (Art. 4 lit.c und 6 i.V.m. Art. 23 Abs. 1 UWG). Nach Art. 162 StGB kann sich derjenige (oder das Unternehmen) strafbar machen, der ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät oder wer den Verrat für sich oder einen andern ausnutzt.

4.2.2 Begriff des Geschäftsgeheimnisses

Was unter einem Geschäftsgeheimnis (bzw. Fabrikationsgeheimnis) zu verstehen ist, ist nicht gesetzlich geregelt. Das Bundesgericht hat hierzu aber festgelegt, dass als Geheimnis alle Tatsachen gelten, die weder offenkundig noch allgemein zugänglich sind, wobei der Geheimnisherr an diesen Tatsachen ein berechtigtes Geheimhaltungsinteresse haben muss. Dem Kriterium der allgemeinen Zugänglichkeit kommt dabei zentrale Bedeutung zu. Eine Information ist dann nicht allgemein zugänglich, wenn sie nur einem abgegrenzten Personenkreis bekannt ist. Der Geheimnisherr muss zudem ein Interesse an der Geheimhaltung haben und die zu geheim haltende Tatsache muss auch objektiv schützenswert sein. Objektiv schützenswert ist die Tatsache, wenn sie einen wirtschaftlichen Wert für das Unternehmen hat, wobei mitunter die Relevanz für die Wettbewerbsfähigkeit ein Indikator sein soll.

4.2.3 Gesetzliche und vertragliche Pflicht zur Geheimhaltung

Eine Pflicht zur Geheimhaltung kann entweder vertraglich oder gesetzlich begründet sein. Insofern wird in der Regel beispielsweise mit potentiellen Investoren oder Partnern die Geheimhaltungspflicht durch vertragliche Regelungen in verschiedener Ausgestaltung (Non-Disclosure Agreements, Know-How Lizenzverträge u.a.) festgehalten. In gesetzlicher Hinsicht ist insbesondere die Pflicht des Auftragnehmers nach Art. 398 Abs.1 OR in Verbindung mit Art. 321e Abs.2 OR oder Art. 321a Abs.4 OR zu nennen, wonach der Auftragnehmer bzw. der Arbeitnehmer verpflichtet ist, Tatsachen geheim zu halten, von denen er im Dienst des Arbeitgebers/Auftraggebers Kenntnis erlangt hat. Auch nach Beendigung des Arbeits- oder Auftragsverhältnisses bleibt er zur Verschwiegenheit verpflichtet, soweit es zur Wahrung der berechtigten Interessen des Auftraggebers/Arbeitgebers erforderlich ist.

4.2.4 Schutz von Geschäftsgeheimnisses im Rahmen von internen Untersuchungen

Im Hinblick auf Geschäftsgeheimnisse ist es daher grundsätzlich ratsam sicher zu stellen, dass diese intern als solche identifiziert werden und der „Geheimnisberechtigte“ festgelegt wird. Der Personenkreis mit Zugang zu den identifizierten vertraulichen Daten sollte limitiert sein. Nur solche

Mitarbeiter sollten Zugang haben, die diesen tatsächlich benötigen. Hierfür sind geeignete Vorkehrungen zu schaffen. Im Rahmen einer internen Untersuchung sollten Ergebnisse, die Geschäftsgeheimnisse beinhalten, sondiert und möglichst nicht an Dritte weitergegeben werden. Für die Behandlung von Geschäftsgeheimnissen Dritter gelten die gleichen Massstäbe wie beim Bankgeheimnis (siehe Abschnitt 4.3). Hinsichtlich eines im Rahmen einer internen Untersuchung zu befragenden Arbeitnehmers ist abzuwägen, ob es im relevanten Untersuchungskontext notwendig ist, den Arbeitnehmer zu einem bestimmten Thema, das möglicherweise die Offenbarung eines Geschäftsgeheimnisses provoziert, zu befragen. Der Grundsatz „nemo tenetur“ gilt bei internen Untersuchungen prinzipiell nicht und aufgrund des Weisungsrechts des Arbeitgebers hat der Arbeitnehmer Stellung zu nehmen. Findet eine Entbindung von der Geheimhaltungspflicht intern statt, so ist es wichtig, darauf zu achten, dass die so erlangten Informationen nicht an Dritte gelangen (siehe auch Abschnitt 4.1).

Liv Bahner
LL.M., Maître en Droit, Rechtsanwältin
Telefon +41 58 258 10 00
liv.bahner@bratschi-law.ch

4.3 Beachtung des Bankgeheimnisses

Entgegen einer weit verbreiteten Auffassung ist das Bankgeheimnis, oder besser das Bankkundengeheimnis, noch nicht ganz tot. Art. 47 BankG stellt das Offenbaren von im Rahmen der Tätigkeit für eine Bank oder für eine Prüfgesellschaft erfahrenen Geheimnissen unter die Androhung einer Gefängnisstrafe oder Busse. Das Bankkundengeheimnis ist zwar im Zusammenhang mit steuerrechtlichen Fragen und dem automatischen Informationsaustausch aufgeweicht worden. Zudem wurde es durch die Möglichkeit, Daten auf CDs zu speichern und dann zu verkaufen, faktisch ausgehebelt. Trotzdem gilt die Strafnorm nach wie vor. Sie ist insbesondere bei internen Untersuchungen durch externe Berater zu beachten, damit zum untersuchten Straftatbestand nicht noch eine Verletzung des Bankkundengeheimnisses hinzutritt.

Insbesondere ist der Bestimmung bei der Planung, Durchführung und Resultatverwertung von derartigen Untersuchungen bei unter das Bankengesetz fallenden Finanzinstituten Rechnung zu tragen. Im Planungsstadium ist sicherzustellen, dass die Problematik für jede Phase im Auge behalten wird, indem die vorgesehenen Abläufe explizit auf die Vereinbarkeit mit dem Bankkundengeheimnis überprüft werden. Die Untersuchungsschritte sind mit dem Finanzinstitut abzusprechen und mit dessen Rechtsabteilung zu koordinieren. So müssen nicht alle Teammitglieder Zugang zu den Daten haben, sollen diese sicher aufbewahrt werden, muss die Anonymisierung der Daten geprüft werden und sind die Anforderungen der Gesetzgebung jederzeit einzuhalten. Die einzelnen Schritte der Untersuchung und deren Dokumentation sind abzusprechen und auf ihre Verträglichkeit mit dem Bankkundengeheimnis zu überprüfen.

Im Rahmen der Durchführung sind diverse Formalitäten zu beachten. So sollten alle externen Teammitglieder Erklärungen zur Geheimniswahrung unterzeichnen. Bei Wechseln im Team ist sicherzustellen, dass die neuen Mitglieder ebenfalls über die Geheimhaltungspflicht informiert werden und die entsprechende Erklärung unterzeichnen. Für den Verletzungsfall ist die Dokumentation über die Massnahmen zum Schutz des Bankkundengeheimnisses an einem geeigneten Ort aufzubewahren, damit sie auch Jahre später noch aufgefunden werden kann. Weiter sind Massnahmen zum Schutz der Daten zu implementieren. Diese werden teilweise auf gespiegelten Systemen zur Verfügung gestellt, damit der normale Betrieb des Instituts nicht gestört wird. Für die Untersuchung stellen die Institute meist eigene Räumlichkeiten mit eigenen Informatikmitteln zur Verfügung, damit keine Zugriffe von ausserhalb erfolgen müssen. Durch die Zuteilung von eigenen Passwörtern lassen sich die Zugriffe durch externe Mitarbeiter auch später nachvollziehen.

Suchresultate werden, soweit sie geschützte Informationen enthalten, am besten innerhalb des Instituts aufbewahrt, wobei der Zugang so zu regeln ist, dass weder externe Berater noch die Mitarbeiter des Instituts alleine Zugriff haben. Zudem darf das Resultat der Untersuchung nur einem begrenzten Kreis zugänglich gemacht werden. Berichte sind soweit möglich zu anonymisieren. Der Schlüssel zur Zuordnung der anonymisierten Identitäten ist besonders sicher am besten ebenfalls innerhalb des Instituts mit geregeltem Zugang aufzubewahren. Werden Daten im Schutzbereich des Bankkundengeheimnisses ausserhalb der Systeme des Finanzinstituts aufbewahrt oder bearbeitet, sind die Vorschriften des Outsourcing-Rundschreibens der FINMA einzuhalten, welches gegenwärtig überarbeitet wird (siehe https://www.finma.ch/de/news/2016/12/20161206---mm---rs---outsourcing/).

Je nach Verwendung der Daten in den Resultaten, z.B. bei Offenlegung von individualisierten Kundendaten gegenüber Dritten, kann sich die Einholung einer Verzichtserklärung betreffend das Bankkundengeheimnis der betroffenen Kunden aufdrängen. Diese ist in der Regel nicht einfach zu bekommen und meist mit einer Forderung des Kunden auf eine Gegenleistung verbunden (ausser sie erfolgt auf Druck ausländischer Behörden).

Florian S. Jörg
Dr. iur., MCJ, Rechtsanwalt, Partner
Co-Leiter Internationale Praxis
Telefon +41 58 258 10 00
florian.joerg@bratschi-law.ch

4.4 Beachtung des Datenschutzes

Im Rahmen einer internen Untersuchung müssen die datenschutzrechtlichen Bearbeitungsgrundsätze eingehalten werden, denn eine interne Untersuchung beinhaltet die Erhebung und Speicherung personenbezogener Daten im Sinne von Art. 3 lit. e DSG. Werden die Datenschutzbearbeitungsgrundsätze nicht eingehalten, liegt eine widerrechtliche Persönlichkeitsverletzung vor, sofern nicht nach Art. 13 DSG eine Einwilligung des Verletzten vorliegt oder die Persönlichkeitsverletzung durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

Eine heimliche Datenbearbeitung verstösst grundsätzlich gegen Treu und Glauben nach Art. 4 Abs. 2 DSG. Personen, über welche Daten bearbeitet werden, steht gemäss Art. 8 DSG ein datenschutzrechtliches Auskunftsrecht zu. Das Wissen um die Datenbearbeitung schafft die Voraussetzung für die Wahrnehmung der weiteren Rechte und Ansprüche der betroffenen Person. Bei internen Untersuchungen ist eine heimliche Datenbearbeitung aber oftmals nötig, um die Untersuchungsergebnisse aufgrund Verdunkelungsgefahr nicht zu gefährden. In der ersten Untersuchungsphase kann somit ein überwiegendes Interesse im Sinne von Art. 13 Abs. 1 DSG angenommen werden und das dem Verpfiffenen zustehende datenschutzrechtliche Auskunftsrecht durch Art. 9 Abs. 1 DSG eingeschränkt werden. Gemäss Art. 9 Abs. 3 DSG fällt die Einschränkung des Auskunftsrechts allerdings weg, sobald der Grund für die Verweigerung, Einschränkung oder Aufschiebung entfällt. Es muss den Betroffenen gemäss Art. 5 Abs. 2 DSG das Recht gewährt werden, unrichtige Daten berichtigen zu können.

Oft ist das von der internen Untersuchung betroffene Unternehmen je nach Untersuchungsausgang auch damit konfrontiert die erhobenen Daten an in- oder ausländische Strafverfolgungs- / Administrativmassnahmebehörden herausgeben zu müssen oder zu wollen, um Strafverfolgung zu vermeiden oder eine drohende Sanktion zu mildern. Die datenschutzrechtliche Zulässigkeit dieser Lieferungen war von Anfang an und ist auch heute noch strittig. Gleichwohl hat sich unter der Leitung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eine Praxis herausgebildet, die als etabliert betrachtet werden kann. Bratschi Wiederkehr & Buob hat in zahlreichen internen Untersuchungen Erfahrungen gesammelt wie diese und die weiteren Anforderungen des Datenschutzgesetzes effektiv und effizient umgesetzt werden.

Mirco Ceregato
lic. iur. HSG, LL.M., Rechtsanwalt
Co-Leiter Compliance und Investigations
Co-Leiter Prozessführung und Insolvenz
Telefon +41 58 258 10 00
mirco.ceregato@bratschi-law.ch

4.5 Beachtung von Art. 271 und Art. 273 StGB

Sobald eine interne Untersuchung auf Anlass einer ausländischen Behörde durchgeführt und/oder Ergebnisse einer solchen Untersuchung einer ausländischen Behörde mit dem Ziel erstellt werden sie einer ausländischen Behörde zur Verfügung zu stellen, gilt es Art. 271 StGB (Verbotene Handlungen für einen fremden Staat) und Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) zu beachten. Gemäss Art. 271 Ziff. 1 StGB macht sich strafbar, wer auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat Handlungen vornimmt, die einer Behörde oder einem Beamten zukommen, oder wer solchen Handlungen Vorschub leistet. Nach Art. 273 StGB macht sich strafbar, wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle zugänglich macht.

Betreffend Art. 271 StGB kann durch das zuständige (Bundes-)Departement bzw. die Bundeskanzlei eine Bewilligung zur Zusammenarbeit mit der ausländischen Behörde erteilt werden. Im US-Steuerstreit erteilte z.B. das Eidgenössische Finanzdepartement auf Gesuch hin die entsprechenden Bewilligungen. Unsere Kanzlei hat in diesem und in anderem Zusammenhang die notwendige Erfahrung für solche Gesuche.

Im Unterschied zu Art. 271 StGB kennt Art. 273 StGB kein Bewilligungsverfahren, sondern überlässt den Entscheid, ob das Geheimnis freigegeben werden soll und darf, dem Geheimnisherrn. Das Unternehmen, welches die interne Untersuchung als Geheimnisherrin durchführen lässt, kann auf das Geschäftsgeheimnis verzichten. Der Verzicht der Geheimnisherrin führt indessen nicht per se zur Nichtanwendbarkeit von Art. 273 StGB. Denn Art. 273 StGB bezweckt nicht (nur) den Schutz der Geheimnisherrin, sondern auch den Schutz der gesamtwirtschaftlichen (öffentlichen) Interessen der Schweiz. Liegt ein solches vor oder sind Geschäftsgeheimnisse eines Dritten betroffen, ist die Kooperation mit einer ausländischen Behörde illegal. Der Vollständigkeit halber sei erwähnt, dass die schweizerischen Strafverfolgungsbehörden nur aktiv werden dürfen, wenn ihnen der Bundesrat oder das Eidgenössische Finanzdepartement eine entsprechende Ermächtigung erteilen (Art. 3 lit. a OV-EJPD i.V.m. Art. 66 Abs. 1 StBOG).

Mirco Ceregato
lic. iur. HSG, LL.M., Rechtsanwalt
Co-Leiter Compliance und Investigations
Co-Leiter Prozessführung und Insolvenz
Telefon +41 58 258 10 00
mirco.ceregato@bratschi-law.ch

5. Fazit

«Gouverner, c'est prévoir» sagte der französische Verleger und Politiker Emile de Girardin bereits im 19. Jahrhundert. Und gerade heute im 21. Jahrhundert hat dieser Satz insbesondere auch für Verwaltungsräte und Geschäftsleitungen nicht das Geringste an seiner Aktualität und auch Richtigkeit eingebüsst.

Mit den aus verschiedenen Rechtsbereichen oben aufgeführten und ausgewählten Szenarien und Ansätzen haben wir versucht aufzuzeigen, mit welchen möglichen Risiken oder Konstellationen zu rechnen ist, wann es sinnvoll sein könnte, eine interne Untersuchung durchzuführen und wie Sie als Verwaltungsrat oder Geschäftsleitung gezielt sowie vorausschauend vorgehen können. Es ist wichtig zu wissen, was es zu berücksichtigen gilt, um das wichtigste Gut Ihres Unternehmens, seine Reputation, zu schützen und den nachhaltigen Erfolg sicherzustellen.

Basel
Lange Gasse 15
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi-law.ch

Bern
Bollwerk 15
Postfach 5576
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi-law.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi-law.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi-law.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi-law.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi-law.ch