Sonderuntersuchungsbericht: Compliance-Fragestellungen im Zusammenhang mit Aktivitäten der ehemaligen Abteilung Konzernsicherheit

Februar 2010

Inhaltsverzeichnis

I. Ausgangssituation

Anlass der Untersuchung war das Ermittlungsverfahren der Staatsanwaltschaft Bonn im Rahmen der sog. „Bespitzelungsaffäre."

Diesem Ermittlungsverfahren liegt zugrunde, dass Beschäftigte des ehemaligen Bereichs „KS3" der Abteilung Konzernsicherheit (im Folgenden „KS3" genannt) der Deutschen Telekom AG (im Folgenden „DTAG" genannt) in den Jahren 2005 und 2006 zur Aufklärung vermuteter Indiskretionen gegenüber der Presse Telefonverbindungsdaten von Arbeitnehmervertretern aus dem Aufsichtsrat der DTAG, Betriebsratsmitgliedern, Journalisten und anderen Personen unter Verstoß gegen das Fernmeldegeheimnis sowie datenschutzrechtliche Bestimmungen erhoben und ausgewertet haben.

Im Zuge dieses Ermittlungsverfahrens hat die Staatsanwaltschaft Ende Mai 2008 mit voller Kooperation der DTAG das gesamte Archiv des Bereichs „KS3", in dem Akten zu abgeschlossenen internen Ermittlungsvorgängen abgelegt waren, sowie Unterlagen aus Büroräumen von Mitarbeitern des Bereichs „KS3" sichergestellt.

Die DTAG hat von der Staatsanwaltschaft Bonn im Juli 2009 im Wege der Teilakteneinsicht eine DVD erhalten, die elektronische Kopien der im Archiv der „KS3" sichergestellten Aktenstücke enthält. Auf der DVD befinden sich 254 Dokumente im Format pdf mit insgesamt 92.118 Seiten und ca. 6,15 GB Umfang. Darüber hinaus wurden der DTAG noch ca. 50 Aktenordner, Sammelmappen sowie diverse gebundene Unterlagen aus dem Büro eines Mitarbeiters der Konzernsicherheit zur Einsichtnahme zur Verfügung gestellt.

Diese Dokumente (im Folgenden „Asservate" genannt) stehen nach dem Ergebnis der bereits durch die Staatsanwaltschaft vorgenommenen Prüfung und Auswertung mit den Bespitzelungsvorwürfen in keinem sachlichen Zusammenhang und haben daher auch keinen Eingang in die staatsanwaltschaftlichen Ermittlungsakten des „Bespitzelungsverfahrens" gefunden, in die DTAG bislang noch keine Akteneinsicht erhalten hat.

Unabhängig von der unter strafrechtlichen Gesichtspunkten erfolgten Auswertung der Asservate durch die Staatsanwaltschaft hat DTAG das Projekt „Open Book" durchgeführt.

Ziel des Projektes war zum einen die Untersuchung der Asservate auf bereits bekannte Compliance-Verstöße, zum anderen die Identifikation und Aufbereitung möglicher weiterer in der Vergangenheit begangener und bislang unbekannt gebliebener Compliance-Verstöße, die nach Auffassung der Staatsanwaltschaft entweder strafrechtlich nicht relevant oder wegen eingetretener Verjährung nicht mehr verfolgbar sind.

Des Weiteren sollten festgestellte Sachverhalte in Bezug auf deren mögliche Auswirkungen sowie einen für DTAG ggf. daraus resultierenden Handlungsbedarf hin beurteilt werden.

Die Untersuchung hat Vorgänge aus dem Zeitraum von 1998 bis 2007 aufgearbeitet.

II. Durchführung der Untersuchung

Die nachfolgenden Ausführungen stellen das im Rahmen der Untersuchung gewählte Vorgehen dar.

1 Projektorganisation

Zur Projektsteuerung und -überwachung wurde ein Steering Committee eingerichtet, in dem Mitglieder des Vorstands von DTAG (Ressorts: VS Datenschutz, Recht und Compliance,VS Personal, VS Südosteuropa) sowie verschiedene Zentralbereichsvertreter, darunter die Leiter Group Compliance Management (GCM), Group Business Security (GBS), Group Internal Audit (GIA), Corporate Communication (Com) und der Konzerndatenschutzbeauftragte von DTAG vertreten waren.

Im Rahmen der Sitzungen des Steering Committees wurden Vorgehensweisen und Zwischenergebnisse sowie wesentliche Einzelsachverhalte, deren Beurteilung und durch DTAG zu ergreifende Maßnahmen erörtert und beschlossen.

Das Steering Committee Open Book kam im Verlauf des Projektes zu vier Sitzungen zusammen.

Die konstituierende Sitzung fand am 11.08.2009, die Abschlussbesprechung am 08.12.2009 statt.

2 Beauftragung KPMG

Wegen der Vielzahl der im Rahmen des Projekts zu untersuchenden Asservate wurde die KPMG AG Wirtschaftsprüfungsgesellschaft sowie die KPMG Rechtsanwaltsgesellschaft mbH (im Folgenden gesamthaft „KPMG“ benannt) von DTAG mit der Analyse der Asservate und der Bewertung der dort vorgefundenen Sachverhalte beauftragt.

Mit diesem Vorgehen verfolgte DTAG das Ziel, eine hohe Sachkunde sowie ein Höchstmaß an Objektivität in der Analyse und Bewertung der Asservate zu gewährleisten.

3 Methodisches Vorgehen bei Dokumentensichtung und Sachverhaltsbewertung

Die Untersuchung und Analyse der Asservate durch KPMG erfolgte überwiegend digitalisiert unter Nutzung der e-discovery Software „Clearwell“. Durch den Einsatz einer e-discovery Software war eine effiziente und systematische Analyse der bereitgestellten großen Datenmenge möglich.

Mit Hilfe von Texterkennungs- sowie besonderen Analyse- und Ordnungsfunktionalitäten konnten die digitalen Dokumente gezielt in mehrstufigen Suchläufen unter anderem nach durch DTAG bereitgestellten, vordefinierten Suchbegriffen durchsucht werden.

Mehrere Mitglieder des Steering Committees haben sich im Projektverlauf bei KPMG in Köln von der Vorgehensweise und Funktionsfähigkeit der Suchsystematik überzeugt. Auch der Konzerndatenschutzbeauftragte von DTAG hat sich in den Projekträumlichkeiten über die getroffenen Vorkehrungen sowie die Vorgehensweise der Untersuchung informiert.

3.1 Kriterien für Relevanzbewertung und Kategorisierung identifizierter Sachverhalte

3.1.1 Relevanzbewertung identifizierter Sachverhalte

Die Kriterien zur Beurteilung der Projektrelevanz ergaben sich unmittelbar aus der Zielsetzung des Projektes, nämlich der Identifikation und Aufbereitung von möglichen Compliance-Verstößen bei der Durchführung von Untersuchungen durch die Konzersicherheit in der Vergangenheit.

Im Vordergrund standen Rechtsverstöße (insbesondere gegen Datenschutz, Strafrecht, Arbeitsrecht und Telekommunikationsgesetz), aber auch sonstige Compliance-Verstöße, darunter z. B. offenkundig unethisches Verhalten.

Unter Praktikabilitäts- und Effizienzgesichtspunkten wurden identifizierte Sachverhalte für die weitere Bewertung und Ergebnisdarstellung den nachfolgenden, typisierten Fallmustern zugeordnet, die letztlich auch die Relevanzkriterien widerspiegeln:

- Mögliche Verstöße gegen das TKG (Telekommunikationsgesetz) bei Ermittlungen gegen externe Personen (z. B. Verbindungsdatenauswertungen) – TKG extern;
- mögliche Verstöße gegen das TKG bei Ermittlungen gegen Mitarbeiter von DTAG (z. B. durch Auswertung Kommunikationsdaten) – TKG intern;
- Personal Screenings, d. h. die Sammlung und Verdichtung von Hintergrundinformationen zu einer Person (geschäftliche oder private Aktivitäten, familiäre Verhältnisse etc.);
- Financial Screenings, d. h. die Erhebung von Finanzinformationen zu Personen oder Unternehmen (Kontobewegungsdaten, Steuerdaten etc.), ggf. im Rahmen eines umfassenden Personal-Screenings;
- Durchsuchungen und Observationen (Durchsuchungen von Arbeitsplätzen, Observationen im privaten und geschäftlichen Umfeld etc.);
- sonstige Sachverhalte (z. B. Führung von Informationsbeschaffungsgesprächen unter Vorspiegelung falscher Tatsachen).

Soweit Sachverhalte Aspekte mehrerer der oben genannten Fallmuster beinhalteten, wurden sie dem in der Gesamtwürdigung vorrangigen Fallmuster zugeordnet.

Zum besseren Verständnis der definierten Falltypen sind im Folgenden generische Beschreibungen sowie Beispiele entsprechender Sachverhalte dargestellt:

Sachverhalte des Fallmusters TKG extern, d. h. mit Ermittlungen gegen Externe, betrafen unter anderem die retrograde Auswertung von Verbindungsdaten von Telefonanschlüssen (Festnetz und Mobiltelefone) durch die Konzernsicherheit.

Beispiele:

- Ein Kunde meldete bei DTAG eine Störung. Die Störungsmeldung wurde nicht ordnungsgemäß in das System von DTAG zur Aufnahme von Störungsmeldungen aufgenommen. Ein unbekannter Servicetechniker mit DTAG-Ausweis meldete sich bei dem Kunden und stellte ihm EUR 150 in Rechnung, ohne die Störung zu beheben. Von der Konzernsicherheit wurden die Verbindungsdaten des Kunden ausgewertet, um zu prüfen, ob dieser die Störungsstelle angerufen hatte. Außerdem wurden dem Kunden Bilder in Frage kommender Mitarbeiter von DTAG zur Identifizierung vorgelegt.

- In einem T-Punkt bestand der Verdacht, dass drei Mobiltelefone gestohlen wurden. Ein mit einem vermissten Telefon baugleiches Gerät fiel bei einer beschäftigten Zeitarbeiterin auf. Im Rahmen der Ermittlungen wurden die IMEI-Nummern der fehlenden Geräte auf eine Einbuchung im Mobilfunknetz überprüft. Es wurde festgestellt, dass eines der fehlenden Geräte auf die betroffene Zeitarbeiterin eingebucht gewesen war. Ihr wurde in der Folge Hausverbot erteilt. Ferner wurde ihr über die Zeitarbeitsfirma gekündigt.

Sachverhalte des Fallmusters TKG intern, d. h. mit Ermittlungen gegen Mitarbeiter von DTAG oder Beteiligungen von DTAG, waren unter anderem im Hinblick auf die retrograde Auswertung der Verbindungsdaten dienstlicher Telefonanschlüsse von Mitarbeitern sowie die Überwachung laufenden E-Mail-Verkehrs erkennbar. Da in der DTAG die private Internet- und E-Mail-Nutzung den Mitarbeitern über dienstlich zur Verfügung gestellte Infrastruktur nicht erlaubt ist, womit ein Verstoß gegen das TKG ausschied, erfolgte deren Kategorisierung aufgrund ethischen Fehlverhaltens oder hohen Reputationsrisikos (vgl. 3.1.2 Kategorisierung).

Beispiel:

- Ein ehemaliger Mitarbeiter eines Konzernunternehmens von DTAG führte ein eigenes Unternehmen, das mit DTAG in vertraglicher Beziehung stand. Gegen diesen Mitarbeiter wurde seitens DTAG Strafanzeige wegen Betruges erstattet, weil Rechnungen von DTAG an sein Unternehmen nicht beglichen wurden. Im Rahmen der Ermittlungen wurden laut einem Vermerk der Konzernsicherheit die Einzelverbindungsnachweise des Betroffenen überprüft, um Personen bei DTAG zu identifizieren, die mit dem Fall in Verbindung stehen. Weiterhin wurde eine Bonitätsprüfung des Betroffenen über externe Dienstleister durchgeführt. In einem weiteren Vermerk der Konzernsicherheit wurde außerdem geschildert, dass ein telefonischer Kontakt zwischen dem Betroffenen und einer Mitarbeiterin des

Konzernunternehmens von DTAG mittels eines internen Überwachungssystems festgestellt worden ist. Das Ermittlungsverfahren gegen den Betroffenen ist von der Staatsanwaltschaft wegen nicht hinreichenden Tatverdachts eingestellt worden.

Sachverhalte mit sog. Personal Screenings betrafen die Recherche und Zusammenstellung umfangreicher Hintergrundinformationen zu Personen (beispielsweise zu Werdegang, Lebensverhältnissen, Vorstrafen). Die genaue Quelle der Informationen ist bei diesen Screenings in der Regel nicht angegeben. Nach der Art der Informationen kann aber nicht ausgeschlossen werden, dass diese teilweise aus nicht offen zugänglichen Quellen gewonnen worden sind. Recherchiert wurde dabei sowohl über Dritte als auch über Mitarbeiter von DTAG bzw. von Beteiligungen von DTAG.

Beispiel:

- Es bestand ein Korruptionsverdacht gegen einen ehemaligen Mitarbeiter eines Konzernunternehmens von DTAG. Dieser wurde von seinem Nachfolger beschuldigt, vor seinem Ausscheiden bei DTAG im Gegenzug für den Abschluss eines mehrjährigen Vertrages mit einem Dienstleistungsunternehmen ein Kraftfahrzeug vom Inhaber dieses Unternehmens erhalten zu haben. Neben einer Befragung dieses Nachfolgers führte die Konzernsicherheit Ermittlungen am Wohnort des ehemaligen Mitarbeiters durch. In den Unterlagen befinden sich Fotos von seinem Wohnhaus, einem Grundstück sowie von zwei Kraftfahrzeugen. Es kann nicht ausgeschlossen werden, dass die Fotos von Mitarbeitern der Konzernsicherheit aufgenommen wurden, da sich eine entsprechende Position in einer Aufstellung des Ermittlungsaufwandes der Konzernsicherheit findet. Die Konzernsicherheit hat sich mittels eines Faxschreibens bei einer Polizeidienststelle nach den Halterdaten eines vor dem Haus des ehemaligen Mitarbeiters stehenden Kraftfahrzeuges erkundigt. Laut einem Vermerk hat die Konzernsicherheit diese Halterdaten telefonisch von der Polizei erhalten. In dem Vermerk wird ausgeführt, dass die Halterdaten überlassen wurden, obwohl noch keine Strafanzeige erstattet worden sei. Aus den Akten geht nicht hervor, ob der Korruptionsverdacht bestätigt wurde.

- In einem Einzelfall ließ die Konzersicherheit durch einen externen Dienstleister ein Personal Screening über einen Arbeitnehmervertreter im Aufsichtsrat einer ausländischen Tochtergesellschaft der DTAG erstellen. In den Unterlagen finden sich Informationen zum Lebenslauf, über Immobilienbesitz und Kontobewegungen sowie das Arbeitsverhältnis der Tochter.

  Die betroffene Person ist bereits durch die DTAG über das Personal Screening informiert worden.

Sachverhalte mit sog. Financial Screenings betrafen die Recherche und Zusammenstellung von Informationen über die Vermögensverhältnisse von Personen (z. B. Einkommen, Grundbesitz, Kontostände und -bewegungen), enthielten teilweise aber auch Komponenten sog. Personal Screenings. Die Informationsquellen wurden in diesen Berichten in der Regel nicht offengelegt. Nach der Art der Informationen ist anzunehmen, dass diese aus nicht offen zugänglichen Quellen stammen. Entspre-

chende Ermittlungen richteten sich sowohl gegen Dritte als auch gegen Mitarbeiter von DTAG oder von Beteiligungen von DTAG.

Beispiel:

- Die Konzernsicherheit ermittelte wegen eines Anfangsverdachts auf Vorteilsgewährung und Korruption gegen einen Mitarbeiter eines Konzernunternehmens von DTAG. Der Mitarbeiter wurde beschuldigt, Marketingaufträge an externe Unternehmen vergeben zu haben, die mangelhafte Arbeiten lieferten. Die Konzernsicherheit forderte Personaldaten an. In den Unterlagen befindet sich ein Dokument unbekannter Herkunft u. a. mit folgenden Angaben: Geburtsdatum, Adresse, Telefonnummer sowie Kontoverbindungsdaten des betroffenen Mitarbeiters, außerdem die Dokumentation von Bewegungen auf dem Privatkonto mit Datum, Betrag und Beschreibung.

Sachverhalte des Typs „Arbeitsplatzdurchsuchungen und Observationen“ betrafen unter anderem die Observation von Personen im Kontext möglicher Korruptionsfälle, aber auch mit dem Ziel der Aufdeckung arbeitsrechtlicher Verfehlungen (z. B. des Verdachts auf eine Nebentätigkeit, obwohl ein Mitarbeiter krankgeschrieben war). Betroffene waren neben Dritten auch Mitarbeiter von DTAG sowie von Beteiligungen von DTAG.

Beispiel:

- Wegen des Verdachts, ein Mitarbeiter von DTAG gehe einer nicht angemeldeten Nebentätigkeit nach, erteilte die Konzernsicherheit einer Detektei den Auftrag zur Observation des Mitarbeiters während dessen angeblich krankheitsbedingter Abwesenheit. In den Unterlagen finden sich Fotos des Mitarbeiters und der Außenansicht seines Wohnhauses. Des Weiteren geht aus einem Bericht hervor, dass eine Fahrzeugzulassung und eine Mobilfunknummer des Mitarbeiters ermittelt wurden. Der Mitarbeiter wurde fünf Tage lang observiert. Während dieser Zeit trafen sich Ermittler der Detektei mit ihm und gaben vor, an von ihm vermieteten Wohnungen interessiert zu sein. Auch befragten sie Personen im Umfeld seines Miethauses. Außerdem wurde ein akribisches Bewegungsprofil über ihn erstellt. Es kann nicht ausgeschlossen werden, dass es sich bei einem entsprechenden Bericht in den Unterlagen um einen Bericht der beauftragten Detektei handelt. Ausweislich dieses Berichtes konnte der Anfangsverdacht nicht bestätigt werden.

Sachverhalte des Typs „Sonstige bedenkliche Sachverhalte“ betrafen beispielsweise die Recherche einzelner geschützter Daten (z. B. Fahrzeughalterdaten), die auf Grundlage der Unterlagen nicht im Zusammenhang mit einem Personal- oder Financial Screening standen. Umfangreiche Screenings zu Unternehmen (Company Screenings), welche nicht eindeutig als Personal oder Financial Screening eingeordnet werden konnten, wurden ebenfalls unter diesen Falltyp gefasst.

Beispiele:

- Die Konzernsicherheit wurde anlässlich einer Geschäftsanbahnung mit einer Hintergrundrecherche zu einem britischen Unternehmen beauftragt. Die Konzernsicherheit beauftragte einen externen Dienstleister. In den Unterlagen findet sich u.

a. ein Kontoauszug eines englischen Kontos des Unternehmens. Es ist aus den Unterlagen nicht ersichtlich, wie dieser Kontoauszug in den Besitz von DTAG gelangt ist.

- Die Konzernsicherheit nahm Ermittlungen im Zusammenhang mit einem Verdacht auf Manipulation öffentlicher Telefonzellen auf. In einem anonymen Schreiben über Beobachtungen wiederholter Telefonate in einer öffentlichen Telefonzelle ohne Telefonkarte teilte der Verfasser einen konkreten Beobachtungszeitpunkt und das Kennzeichen eines Kraftfahrzeugs mit, das von einer verdächtigen Person genutzt wurde. Einem Ermittlungsbericht der Konzernsicherheit ist zu entnehmen, dass Fahrzeughalterdaten sowie Verbindungsdaten ermittelt wurden. Die Ermittlungen wurden eingestellt, weil aus den Verbindungsdaten hervorging, dass nur Anrufe an kostenfreie 0800-Nummern erfolgten, für die keine Telefonkarten benötigt wurden.

Der Anlass und der Auftraggeber für Untersuchungshandlungen der Konzernsicherheit konnte nicht in allen Fällen eindeutig erkannt werden. Allerdings konnte häufig ein Bezug zu Maßnahmen der Betrugs-, Korruptions- und/oder Missbrauchsbekämpfung erkannt werden.

3.1.2 Kategorisierung relevanter Sachverhalte

Mit Blick auf eine effiziente Bewertung festgestellter Sachverhalte und entsprechender Maßnahmengestaltung wurde vom Steering Committee von DTAG ein System zur vorläufigen Kategorisierung der Sachverhalte beschlossen. Auf Basis noch zu erläuternder Kriterien wurden potenzielle Sachverhalte aus der Sichtungsphase in die vier folgenden Kategorien eingeordnet:

- A – kritischer Sachverhalt;
- B – weniger kritischer Sachverhalt;
- Y – unvollständige Sachverhaltsdokumentation, Fallbewertung nicht zuverlässig/nicht abschließend möglich;
- Z – mit überwiegender Wahrscheinlichkeit oder offensichtlich unkritischer Sachverhalt.

Die Kategorisierung basierte dabei auf folgenden Kriterien:

- erkennbarer Rechtsverstoß;
- schwerwiegendes ethisches Fehlverhalten;
- hohes Reputationsrisiko.

Sachverhalte, bei denen mindestens zwei dieser Kriterien zutrafen, waren der Kategorie A zuzuordnen. Soweit bei einem Sachverhalt nur eines dieser Kriterien zutraf, war dieser der Kategorie B zuzuordnen.

Zusätzlich haben „schwere Rechtsverstöße“ zur Einordnung in Kategorie A geführt. Als schwerer Rechtsverstoß werden Rechtsverletzungen behandelt, die – unabhängig von der Verfolgbarkeit (etwa Unverjährtheit) – materielles Strafrecht verletzen.

Darunter fallen u. a. Verstöße gegen das Post- oder Fernmeldegeheimnis oder die Verletzung des Steuergeheimnisses.

Aufgrund des starken Bezugs der Bewertungskriterien zu rechtlichen Vorschriften erfolgte die Vorkategorisierung der Sachverhalte durch KPMG Rechtsanwaltsgesellschaft. Insbesondere wegen der teilweise lückenhaften Dokumentation in den Asservaten war eine abschließende rechtliche Bewertung der Sachverhalte in weiten Teilen jedoch nicht möglich.

3.1.3 Sachverhaltsstatistik

Im Ergebnis wurden insgesamt 84 kritische Sachverhalte der Kategorie A identifiziert, von denen 3/4 auf den Zeitraum von 2001 bis 2005 entfallen.

Von den 84 Sachverhalten entfallen 55 auf Deutschland, 19 auf Osteuropa und 10 auf sonstige Länder.

Eine Aufteilung auf die Fallmuster (Definition siehe 3.1.1) zeigt folgendes Ergebnis: Personal Screening 38, Financial Screening 22, TKG – Verletzungen bei Konzernexternen 17, TKG – Verletzungen bei Konzerninternen 3, Arbeitsplatzdurchsuchungen und Observationen 1, sonstige Sachverhalte 3.

22 Fälle wurden der Kategorie B zugeordnet.

Hierfür ein Beispiel: Ein Mitarbeiter eines externen Dienstleisters hat sich unter wahrheitswidriger Vorspiegelung, bei eine Headhunter beschäftigt zu sein, in einem persönlichen Gespräch mit einem Betroffenen personenbezogene Informationen über diesen erschlichen.

3.2 Maßnahmen

Die 84 Sachverhalte der Kategorie A wurden im Detail im Steering Committee von DTAG diskutiert und es wurden seitens der DTAG entsprechende auf den Einzelfall abgestimmte Maßnahmen beschlossen.

Ausgehend von einem Katalog möglicher Maßnahmen (vgl. 3.2.1) hat das Steering Committee zum Zwecke der Entscheidungskonsistenz eine Entscheidungssystematik (vgl. 3.2.2) entwickelt und auf dieser Basis über Maßnahmen hinsichtlich der Sachverhalte entschieden.

Aufgrund bereits vorab bekannt gewordener Sachverhalte („Bespitzelungsaffäre“) hat die DTAG die Konzernsicherheit grundlegend umorganisiert und personelle Maßnahmen ergriffen. Gegen die verantwortlichen Führungskräfte wird in diesem Zusammenhang strafrechtlich ermittelt. Gegen zwei Beamte wird ein Disziplinarverfahren geführt, in das die hier ermittelten Sachverhalte ggfs. einfließen werden. Soweit die belasteten Personen die DTAG nicht zwischenzeitlich verlassen haben, sind sie nicht mehr in der Konzernsicherheit tätig.

3.2.1 Maßnahmenkatalog

Grundlage der Entscheidung war ein „Katalog“ möglicher Handlungsoptionen und Maßnahmen, die sich sowohl auf Betroffene (z. B. Zielpersonen eines Screenings) als auch auf sonstige Beteiligte (z. B. handelnde Ermittler) beziehen:

- Betroffeneninformation;
- Sensibilisierungsmaßnahmen (individuell oder abteilungsbezogen);
- ergänzende Prüfung etwaiger dienst- und arbeitsrechtlicher Schritte;
- erneute Vorlage an die Staatsanwaltschaft.

Die Information der betroffenen Person ist datenschutzrechtlich determiniert.

Sensibilisierungsmaßnahmen kommen u. a. als Gespräche mit seinerzeit handelnden Personen oder Schulungen von Mitarbeitern (z. B. zum Datenschutz) in Betracht, die auch durch strukturelle Änderungen oder Neuaufsatz von Prozessen realisiert bzw. unterstützt werden können.

3.2.2 Entscheidungssystematik bei Maßnahmen

Das Steering Committee von DTAG hat für die Sachverhalte der Kategorie A erörtert, welche der vorgenannten Maßnahmen im Einzelfall zu ergreifen sind. Ausgangslage der Entscheidung des Steering Committee waren in der Regel Maßnahmenvorschläge, die auf der Ebene der Projektteams von DTAG und KPMG gemeinsam entwickelt worden sind (vgl. obenstehende Erläuterungen).

Die Entscheidung über zu ergreifende Maßnahmen hat das Steering Committee vor dem Hintergrund folgender Kriterien getroffen:

- Die **Betroffenen** wurden und werden im Einklang mit den datenschutzrechtlichen Bestimmungen umfassend informiert. Mit Stand 09.02.2010 sind rund zwei Drittel der ca. 50 identifizierbaren Betroffenen benachrichtigt. Dabei hat sich die DTAG für die Vorfälle entschuldigt.

- Das Steering Committee hat nahezu durchgängig in Fällen der Kategorie A beschlossen, dass **Sensibilisierungsmaßnahmen** ergriffen werden, um entsprechende Fälle für die Zukunft zu vermeiden.

  Unabhängig von der Ergreifung einzelner Maßnahmen der Sensibilisierung wurde der Bereich der Konzernsicherheit (inzwischen in GBS -Group Business Security- umbenannt) zwischenzeitlich organisatorisch und personell umstrukturiert. Dies umfasst u. a. die organisatorisch klare Abgrenzung der Bereiche Missbrauchserkennung, Betrugsbekämpfung und Prävention sowie deren Überwachung durch ein zentrales Auftragsmanagement im Sinne eines Vier-Augen-Prinzips. Auch wurde der Prozess zur Beauftragung externer Ermittlungs-Dienstleistungen für den Bereich GBS dahingehend definiert, dass solche Beauftragungen unter Wahrung eines Vier-Augen-Prinzips (u. a. unter Einbindung des

Leiters Wirtschaftsstrafrecht) über den Einkauf von DTAG erfolgen muss, wobei bestimmte in der Vergangenheit auffällig gewordene Dienstleister grundsätzlich von einer Beauftragung ausgeschlossen sind.

Nachfolgend wird am Beispiel eines anonymisierten Sachverhalts der Kategorie A dargestellt, welche Maßnahmen durch das Steering Committee beschlossen wurden:

Bei einem namentlich nicht bekannten Dienstleister gab die Konzernsicherheit von DTAG ein Personal Screening eines neuen Mitarbeiters einer in Ungarn ansässigen Mehrheitsbeteiligung von DTAG in Auftrag. Der Ermittlungsbericht des externen Dienstleisters enthält personenbezogene Daten der betroffenen Person, wie beispielsweise die polizeilich gemeldete Anschrift oder die Anzahl ihrer Kinder. Des Weiteren wurden ausweislich des Ermittlungsberichts des Dienstleisters ehemalige Kollegen und Freunde zum Privat- und Berufsleben des Betroffenen befragt. In dem Bericht werden beispielsweise Aussagen zur Stabilität seiner Ehe oder zu seinen Reisepräferenzen gemacht.

Als Maßnahme wurde zunächst beschlossen, den Betroffenen über das zu seiner Person durchgeführte Personal Screening sowie dessen Ergebnisse zu informieren. Ferner wurde in diesem Kontext beschlossen, dass sich Vertreter von DTAG zur Vorbereitung der Betroffeneninformation mit der Sachverhaltsdokumentation eingehend beschäftigen werden. Abschließend wurden unter anderem vor dem Hintergrund der Aussagen zur Stabilität der Ehe des Betroffenen Sensibilisierungsmaßnahmen auf Abteilungsebene der GBS (vormals Konzernsicherheit) beschlossen, um im Hinblick auf künftige Ermittlungen der Konzernsicherheit bzw. der GBS die Erhebung solcher Informationen ausschließen zu können.

III. Zusammenfassung und wesentliche Untersuchungsergebnisse

Im Zuge der sogenannten „Bespitzelungsaffäre“ hat die Staatsanwaltschaft Ende Mai 2008 umfangreiche Unterlagen der ehemaligen Abteilung Konzernsicherheit der DTAG sichergestellt.

Nachdem die DTAG im Juli 2009 von der Staatsanwaltschaft Bonn Einsicht in diese Unterlagen erhalten hatte, wurden diese mit Unterstützung von KPMG intern umfassend ausgewertet.

Als Ergebnis einer mehrstufigen, IT-unterstützten Untersuchung der digitalisierten Unterlagen wurden sechs Grundtypen relevanter Sachverhalte identifiziert. Es handelt sich dabei im Wesentlichen um mögliche Verstöße gegen das TKG bei Ermittlungen gegen Externe und gegen Mitarbeiter von DTAG, Personal Screenings, Financial Screenings sowie um sonstige als kritisch erachtete Maßnahmen, wie Observationen und Durchsuchungen.

Der Anlass und der Auftraggeber für Untersuchungshandlungen der Konzernsicherheit konnte nicht in allen Fällen eindeutig erkannt werden. Allerdings konnte häufig

ein Bezug zu Maßnahmen der Betrugs-, Korruptions- und/oder Missbrauchsbekämpfung erkannt werden.

Die Vorgänge, bei denen nach dem Ergebnis der Untersuchung von einem Compliance-Verstoß auszugehen ist, sind weder qualitativ noch quantitativ mit der sogenannten „Bespitzelungsaffäre“ vergleichbar. Dort wurde das Kommunikationsverhalten von Betroffenen alleine aufgrund ihrer Zugehörigkeit zu einer bestimmten Personengruppe, wie Arbeitnehmervertreter im Aufsichtsrat und in Betriebsräten sowie Medienvertreter, und aufgrund eines Generalverdachts systematisch ausgeforscht.

Alle projektrelevanten Sachverhalte wurden nach einem von dem Steering Committee von DTAG beschlossenen Schema kategorisiert. Es wurden kritische („A“), weniger kritische („B“), unvollständige („Y“) und eher unkritische Sachverhalte („Z“) identifiziert. Dieser Kategorisierung lagen neben möglichen (straf-) rechtlichen Erwägungen vor allen Dingen auch ethische und reputationsorientierte Erwägungen zu Grunde.

Anhand der Kategorisierung wurden insgesamt 84 kritische Sachverhalte identifiziert, von denen 3/4 auf den Zeitraum von 2001 bis 2005 entfallen.

Das Steering Committee von DTAG hat beschlossen, mit unterschiedlichen Maßnahmen auf die kritischen Sachverhalte zu reagieren. Beschlossen wurde, ggfs. weitere Sachverhaltsaufklärung zu betreiben, unter bestimmten Bedingungen die Betroffenen zu informieren und involvierte Mitarbeiter durch geeignete Maßnahmen zu sensibilisieren. Weitere Schritte (Schadensersatzforderungen, arbeitsrechtliche Schritte, Strafanzeigen etc.) stehen unter dem Vorbehalt einer weiteren rechtlichen Prüfung seitens DTAG.

Darüber hinaus wurden im Bereich GBS bereits in der Vergangenheit personelle und strukturelle Maßnahmen eingeleitet, die neben Belangen des Datenschutzes (u. a. datenschutzrechtliche Schulungen von Mitarbeitern, Implementierung datenschutzrechtlicher Vorgaben in Prozessen) die Überwachung der Ermittlungsaktivitäten im Sinne eines Vier-Augen-Prinzips durch ein zentrales Fallmanagement sowie die Implementierung eines Prozesses zur Beauftragung externer Dienstleister über den Einkauf von DTAG, bei dem im Sinne eines Mehraugen-Prinzips zwingend weitere Stellen (u. a. der Leiter Wirtschaftsstrafrecht) involviert werden müssen, umfassen.

Aus den vorliegenden Unterlagen ergeben sich für DTAG keine Hinweise darauf, dass im Zusammenhang mit den Aktivitäten der ehemaligen Konzernsicherheit von DTAG weitere relevante Sachverhalte der Kategorie A existieren.

Entsprechend der Darstellung im Abschlussbericht der KPMG zu diesem Projekt erscheinen auch KPMG die von DTAG im Rahmen des Projekts eingeleiteten Untersuchungen (auf Basis der Durchsicht der Asservate und der sonstigen von DTAG übergebenen Unterlagen und Dokumentation) sowie die bereits umgesetzten Veränderungen im organisatorischen Ablauf grundsätzlich geeignet, die Durchführung rechtlich oder ethisch zweifelhafter Untersuchungshandlungen zu verhindern oder jedenfalls wesentlich zu erschweren.

Auch die von DTAG in Bezug auf die identifizierten Einzelsachverhalte beschlosse-

nen Maßnahmen bezeichnet KPMG im Abschlussbericht zu diesem Projekt als angemessen.

IV. Weiteres Vorgehen

Der Abschluss der Maßnahmenumsetzung ist bis zum 30.06.2010 geplant.