HELBING
Kanzlei für IT- und Datenschutzrecht

DATENSCHUTZ BEI COMPLIANCE PROGRAMMEN

Eine Checkliste mit Erläuterungen und Best Practices

Rechtsanwaltskanzlei
Dr. Thomas Helbing

www.thomashelbing.com

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465-28
E helbing@thomashelbing.com

USt.-IdNr. DE815182912

VORWORT

Immer mehr Unternehmen ernennen Compliance Officer und implementieren zum Teil umfassende Compliance Programme. Deren Aufgabe ist, die Einhaltung von Rechtsvorschriften durch das Unternehmen sicherzustellen, z.B. Korruption und unzulässige Kartellabsprachen, Geldwäsche sowie Betrugs- und Untreuefälle zu verhindern und aufzuklären.

Doch auch das Compliance-Programm selbst muss den gesetzlichen Anforderungen genügen. Vor allem das Datenschutzrecht stellt hierbei eine Reihe von Anforderungen und setzt Grenzen.

Wie Fälle aus der Vergangenheit gezeigt haben, können selbst vermeintliche Verstöße des Compliance-Programms gegen den Datenschutz erhebliche Imageschäden für das Unternehmen und sogar persönliche Konsequenzen für das Management haben. Es drohen Bußgelder und im Extremfall strafrechtliche Verfolgung.

Mit der geplanten Vereinheitlichung des Datenschutzes durch eine Europäische Datenschutz-Grundverordnung wird der Datenschutz zukünftig weiter an Bedeutung gewinnen. Dies auch deshalb, weil die drohenden Sanktionen bei Datenschutzverletzungen massiv verschärft werden sollen.

Die vorliegende Checkliste hilft, datenschutzrelevante Themen bei Compliance-Programmen zu erkennen. Neben Kontrollfragen enthält die Checkliste Erläuterungen sowie Empfehlungen und Best Practices.

Die Checkliste wendet sich an Compliance Officer, Mitarbeiter von Compliance-, Rechts- und Revisions-Abteilungen und Datenschutzbeauftragte.

Die Checkliste deckt derzeit folgende Bereiche ab:

A) Interne Compliance Ermittlungen
B) Einsichtnahme und Auswertung von Mitarbeiter E-Mails
C) IT-Forensische Untersuchungen / Compliance Screenings / Massendatenanalysen
D) Hinweisgebersysteme (Whistleblowing)
E) Zentrale Compliance im Konzern / Verbund

Geplante weitere Themen sind:

- E-Discovery
- Pre-Employment Screenings
- Terrorlisten Screenings
- Geldwäscheprävention

Die Checkliste wird regelmäßig aktualisiert und ergänzt. Bitte laden Sie die jeweils aktuelle Version herunter auf: www.thomashelbing.com

Ich freue mich über Anregungen, Kritik und einen Erfahrungsaustausch.

München, im März 2013

Dr. Thomas Helbing
Rechtsanwalt

A INTERNE COMPLIANCE ERMITTLUNGEN

Ermittelt das Unternehmen gegen Mitarbeiter oder Dritte wegen des Verdachts von Compliance-Verstößen werden Interviews geführt, E-Mails durchforstet, Buchungs-Daten ausgewertet und Ermittlungsakten angelegt. Dabei werden personenbezogene Daten erhoben und genutzt. Dies ist nur zulässig, wenn das Datenschutzrecht hierfür eine Erlaubnisnorm bereit hält und bestimmte Datenschutzgrundsätze beachtet werden.

A.1 Zulässigkeit von Ermittlungsmaßnahmen

Wie ist sichergestellt, dass interne Ermittlungen gegen Mitarbeiter dem datenschutzrechtlichen Verhältnismäßigkeitsgebot genügen?

Das BDSG erlaubt bei zielgerichteten Ermittlungen die Erhebung und Verwendung von personenbezogenen Daten zu Ermittlungszwecken grundsätzlich nur, wenn ein entsprechender Anfangsverdacht vorliegt und dokumentiert wird. In jedem Fall muss die Verhältnismäßigkeit von Ermittlungsmaßnahmen gewahrt sein.

→ *Richtlinie/Arbeitsanweisung und Checkliste zur Dokumentation des Anfangsverdachts und der Verhältnismäßigkeit von Ermittlungsmaßnahmen*

A.2 Information von Betroffenen

Wie werden Betroffene bei Ermittlungen datenschutzkonform informiert?

Wenn im Rahmen der Fallermittlung erstmalig personenbezogene Daten ohne Kenntnis des Betroffenen gespeichert werden (z.B. Aufnahme von Erkenntnissen in eine Fallakte, Dokumentation von Hinweisen gegen einen Mitarbeiter) müssen Betroffene gemäß den Datenschutzbestimmungen hierüber informiert werden.

→ *Prüfung und Sicherstellung der Betroffeneninformation durch Aufnahme als Schritt im Fallermittlungsprozess (Richtlinie/Arbeitsanweisung)*

A.3 Löschung

Wann und wie werden Ermittlungsergebnisse gelöscht?

Fallermittlungsakten enthalten personenbezogene Daten. Eine Speicherung auf unbestimmte Zeit ist datenschutzrechtlich unzulässig.

→ *Festlegung und Umsetzung eines Löschungs- und Archivierungskonzeptes für Ermittlungsergebnisse*

→ *Geeignete Organisation von E-Mail-Ablagen und Fallakten*

A.4 Datenweitergabe an Ermittlungsbehörden

Wie ist sichergestellt, dass die Weitergabe von Daten an Behörden datenschutzkonform erfolgt?

Bei Compliance-Fällen arbeitet das Unternehmen oft mit Ermittlungsbehörden, z.B. der Staatsanwaltschaft, dem Bundeskartellamt oder der Europäischen Kommission zusammen, um den Sachverhalt aufzuklären. Manchmal werden auch seitens der Behörden Auskunftsersuchen an das Unternehmen herangetragen. Werden Daten über Mitarbeiter oder Kunden des Unternehmens an die Behörde übermittelt, so ist dies nur zulässig, wenn eine datenschutzrechtliche Erlaubnisnorm greift. Das bloße Auskunftsersuchen der Behörde genügt nicht per se.

- → *Forderung eines schriftlichen Ersuchens der Behörde mit Sachverhaltsschilderung*
- → *Dokumentation der Rechtsgrundlage für die Daten-Weitergabe*
- → *Richtlinie/Arbeitsanweisung und Checkliste zur Prüfung und Dokumentation der datenschutzrechtlichen Zulässigkeit einer Datenweitergabe*

A.5 Need to know

Wie ist sichergestellt, dass nur relevante Personen Zugriff auf Ermittlungsergebnisse haben?

Die Gebote der Datensparsamkeit und der Datensicherheit verlangen, dass nur solche Personen Zugriff auf Ermittlungsdaten haben, die diese für ihre Arbeit zwingend benötigen (z.B. nur der konkrete Fallermittler und dessen Vorgesetzter, nicht der Vorgesetzte des Beschuldigten oder andere Abteilungen)

- → *Kategorisierung der Sensitivität von Ermittlungsdaten*
- → *Festlegung und Umsetzung eines Berechtigungs- und Zugriffskonzeptes*
- → *Geeignete Organisation von E-Mail-Ablagen und Fallakten*
- → *Datenschutz-Schulung von Compliance Mitarbeitern*

A.6 Einbindung des Datenschutzbeauftragten

Wie ist die gesetzlich vorgeschriebene Einbindung des Datenschutzbeauftragten sichergestellt?

Über bestimmte Datenverarbeitungsverfahren muss nach dem Bundesdatenschutzgesetz der Datenschutzbeauftragte des Unternehmens vorab informiert werden. In manchen Fällen muss dieser sogar eine Stellungnahme zur Datenschutzkonformität abgeben (Vorabkontrolle), bevor mit der Datenverwendung begonnen werden kann.

- → *Abstimmung des Fallermittlungsprozesses mit dem Datenschutzbeauftragten*
- → *Prüfung der Einbindung des Datenschutzbeauftragten als Schritt im Fallermittlungsprozess aufnehmen (bei bestimmten Ermittlungsmaßnahmen, z.B. E-Mail Screening)*

B EINSICHTNAHME UND AUSWERTUNG VON MITARBEITER E-MAILS

Der Verdacht von Compliance-Verstößen kann oft nur aufgeklärt werden, wenn der interne Fallermittler in E-Mails von Mitarbeitern Einsicht nimmt bzw. diese ausgewertet werden. Diese Ermittlungsmaßnahmen unterliegen jedoch datenschutzrechtlichen Einschränkungen. Werden E-Mails unzulässig für Ermittlungszwecke verwendet, kann dies auch eine strafbare Verletzung des Fernmeldegeheimnisses darstellen.

B.1 Regelung zur E-Mail Nutzung

Ist die Nutzung des E-Mail Dienstes und anderer elektronischer Kommunikationssysteme durch die Mitarbeiter geregelt?

Wann und wie ein Arbeitgeber in E-Mails der Mitarbeiter Einsicht nehmen darf, ist rechtlich komplex. Eine Rolle spielt dabei noch, ob der Arbeitgeber seinen Mitarbeitern die private Nutzung der Firmen E-Mail untersagt hat, und ob dieses Verbot auch kontrolliert und Verstöße geahndet werden. Zu diesen Punkten sollte deshalb Klarheit herrschen.

Vorzugswürdig aus Compliance-Sicht ist ein Verbot der privaten E-Mail Nutzung. Dies kann kombiniert werden mit einer Erlaubnis zur privaten Nutzung für solche Mitarbeiter, die im Gegenzug der Einsichtnahme in ihre E-Mails unter bestimmten Voraussetzungen vorab zustimmen.

- → *Regelung der E-Mail-Nutzung durch schriftliche Arbeitsanweisung*
- → *Kommunikation der Nutzungsbedingungen*
- → *Kontrolle der Einhaltung der Nutzungsbedingungen und Sanktionierung von Verstößen*
- → *Betriebsvereinbarung zur E-Mail Nutzung*

B.2 Festlegung des Verfahrens

Ist das Verfahren festgelegt, gemäß dem E-Mails für Ermittlungszwecke verwendet werden dürfen?

Wenn der Verdacht auf einen Compliance-Verstoß aufgeklärt werden muss, soll alles schnell gehen. Ist dann unklar, wer im Unternehmen wie und unter welchen Voraussetzungen E-Mails einsehen und auswerten darf, erhöht sich die Gefahr von zeitlichen Verzögerungen oder der Missachtung des Datenschutzes.

- → *Richtline / Arbeitsanweisung zur Verwendung von E-Mails für Ermittlungszwecke (Voraussetzungen, interne Zuständigkeit, Pflicht zur Einbindung von bestimmten Abteilungen, technische Umsetzung)*
- → *Betriebsvereinbarung zur Einsichtnahme in E-Mails*

B.3 Externe IT-Dienstleister

Wurden mit externen IT-Dienstleistern die notwendigen Datenschutzvereinbarungen getroffen?

Müssen umfangreiche E-Mail Datenbestände ausgewertet werden, z.B. bei Kartellverstößen oder systematischen Betrugsfällen, können spezialisierte IT Dienstleister oder Wirtschaftsberatungen helfen. Erhalten diese Zugriff auf Mitarbeiter E-Mails, verlangt das Gesetz bestimmte Datenschutzverträge. Ohne die notwendigen Verträge drohen Bußgelder.

→ *Auftragsdatenverarbeitungsverträge mit entsprechenden Dienstleistern schließen, ggf. auch vorsorglich.*

Zu weiteren Anforderungen bei der Einsichtnahme und Auswertung von Mitarbeiter E-Mails siehe unbedingt unten Abschnitt C " IT-Forensische Untersuchungen / Compliance Screenings / Massendatenanalysen"

C IT-FORENSISCHE UNTERSUCHUNGEN / COMPLIANCE SCREENINGS / MASSENDATENANALYSEN

Die Aufklärung von Korruption, Kartellabsprachen oder Fraud-Fällen (Untreue, Betrug), kann die strukturierte Analyse und Auswertung größerer Datenmengen erforderlich machen. Das können E-Mails aber auch Dateien auf Servern, Laptops und Mobilfunkgeräten sein. Auch Daten aus ERP-Systemen, insbesondere Finanzbuchhaltungsdaten, sollen unter Umständen herangezogen werden. Neben der (repressiven) Aufklärung von konkreten Verdachtsfällen werden solche IT forensische Untersuchungen auch (präventiv) eingesetzt, um mögliche Verstöße zu identifizieren oder geeignete Stichproben für die Arbeit der Revisionsabteilung zu ermitteln. Das Unternehmen verarbeitet und nutzt dabei fast immer personenbezogene Daten von Mitarbeitern und Geschäftspartnern und muss entsprechend die datenschutzrechtlichen Anforderungen beachten.

C.1 Zulässigkeit und Zweckbindung

Liegt ein konkreter Anfangsverdacht vor (repressiv) bzw. wurde der Zweck der forensischen Untersuchung definiert und dokumentiert (präventiv)?

Bei der (repressiven) Datenanalyse zur Aufklärung des Verdachts von Straftaten oder schweren Pflichtverletzungen verlangt das Gesetz "zu dokumentierende tatsächliche Anhaltspunkte", die den Verdacht begründen. Bei (präventiven) Datenanalysen sind das spezifische Risiko und das Ziel der Datenanalyse zu definieren.

→ *Dokumentation der tatsächlichen Anhaltspunkte, die einen Verdacht begründen (repressiv) bzw. spezifisches Risiko und Zweck der Untersuchung (präventiv).*

→ *Dokumentation des geplanten Inhalts, Umfangs und Ablaufs der Untersuchung in einem "Vorabkonzept" (siehe hierzu auch unten C.2 bis C.4)*

C.2 Datensparsamkeit und Verhältnismäßigkeit

Wurde der Umfang der zu analysierenden Daten soweit wie möglich eingeschränkt und der Verhältnismäßigkeitsgrundsatz gewährt?

Die Grundsätze der Datensparsamkeit und Verhältnismäßigkeit verlangen, dass der Umfang der Daten soweit wie möglich eingeschränkt wird. Dies gilt im Hinblick auf die Zahl der Betroffenen (z.B. nur E-Mails von Mitarbeitern der Einkaufsabteilung) und den Umfang der Daten (z.B. Auswertung nur bestimmter Datenfelder der Finanzbuchhaltung). Besondere Vorsicht ist bei Kommunikations-Daten geboten (E-Mail-Verkehr, Telefondaten), da diese ggf. dem Fernmeldegeheimnis unterliegen und eine Auswertung strafbar sein kann. Nicht dienstliche (private) Mitarbeiterdaten sind zudem durch geeignete Maßnahmen frühzeitig auszusondern.

→ *Dokumentation der relevanten Daten und ihrer Herkunft*

→ *Dokumentation, inwieweit eine Datenreduktion in Betracht kommt*

→ *Aussonderung privater Mitarbeiterdaten*

→ *Dokumentation der Einhaltung des datenschutzrechtlichen Verhältnismäßigkeitsgrundsatzes (Erwägungsgründe)*

C.3 Pseudonymisierung

Wird die Datenanalyse - soweit möglich - auf Basis pseudonymisierter Daten durchgeführt?

Für die Datenanalyse werden Datenbestände zunächst aus den Produktivsystemen kopiert. Bevor eine Analyse stattfindet, sollte soweit wie möglich eine Pseudonymisierung erfolgen, das heißt alle Merkmale, die Rückschluss auf eine einzelne Person erlauben sind zu löschen (z.B. Nutzerkennung des Mitarbeiters, der eine Buchung vorgenommen hat). Nur im Falle eines "Treffers" und soweit zur weiteren Aufklärung nötig, werden die persönlichen Merkmale im Einzelfall wieder einbezogen.

→ *Dokumentation der Pseudonymisierung bzw. des Grundes, warum eine solche nicht möglich war*

C.4 Transparenz

Wurde der Transparenzgrundsatz beachtet?

Werden erstmalig personenbezogene Daten zu einer Person ohne deren Kenntnis gespeichert, muss diese informiert werden, so verlangt es das Bundesdatenschutzgesetz. Eine Information kann auch erforderlich werden, wenn Betroffene mit der Nutzung ihrer Daten für die Untersuchung nicht rechnen mussten (wesentliche Zweckänderung in der Nutzung der Daten).

→ *Prüfung von Transparenzverpflichtungen und Dokumentation des Ergebnisses*

→ *Ggf. Information der Betroffenen*

C.5 Einbindung des Datenschutzbeauftragten

Wurde der Datenschutzbeauftragte eingebunden?

Repressive Datenanalysen sollten vorher mit dem Datenschutzbeauftragten im Einzelfall abgesprochen werden. Bei präventiven Analysen empfiehlt sich, das grundsätzliche Vorgehen und etwaige datenschutzrechtliche Grenzen mit dem Datenschutzbeauftragten vorab abstrakt zu klären.

→ *Arbeitsanweisung/Richtlinie zur Sicherstellung des Datenschutzes bei präventiven Datenanalysen*

C.6 Vertrag mit Dienstleister

Wurde mit einem externen Dienstleister eine Datenschutzvereinbarung getroffen?

Werden externe Dienstleister mit der Durchführung der Datenanalysen beauftragt, liegt eine Auftragsdatenverarbeitung vor. Das Gesetz verlangt einen Vertrag, der zehn inhaltliche Vorgaben erfüllen muss. Außerdem sind die Datensicherheitsmaßnahmen zu dokumentieren und ihre Einhaltung sicherzustellen. Das gilt auch, wenn eine Wirtschaftsberatung oder Kanzlei die Datenanalyse als abgrenzbaren Teil ihrer sonstigen Beratungsleistung erbringt.

→ *Berücksichtigung der Datenschutzbelange schon bei Auswahl des Anbieters, d.h. vor Vertragsschluss*

→ *Prüfung der Datensicherheitsmaßnahmen des Anbieters vor Vertragsschluss*

→ *Abschluss eines schriftlichen Auftragsdatenverarbeitungsvertrages*

C.7 Betriebsvereinbarung

Wurde eine Betriebsvereinbarung zu IT forensischen Untersuchungen geschlossen?

Forensische Untersuchungen sind oft mitbestimmungspflichtig. Aus Datenschutzsicht kann eine Betriebsvereinbarung zudem helfen, die datenschutzrechtliche Zulässigkeit sicherzustellen.

→ *Betriebsvereinbarung zu IT forensischen Untersuchungen schließen (Zuständigkeiten, Verfahren, Einbindung relevanter Personen, Voraussetzungen und Grenzen)*

D HINWEISGEBERSYSTEME (WHISTLEBLOWING)

Hinweisgebersysteme sind eine wichtige Quelle für das Unternehmen, um etwaigen Compliance-Verstößen auf die Spur zu kommen. Über eine Webseite oder telefonisch können Mitarbeiter oder Geschäftspartner Hinweise auf mögliches Fehlverhalten geben. Mit einer solchen Webseite oder Hotline erhebt der Arbeitgeber zielgerichtete personenbezogene Daten über Fehlverhalten seiner Mitarbeiter. An diese Datenerhebung und die anschließende Verwendung zu Ermittlungszwecken haben Datenschutzaufsichtsbehörden in Europa strenge Anforderungen gestellt.

D.1 Meldefähige Verstöße

Wie wird sichergestellt, dass das Hinweisgebersystem nur für Hinweise auf schweres Fehlverhalten genutzt wird?

Datenschutzbehörden verlangen, dass Arbeitgeber über Whistleblowing-Systeme nur Hinweise auf schweres Fehlverhalten erheben, z.B. auf Verhaltensweisen, die einen gegen das Unternehmensinteresse gerichteten Straftatbestand erfüllen, Menschenrechte verletzen (Kinderarbeit) oder gegen Umweltschutzbelange verstoßen. Dies gilt insbesondere bei anonymen Hinweisen und wenn Mitarbeiter zur Meldung von Verstößen angehalten werden.

→ *Klare Definition und Kommunikation der meldefähigen Verstöße*

→ *Zurückweisung von Meldungen zu Bagatellfällen*

D.2 Kreis möglicher Hinweisgeber und Beschuldigter

Wurde geprüft, ob der Kreis der möglichen Hinweisgeber und Beschuldigten begrenzt werden kann?

Nach dem Willen der Aufsichtsbehörden sollen Unternehmen prüfen, inwieweit der Personenkreis, der Hinweise geben darf, eingegrenzt werden kann (z.B. nur Mitarbeiter im Einkauf, Vertrieb, Management). Ebenso soll geprüft werden, ob der Kreis der Beschuldigten eingegrenzt werden kann, z.B. weil bei gewerblichen Mitarbeitern ein geringeres Korruptionsrisiko besteht.

→ *Mögliche Einschränkungen der Personenkreise prüfen und Ergebnis dokumentieren*

→ *Ggf. interne Kommunikation zum Hinweisgebersystem auf bestimmte Zielgruppen beschränken*

D.3 Anonyme Hinweise

Werden geeignete Maßnahmen getroffen, um Hinweisgeber zur Offenlegung ihrer Identität zu motivieren?

Anonyme Hinweise sind nicht per se unzulässig. Nach Auffassung der Aufsichtsbehörden sollten diese aber die Ausnahme bilden und Hinweisgeber zur Offenlegung ihrer Identität motiviert werden.

→ *Sicherstellung und Zusicherung der vertraulichen Behandlung der Identität von Hinweisgebern*

→ *Hinweisgeber zur Offenlegung der Identität ermutigen*

→ *Kein expliziter Hinweis auf Möglichkeit anonymer Hinweise, Möglichkeit anonymer Hinweise nur als "zweite Wahl" anbieten*

D.4 Mitbestimmung

Wurden die Mitbestimmungsrechte beachtet?

Hinweisgebersysteme in Form von Websites sind mitbestimmungspflichtig. Dies ist zwar eine Anforderung aus dem Betriebsverfassungsrecht und nicht dem Datenschutzrecht. Haben aber Arbeitgeber und Betriebsrat eine Betriebsvereinbarung geschlossen, so kann diese in gewissem Umfang auch als datenschutzrechtliche Erlaubnis dienen.

→ *Hinweisgebersystem in Betriebsvereinbarung regeln*

D.5 Vertrag mit Dienstleister

Wurde mit dem externen Anbieter eines Hinweisgebersystems eine entsprechende Datenschutzvereinbarung getroffen?

Web-basierte Hinweisgebersysteme werden oft von externen Dienstleistern technisch betrieben. Das Datenschutzrecht verlangt dann einen sogenannten Auftragsdaten-verarbeitungsvertrag. Ohne diesen Vertrag drohen dem Arbeitgeber Bußgelder. Außerdem fordert das Gesetz, dass sich das Unternehmen vor Vertragsschluss von der Angemessenheit der Datensicherheitsmaßnahmen des Anbieters überzeugt.

→ *Berücksichtigung der Datenschutzbelange schon bei Auswahl des Anbieters, d.h. vor Vertragsschluss*

→ *Prüfung der vom Anbieter getroffenen Datensicherheitsmaßnahmen bereits im Vorfeld des Vertragsschlusses*

→ *Abschluss eines schriftlichen Auftragsdatenverarbeitungsvertrages*

D.6 Einbindung des Datenschutzbeauftragten

Wurde der Datenschutzbeauftragte frühzeitig vor Einführung des Hinweisgebersystems informiert?

Das BDSG verpflichtet Unternehmen, ihrem Datenschutzbeauftragten frühzeitig bestimmte Informationen über das geplante Hinweisgebersystem mitzuteilen. Der Datenschutzbeauftragte muss dann vor Inbetriebnahme die Einhaltung des Datenschutzes prüfen (sogenannte Vorabkontrolle).

→ *Frühzeitige Information des Datenschutzbeauftragten*

→ *Abwarten der Stellungnahme des Datenschutzbeauftragten vor Start des Hinweisgebersystems*

D.7 Aufklärung von Hinweisen

Werden bei der Aufklärung von Hinweisen die datenschutzrechtlichen Vorgaben beachtet?

Siehe Ziffer A oben. Wichtig ist insbesondere: Beschuldigte müssen über Hinweise zu ihrer Person informiert werden, wenn dies den Ermittlungszweck nicht mehr gefährdet. Sich als haltlos erweisende Hinweise sind zeitnah zu löschen (oder zu anonymisieren).

→ Siehe Ziffer A oben.

D.8 Zentrales Hinweisgebersystem im Konzern

Bei einem Konzern oder sonstigen Verbund: Wurde dem fehlenden Konzernprivileg ausreichend Rechnung getragen?

Siehe Ziffer E unten. Besteht ein Unternehmen aus mehreren rechtlich selbstständigen Gesellschaften (Konzern, Unternehmensverbund), so werden diese aus Sicht des Datenschutzes nicht als Einheit, sondern isoliert betrachtet. Oft haben solche Unternehmen aber ein zentrales Hinweisgebersystem und eine zentrale Compliance-Abteilung. Es ist dann sicherzustellen, dass der damit einhergehende konzerninterne Datenfluss (z.B. Weitergabe von Daten zu Ermittlungszwecken) datenschutzkonform erfolgt.

→ Siehe Ziffer E unten.

E ZENTRALE COMPLIANCE IM KONZERN / VERBUND

Bei einem Konzern oder sonstigen Unternehmensverbund hat die Muttergesellschaft oft eine zentrale Compliance-Abteilung eingerichtet, die Richtlinien erlässt, Mitarbeiter schult, Compliance-Tools zur Verfügung stellt und ggf. Verstöße ermittelt. Bei diesen Tätigkeiten werden Mitarbeiter- und Kundendaten zwischen den Tochterunternehmen und der Muttergesellschaft ausgetauscht. Das Datenschutzrecht kennt jedoch kein Konzernprivileg: die Weitergabe von Daten im Konzern bzw. Verbund unterliegt grundsätzlich den selben Anforderungen wie eine Weitergabe an sonstige Dritte.

E.1 Datenweitergabe im Konzern / Verbund

Ist die Übermittlung von personenbezogenen Daten zu Compliance-Zwecken innerhalb des Konzerns bzw. Verbundes datenschutzkonform?

Jede Datenweitergabe zwischen Konzern- oder Verbundunternehmen zu Compliance-Zwecken bedarf einer Erlaubnisnorm.

Zur Absicherung der Zulässigkeit der Datenübermittlung empfiehlt sich eine verbindliche Vereinbarung, in der die Konzern- bzw Verbundunternehmen festlegen, wie Daten für Compliance-Zwecke gehandhabt werden dürfen und wie die Rechte der betroffenen Mitarbeiter gewahrt werden.

Soweit die Konzernmutter im Rahmen der Compliance-Arbeit IT technische Dienstleistungen erbringt (z.B. IT gestützte Compliance-Tools), kann dies zudem eine Auftragsdaten-verarbeitung darstellen, sodass zwischen Tochter und Mutter ein spezieller Auftragsdaten-verarbeitungsvertrag geschlossen werden muss.

→ *Abschluss eines konzerninternen Vertrages zur Auftragsdatenverarbeitung und zur Datenübermittlung für Compliance-Zwecke*

E.2 Ausländisches Datenschutzrecht

Werden etwaige Besonderheiten nach ausländischem Datenschutzrecht berücksichtigt?

Das Datenschutzrecht in der Europäischen Union ist durch eine Datenschutzrichtlinie harmonisiert. Dennoch hat jedes Land (noch) sein eigenes Datenschutzgesetz, mit Abweichungen und unterschiedlicher Interpretation der nationalen Aufsichtsbehörden. Das deutsche Datenschutzgesetz gilt als besonders streng. Dennoch gibt es Besonderheiten im Ausland zu beachten: So müssen zum Beispiel in vielen Ländern, wie etwa Österreich oder Frankreich, Datensammlungen gegenüber Behörden gemeldet werden. Grobe Daumenregel: Für Mitarbeiter- und Kunden-Daten gilt in der EU jeweils das Recht des Landes, in der der Arbeitgeber des Mitarbeiters, bzw. der Vertragspartner des Kunden seinen Sitz hat (für Kunden- und Mitarbeiterdaten der französischen Vertriebstochter gilt etwa französisches Recht).

→ *Datenschutzorganisation bei Auslandsgesellschaften etablieren*

→ *Datenschutzfragen durch lokale Ansprechpartner klären*

Rechtsanwaltskanzlei
Dr. Thomas Helbing

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465-28
E helbing@thomashelbing.com
www.thomashelbing.com