Datenschutz in der HR-Praxis

Inhaltsverzeichnis

I. FRAGEN UND ANTWORTEN RUND UMS PERSONALDOSSIER

lic. iur. Barbara Meyer, Fachanwältin SAV Arbeitsrecht

1. EINLEITUNG

Bereits das Wort "Personaldossier" mag sich für den einen oder anderen etwas angestaubt, trocken und uninteressant anhören. Dabei besteht durchaus einiges Sprengpotential, z.B. in dem derzeit vor Bundesgericht hängigen Verfahren 4A_215/2014. In diesem Verfahren streiten aktuell ein frühzeitig pensionierter Bankdirektor (mit schweizerisch-amerikanischer Doppelstaatsbürgerschaft) und seine ehemalige Arbeitgeberin, die Credit Suisse, darüber, ob der Bankdirektor Anspruch auf Kopien all jener Akten hat, welche die Credit Suisse dem "Department of Justice" in den USA im Zusammenhang mit Abklärungen zu ihrem Crossborder-Geschäft übergeben hat.

Der Bankdirektor gibt an, dass er die Rechtmässigkeit der Datenbearbeitung kontrollieren bzw. sich vor einem allfälligen Nachteil schützen will. Weiter weist er daraufhin, dass es sich um rund 75 Dokumente mit total ca. 200 Seiten handle, und damit um eine schlicht zu grosse Datenmenge, die man sich nicht merken könne. Kopien seien daher unerlässlich.

Die Credit Suisse beharrt dagegen auf dem Standpunkt, dass sie mit der angebotenen Einsicht in die Dokumente den datenschutzrechtlichen Verpflichtungen nachgekommen sei. Einerseits würde einer Herausgabe der Akten das Bankkundengeheimnis entgegenstehen, selbst bei vorgenommenen Schwärzungen. Andererseits befürchtet die Credit Suisse eine Weitergabe von Personendaten Dritter, weil in den Dokumenten auch andere Arbeitnehmer erwähnt werden.

In zweiter Instanz hat nun das Obergericht Zürich entschieden, dass der Kläger ein Anrecht auf Kopien hat, wobei Daten von Dritten zu schwärzen seien. Es gilt abzuwarten, wie das Bundesgericht entscheiden wird.

Der Fall illustriert die Brisanz, welche in Personaldossiers stecken kann, egal ob die Datensammlung als Personaldossier bezeichnet wird oder einen anderen Namen trägt. Worauf muss der Arbeitgeber beim Erstellen von Personalakten achten? Auf welche Akten hat der Arbeitnehmer welche Ansprüche? Und bis zu welchem Zeitpunkt können welche Rechte geltend gemacht werden? Derartige Fragen sind in der Arbeitswelt allgegenwärtig. Der geschilderte Fall unterstreicht die Komplexität, welche der Streitpunkt "Personaldossier" unter Umständen annehmen kann.

2. PFLICHT EIN PERSONALDOSSIER ZU FÜHREN?

Der einleitend beschriebene Fall zeigt exemplarisch, dass es nicht einfach ist, Personaldossiers zu führen. Dies kann aufwändig sein und es kann sich eine Vielzahl von Rechtsfragen stellen. Es stellt sich daher die Frage, ob eine Pflicht zur Führung von Personaldossiers besteht.

Eine direkte bundesrechtliche Pflicht Personaldossiers zu führen, findet sich nirgends. Allerdings leitet sich diese Pflicht indirekt von verschiedenen anderen gesetzlichen Normen ab. Zu denken ist z.B. an Art. 330a OR. Ohne ein Personaldossier dürfte es schwer fallen, ein Zeugnis zu erstellen. Auch bestehen diverse Melde- und Abrechnungspflichten bei den Sozialversicherungen sowie allenfalls der Quellensteuer. In der Praxis ergeben sich sehr wichtige Gründe für ein Personaldossier auch aus Praktikabilitäts- und Beweisgründen. Wurde mit dem Arbeitnehmer eine Zielvereinbarung oder eine Provisionsvereinbarung abgeschlossen, muss anhand von Unterlagen überprüft werden können, ob und wie diese Ziele erfüllt wurden. Der Bezug von Ferien, das Vorliegen von Absenzen (inkl. Arztzeugnisse, Marschbefehle etc.) muss ebenfalls dokumentiert werden. Diese Dokumente werden ganz bewusst aufbewahrt, um auch später beweisen zu können, dass Zahlungsverpflichtungen nachgekommen wurde bzw. keine weiteren Zahlungsverpflichtungen bestehen.

Darüber hinaus ist die Erstellung von Personaldossiers oft in kantonalen Richtlinien und Personalgesetzen vorgesehen. So hat z.B. das Finanzdepartement des Kantons Basel-Stadt Richtlinien für das Personaldossier erlassen. Auch im Personalgesetz des Kantons Zürich finden sich Rechtsnormen zum Personaldossier.

3. INHALT EINES PERSONALDOSSIERS

Grundsätzlich dürfen nur Personendaten gesammelt werden, die in unmittelbarem Zusammenhang zur Arbeitstätigkeit des Arbeitnehmers stehen. Dazu gehört alles, was über einen Arbeitnehmer in Bezug auf die Entstehung, den Verlauf und die Beendigung des Arbeitsverhältnisses aufgezeichnet wird. Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) nennt exemplarisch die folgenden Daten:

- Personalien, Adresse
- Bewerbungsunterlagen, Referenzauskünfte, graphologische Gutachten, Testunterlagen
- Arbeitsvertrag, Bonusvereinbarungen, Weiterbildungsvereinbarungen, Beurteilungen
- Lohn- und Versicherungsdaten
- Abwesenheiten (Ferien, Krankheit/Unfall, Militär)
- Disziplinarmassnahmen (Verwarnungen, Verweise, Bussen)

Unzulässig sind sog. "Schattendossiers" oder "graue Dossiers". Wird eine Datensammlung über den Arbeitnehmer angelegt, muss er auch Zugang zu ihr haben. Es dürfen nicht einfach einzelne Teile abgespalten oder parallel noch ein weiteres Dossier geführt werden. Der EDÖB empfiehlt deshalb, das Personaldossier einer regelmässigen Triage zu unterziehen und nicht mehr benötigte Unterlagen zu entfernen (entsprechend dem datenschutzrechtlichen Verhältnismässigkeitsprinzip). Es stellt aber kein "Schattendossier" dar, wenn persönliche Notizen des Vorgesetzten (bspw. Gedächtnisstützen für Mitarbeitergespräche etc.) nicht gezeigt werden. Solche Daten müssen dem Arbeitnehmer im Rahmen der Einsicht in das Personaldossier nicht gezeigt werden, da hier die überwiegenden Interessen des Arbeitgebers vorgehen.

4. ANWENDBARE RECHTSNORMEN

A. Ist ein Personaldossier eine Datensammlung im Sinne des Datenschutzgesetzes?

Das Datenschutzgesetz (DSG) definiert, dass jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind, eine Datensammlung begründet. Damit ist das arbeitsrechtliche Personaldossier zweifelsohne als Datensammlung im Sinne des DSG zu qualifizieren. Unwesentlich für diese Zuordnung ist die Art, in welcher die Datensammlung angelegt ist (Systematik, Ordnung, Speicherungsart etc.). Durch die Qualifizierung als Datensammlung nach DSG sind die allgemeinen Grundsätze des Datenschutzgesetzes vom Arbeitgeber zu beachten.

B. Allgemeine Grundsätze des Datenschutzgesetzes

Das DSG ist von folgenden Grundsätzen geprägt:

- Rechtmässigkeit
- Erkennbarkeit
- Verhältnismässigkeit und Richtigkeit
- Zweckmässigkeit

Der Grundsatz der Rechtmässigkeit bedeutet, dass nur Daten gesammelt werden dürfen, die ohne Drohung oder Täuschung erhoben worden sind. Zugleich müssen die Daten im Wissen des Arbeitnehmers erhoben worden sein. Der Datenbeschaffungsprozess muss also transparent ausgestaltet sein. Gemäss dem Verhältnismässigkeitsprinzip dürfen nur so viele Daten wie nötig und so wenige als möglich gesammelt werden. Blindlings schlichtweg alles über die Mitarbeitenden zu sammeln, wäre unter diesem Aspekt unzulässig. Weiter müssen die Daten richtig sein. Daten dürfen zudem nur zu dem Zweck verarbeitet werden, der bei der Datenbeschaffung angegeben wurde. Zuletzt hat der Arbeitgeber sicherzustellen, dass die Daten gegen unberechtigten Zugriff geschützt sind. Personendaten dürfen daher nur durch die Personalabteilung bzw. durch Stellen, die ein auf den Arbeitsplatz bezogenes berechtigtes Interesse haben, bearbeitet werden. Gemäss datenschutzrechtlichen Prinzi-

pien muss die Verarbeitung von Personendaten darüber hinaus durch einen Rechtfertigungsgrund geschützt sein. Für das Arbeitsverhältnis ist dies durch die oben erwähnten gesetzlichen Vorschriften grundsätzlich erfüllt.

C. Datenschutzgesetz und Art. 328b OR

Im Arbeitsrecht gilt ein noch strengerer Massstab, da zusätzlich zu den datenschutzrechtlichen Vorgaben obligationenrechtliche Spezialnormen respektiert werden müssen, von denen vertraglich nicht abgewichen werden kann (Art. 328b OR). So darf der Arbeitgeber nur Daten bearbeiten, die für die Eignungsprüfung für das Arbeitsverhältnis, resp. für die Durchführung des Arbeitsvertrages erforderlich sind. Das heisst, dass jegliche Bearbeitung von Arbeitnehmerdaten, die keinen Bezug zum Arbeitsplatz haben, unzulässig ist. Dies gilt selbst dann, wenn die Datenbearbeitung im Lichte des Datenschutzgesetzes rechtskonform wäre, oder wenn eine Einwilligung des Arbeitnehmers vorliegen würde.

5. RECHTE DES ARBEITNEHMERS

Die zwei wichtigsten Rechte des Arbeitnehmers in Bezug auf sein Personaldossier sind das Auskunfts- und Einsichtsrecht sowie das Berichtigungs- und/oder Vernichtungsrecht.

A. Auskunfts- und Einsichtsrecht

Ein Arbeitnehmer hat das Recht, mittels eines Auskunftsgesuches über den Inhalt seines Personaldossiers informiert zu werden (Art. 8 Abs. 1 DSG). Das Auskunftsrecht ist an keine besonderen Voraussetzungen gebunden. Der Arbeitnehmer muss weder ein schützenswertes Interesse, noch eine Persönlichkeitsverletzung glaubhaft machen. Das Auskunftsrecht erstreckt sich auf alle vorhandenen Daten, seien es Tatsachen, seien es Werturteile. Ausgenommen sind lediglich persönliche Notizen des Vorgesetzten, die nicht an Dritte bekannt gegeben werden müssen (bspw. Gedächtnisstützen für Mitarbeitergespräche u.ä.). Verweigerungen, Beschränkungen oder Aufschiebungen eines Auskunftsbegehrens sind nur ausnahmsweise zulässig und müssen begründet sein. Derartige Ausnahmen können bestehen, wenn überwiegend private oder öffentliche Interessen dem Auskunftsgesuch entgegenstehen.

Betreffend die Einsicht bzw. das Anrecht auf Kopien kann auf den Einleitungsfall verwiesen werden. Derzeit sind diese Fragen noch nicht in allen Konstellationen geklärt. Gemäss Art. 8 Abs. 5 DSG hat ein Arbeitnehmer grundsätzlich das Recht auf schriftliche Auskunft mittels Fotokopien. Diese haben kostenlos zu erfolgen. Die Herausgabe des Original-Personaldossiers empfiehlt sich nicht. Dieses sollte einzig dem Rechtsvertreter des Arbeitnehmers (per Einschreiben) zugestellt werden. Es empfiehlt sich aber auch dann, eine Sicherungskopie zu behalten. Nicht durchsetzbar sind Auskunftsrechte (und weitere datenschutzrechtliche Behelfe) bei hängigen Zivilprozessen.

B. Berichtigungs- und/oder Vernichtungsrecht

Sind Personendaten fehlerhaft, haben Angestellte das Recht auf eine Berichtigung. Diesem Recht kann der Arbeitnehmer keine ausschliessenden Rechtfertigungsgründe entgegensetzen. Betroffen sind Informationen, die einen konkreten Tatsachenbezug aufweisen, wohingegen sich der Berichtigungsanspruch nicht auf reine Werturteile erstreckt. Bei unzulässig erhobenen Daten oder solchen, die nicht (mehr) bearbeitet werden dürfen, besteht zudem ein Vernichtungs- bzw. Löschungsrecht. Diesbezüglich verweist das Datenschutzrecht auf die zivilrechtlichen Klagen und Massnahmen zum Schutze der Persönlichkeit. Wahlweise können Betroffene verlangen, dass Daten über sie berichtigt oder vernichtet werden oder dass die Bekanntgabe an Dritte gesperrt wird. Die Beweislast über die Richtigkeit der Daten liegt beim Datenbearbeiter, d.h. beim Arbeitgeber. Ausserdem stehen gegebenenfalls strafrechtliche Mittel zur Verfügung, falls etwa berufliche Schweigepflichten verletzt worden sind oder vorsätzlich falsche oder unvollständige Auskünfte über das Personaldossier erteilt worden sind. In Bezug auf vernichtete Daten entfällt das Auskunfts- respektive das Einsichtsrecht des Arbeitnehmers.

Der Praxis ergeben sich Berichtigungs- oder gar Löschungsansprüche meist im Zusammenhang mit Verwarnungen. Oft beklagen sich Arbeitnehmer über schriftliche Verwarnungen und streben deren Entfernung aus dem Personaldossier an. Ob einem solchen Begehren nachzukommen ist, ist im Einzelfall zu prüfen. Auf Arbeitgeberseite empfiehlt sich eine gewisse Zurückhaltung. Dem Arbeitnehmer bleibt meistens nichts anderes übrig, als seinerseits schriftlich an die Arbeitgeberin heranzutreten und seine Sicht der Dinge darzustellen. Dieses Schreiben ist im Personaldossier (zusammen mit der Verwarnung) abzulegen.

C. Zeitliche Aspekte

Der zeitliche Anwendungsbereich der arbeitsrechtlichen Datenbearbeitung erstreckt sich von der Bewerbungsphase bis weit nach Beendigung des Arbeitsverhältnisses. Gleichzeitig ist in diesem Zusammenhang an das Verhältnismässigkeitsprinzip zu erinnern, wonach nur diejenigen Daten aufbewahrt werden dürfen, die wirklich erforderlich sind.

Ein Enddatum stellt die Verjährungsfrist dar. Die allgemeine Verjährung für vertragliche Forderungen beträgt 10 Jahre. Kontrovers diskutiert wird, ob die spezialgesetzliche Verjährung von 5 Jahren – die prinzipiell innerhalb arbeitsrechtlicher Verhältnisse gilt – auch für die Aufbewahrung von Personendaten einschlägig ist. Sicherheitshalber ist die Mehrheitsmeinung vorzuziehen, die für eine zehnjährige Aufbewahrungsdauer votiert. In der Praxis empfiehlt es sich, die Frist für die aus gesetzlichen Gründen 10 Jahren aufzubewahrenden Daten ab Beendigung des Arbeitsverhältnisses laufen zu lassen.

II. ÜBERWACHUNG DES ARBEITNEHMERS, INSBESONDERE E-MAIL MONITORING

lic. iur. Gili Fridland, LL.M.

1. PROLOG

Der Leser möge sich folgendes Szenario vorstellen:

Der Leser ist Geschäftsführer eines mittelgrossen Unternehmens, das bisher stets erfolgreich war. Der Geschäftsführer hat gerade erfahren, dass das Unternehmen einen ihrer grössten Kunden verloren hat. Der Verlust des Kunden ist nicht vom Unternehmen verschuldet, der Kunde wurde aufgekauft und die Käuferin hat Verträge mit anderen Lieferanten. Er ist dennoch nicht wieder rückgängig zu machen. Die Folge ist, dass das Unternehmen in naher Zukunft gezwungen sein wird, hinsichtlich der Belegschaft schmerzhafte Entscheide zu fällen, sprich: Entlassungen sind unvermeidlich. Diese Umstände sind noch streng geheim. Würde es allgemein bekannt, könnte die Position des Unternehmens im Markt einen noch grösseren Schaden annehmen. Selbst im eigenen Betrieb wissen nur eine Handvoll Eingeweihte, dass das Unternehmen schwierigen Zeiten entgegensieht.

Der Leser möge sich nun vorstellen, dass es Samstag ist und draussen die Sonne scheint. Der Geschäftsführer hat sich das Wochenende nach dieser äusserst stressreichen Woche redlich verdient. Nun sitzt er beim Brunch und schlägt die Zeitung auf – nur um den Namen seines Unternehmens in Grossbuchstaben zu sehen. Der dazugehörige Zeitungsartikel deutet finanzielle Schwierigkeiten des Unternehmens an und mutmasst über die Rettungsmassnahmen, die das Unternehmen planen könnte.

Was würde nun der Leser anstelle des Geschäftsführers tun? Natürlich fällt dieser erst mal aus allen Wolken! Aber, was dann? Eine der Prioritäten wird die Schadensbegrenzung sein. Eine weitere Priorität dürfte auch sein, herauszufinden, wer diese hochgeheimen Informationen verraten hat, um weitere Enthüllungen zu unterbinden.

2. EINLEITUNG

So ganz ohne Überwachung der Mitarbeitenden kommt keine Arbeitgeberin aus. In aller Regel akzeptieren umgekehrt auch die Mitarbeitenden, dass eine gewisse Überwachung stattfindet. Eine grosse Unsicherheit besteht dagegen in Bezug auf den Umfang und den Inhalt der Überwachung. Spätestens seit den Enthüllungen von Edward Snowden dürfte jedem klar geworden sein, dass die technischen Möglichkeiten der Überwachung den Rahmen des gesetzlich Erlaubten bei Weitem sprengen.

Geht die Arbeitgeberin jedoch mit der Überwachung zu weit und überschreitet sie die gesetzlichen Einschränkungen, so muss sie nicht nur mit zivilrechtlichen und strafrechtlichen Sanktionen rechnen, sondern möglicherweise auch mit Reputationsschäden.

Der vorliegende Beitrag fasst zunächst die grundsätzlichen Regeln zusammen, die es bei einer Überwachung zu beachten gilt. Danach befasst er sich mit dem konkreten Vorgehen beim E-Mail Monitoring. Zum Schluss betrachtet er das eingangs genannte Beispiel.

3. DIE GRÜNDE FÜR EINE ÜBERWACHUNG

Um es vorwegzunehmen: Gleichgültig, welche Überwachungsmethode angewendet wird – die reine Verhaltensüberwachung ist und bleibt unzulässig. Wenn also die Videokamera eingesetzt wird, um zu überprüfen, wer sich ständig bei der Kaffeemaschine aufhält und endlos Klatsch betreibt, befindet man sich schon im illegalen Bereich. Zulässig ist die Überwachung somit nur, wenn weitere objektiv nachvollziehbare Gründe vorliegen.

Die zulässigen Gründe für eine Überwachung sind sehr vielfältig. Zu denken ist etwa an die Qualitätssicherung, die Sicherheit von Personen oder Eigentum, die Gewährleistung der Infrastruktur oder die Sicherstellung des geordneten Geschäftsbetriebs. Die beispielhaft aufgeführten Gründe brauchen kaum erläutert zu werden.

Daneben gibt es besondere Situationen etwa im eingangs beschriebenen Fall, in dem sich ein Unternehmen mit Geheimnisverrat konfrontiert sieht. Situationen also, in denen der Verdacht entsteht, dass gesetzes- oder vertragswidrige Handlungen zum Schaden des Arbeitgebers begangen wurden.

4. DIE GRUNDREGELN

A. Die wichtigsten Regeln des Obligationenrechts

Im Arbeitsverhältnis wird das Recht der Arbeitgeberin zur Datenbearbeitung durch Art. 328b des Obligationenrechts konkretisiert. Danach darf die Arbeitgeberin nur Daten bearbeiten:

- soweit sie die Eignung der Arbeitnehmer für das Arbeitsverhältnis betreffen oder
- soweit sie zur Durchführung des Arbeitsvertrages erforderlich sind.

Die Art und Weise der Datenbearbeitung wird aber auch von den weiteren Pflichten und Rechten der Parteien bestimmt:

Art. 321d OR gewährt der Arbeitgeberin ein Weisungsrecht gegenüber ihren Mitarbeitenden. Das Weisungsrecht erlaubt es der Arbeitgeberin, die private Nutzung von Geschäftsmail und Internet zu regulieren. Die Mitarbeitenden sind verpflichtet, diese Weisungen zu befolgen.

Die Arbeitgeberin untersteht andererseits der Fürsorgepflicht. Diese besagt kurz gesagt, dass die Arbeitgeberin bei der Überwachung ihrer Mitarbeitenden fair vorzugehen hat. Die eingesetzten Überwachungsmethoden dürfen die Bewegungsfreiheit und Gesundheit der Mitarbeitenden möglichst wenig behindern. Ausgeschlossen ist somit die heimliche Überwachung. Die Fürsorgepflicht der Arbeitgeberin findet ihre Grenzen dort, wo die berechtigten Eigeninteressen der Arbeitgeberin tangiert sind.

Die Mitarbeitenden unterstehen schliesslich der Treuepflicht und haben alles zu unterlassen, was der Arbeitgeberin schaden könnte. Im Rahmen von Überwachungen bedeutet die Treuepflicht auch, dass Mitarbeitende die rechtmässige Überwachung nicht vereiteln dürfen. Im Ernstfall muss der Mitarbeitende der Arbeitgeberin Auskunft über Vorfälle im Betrieb erteilen. Ein Aussageverweigerungsrecht wie im Strafprozess existiert im Arbeitsrecht nicht. Die Treuepflicht findet ihre Grenze wiederum in den berechtigten Eigeninteressen des Mitarbeitenden.

Die Abwägung der Interessen von Arbeitgeberin und Mitarbeiter ist oft nicht ganz einfach. Es gilt, objektiv zu bleiben.

B. Die Regelung des Datenschutzgesetzes

Die Überwachung des Mitarbeiters ist eine Datenbearbeitung; folglich müssen auch die Regeln des Datenschutzes befolgt werden. Das bedeutet, dass die Grundsätze von Rechtmässigkeit, Zweckgebundenheit, Verhältnismässigkeit und Transparenz einzuhalten sind. Diese werden nachfolgend kurz umrissen:

- Rechtmässigkeit: Daten dürfen nur rechtmässig beschafft werden. D.h.: Daten dürfen nicht entgegen den Grundsätzen des Datenschutzgesetzes gesammelt oder bearbeitet werden. Insbesondere dürfen Daten nicht heimlich, durch Täuschung oder unter Zwang beschafft werden.
- Transparenz: Die Beschaffung und Bearbeitung von Daten hat stets nach Treu und Glauben zu erfolgen: Die betroffene Person muss wissen, dass und welche Daten über sie bearbeitet werden.
- Zweckgebundenheit: Personendaten dürfen sodann nur zum ursprünglich angegebenen Zweck bearbeitet werden. Dieser Zweck muss der betroffenen Person bei der Sammlung der Daten angegeben werden, aus den Umständen ersichtlich oder gesetzlich vorgesehen sein.
- Verhältnismässigkeit: Die Bearbeitung hat ausserdem verhältnismässig zu sein. Es dürfen nur so viele Daten wie nötig und nur so wenige wie möglich bearbeitet werden. Zugriff dürfen nur Personen haben, die diese Daten für ihre Arbeit wirklich benötigen. Nach Abschluss der Datenbearbeitung sind die Daten zu archivieren oder zu löschen. Wie viele Daten bearbeitet werden müssen, hängt nicht von der subjektiven Neugierde der Arbeitgeberin ab. Entscheidend sind objektive Gesichtspunkte.
- Schutzpflicht: Wer Daten bearbeitet, hat ausserdem geeignete technische und organisatorische Massnahmen zu treffen, um die Daten vor unbefugtem Bearbeiten zu schützen. Detaillierte Regelungen, vor welchen

Risiken die Daten zu schützen sind, befinden sich in der Verordnung zum Datenschutzgesetz.

- Richtigkeit: Der Dateninhaber muss sodann sicherstellen, dass die Daten richtig und aktuell sind. Die Aufnahme der richtigen Daten erleichtert auch dem Bearbeiter die Arbeit. Falsche Daten müssen korrigiert werden können.
- Erfordert das Bearbeiten von Daten eine Einwilligung, so gilt die Einwilligung nur dann als erteilt, wenn sie aufgrund einer angemessenen Information freiwillig erfolgt. Die Einwilligung muss sodann ausdrücklich erteilt werden, wenn besonders schützenswerte Personendaten bearbeitet werden.
- Eine besondere Informationspflicht besteht bei der Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen. Der Datenbearbeiter hat den betroffenen Personen bestimmte Mindestinformationen zukommen zu lassen, auch wenn er die Daten nicht bei ihnen beschafft hat. Die betroffene Person ist mindestens über den Inhaber der Datensammlung, den Zweck des Bearbeitens und die Kategorien der Datenempfänger zu orientieren. Ausnahmen von dieser Informationspflicht gelten nur in Ausnahmefällen.

In Situationen, wo diese Grundsätze durch die Überwachung verletzt werden könnten, braucht es eine Rechtfertigung. Rechtfertigungsgründe sind: Gesetzliche Vorschriften, ein überwiegendes privates oder öffentliches Interesse oder die Einwilligung des Betroffenen.

Der Arbeitsvertrag allein stellt grundsätzlich keine Rechtfertigung für eine Überwachung dar. Eine Rechtfertigung sind selbstverständlich gesetzliche Vorschriften, welche eine Überwachung vorschreiben. Solche Vorschriften gibt es namentlich in der Finanzbranche, wo es bestimmte Delikte zu verhindern gilt, z.B. Insiderhandel. In der Regel kann sich eine Arbeitgeberin aber nicht auf solche klare gesetzliche Vorschriften berufen. Stattdessen begründen aber häufig wichtige betriebliche Gründe ein überwiegendes privates Interesse der Arbeitgeberin.

Vorsicht: Die Einwilligung des Mitarbeiters sollte im Rahmen einer Überwachung nur mit grösster Zurückhaltung als Rechtfertigung herangezogen werden. Eine Einwilligung wird generell nur dann als ein Rechtfertigungsgrund in Betracht gezogen, wenn sie nach angemessener Information freiwillig erteilt wird. Im Arbeitsverhältnis wird gerade die Freiwilligkeit kritisch betrachtet. Je weiter die Überwachungsmassnahmen gehen, desto weniger sollte sich die Arbeitgeberin darauf verlassen, eine Einwilligung des Mitarbeitenden als Rechtfertigungsgrund heranziehen zu können.

Im Grundsatz gilt, dass die Arbeitgeberin bei Überwachungen auf sämtliche geschäftsbezogene Daten zugreifen kann, nicht aber auf private E-Mails des Mitarbeitenden. Hier ist Vorsicht geboten, weil die private Natur einer E-Mail

nicht immer einfach erkennbar ist, ganz besonders, wenn die E-Mail nicht entsprechend gekennzeichnet ist.

Die Ausgangslage ist aus datenschutzrechtlicher Sicht bedeutend einfacher, wenn die Arbeitgeberin den privaten Gebrauch der geschäftlichen E-Mail Adresse verbietet. Dann kann sie nämlich grundsätzlich davon ausgehen, dass sich in ihren Systemen keine privaten Dateien befinden. Das entspricht jedoch nicht der gängigen Praxis.

Wichtig ist eine klare Kommunikation darüber, was erlaubt ist und wie sich die Mitarbeitenden zu verhalten haben. Wichtig ist es, den Mitarbeitenden unmissverständlich mitzuteilen, dass es ihre Sache ist, ihre privaten E-Mails zu schützen, beispielsweise indem sie diese klar kennzeichnen, gesondert abspeichern oder – am besten – umgehend aus den Systemen der Arbeitgeberin entfernen.

5. DAS E-MAIL MONITORING

Nachdem nun die zahlreichen Regeln besprochen wurden, sollen die konkreten Schritte aufgezeigt werden, die es der Arbeitgeberin erlauben, die E-Mail Korrespondenz der Mitarbeitenden zu überwachen.

A. Definition

Zunächst gilt es klarzustellen, was mit E-Mail Monitoring überhaupt gemeint ist. E-Mail Monitoring bedeutet, dass die Arbeitgeberin Informationen darüber sammelt und auswertet, wie ihre Mitarbeitenden die E-Mail Systeme der Arbeitgeberin benutzen. Beim E-Mail Monitoring werden nicht die E-Mails der Mitarbeitenden gelesen, sondern die Randdaten dieser E-Mails erfasst, konkret also Informationen über Absender, Empfänger, Betreff, Datum, etc.

B. Vorgehen bei der Einführung

Es empfiehlt sich zunächst, technische und organisatorische Massnahmen zu prüfen, die eine Überwachung von Anfang an unnötig machen. Eine solche Massnahme wäre beispielsweise das Sperren des Zugriffs auf einschlägige Webseiten. Beim E-Mail System kann es auch bedeuten, dass bestimmte Kategorien von Mitarbeitenden gar nicht erst eine persönliche E-Mail Adresse erhalten, z.B. kundendienst@... oder IT-Support@... Auf solche funktionsbezogenen E-Mails kann die Arbeitgeberin jederzeit zugreifen.

Sodann gilt es, die Mitarbeitenden vorab über die Überwachung zu informieren. In diesem Zusammenhang empfiehlt es sich schon nur aus Verständnis- und Beweisgründen, ein Nutzungs- und Überwachungsreglement zu erlassen. Oder einfach ausgedrückt: Ohne ein solches Reglement ist ein zulässiges E-Mail Monitoring kaum möglich.

Ohne ein Nutzungs- und Überwachungsreglement müsste der eingangs erwähnte Geschäftsführer jetzt erst mal seine Mitarbeitenden darüber informieren, dass eine Überwachung stattfinden wird. Damit wird er aber die Aufklä-

rung der Frage, wer hochvertrauliche Informationen an die Presse verraten hat, wohl vereiteln.

Die Regeln der Nutzung und der Überwachung der E-Mail Systeme sind klar verständlich und angemessen detailliert zu erläutern. Verzichten Sie auf die Verwendung von generellen Floskeln und verharmlosenden Aussagen.

C. Auswertungsformen

Stets erlaubt sind anonyme Auswertungen der Randdaten. Hierbei handelt es sich um statistische Auswertungen der E-Mail Benutzung. Solche Auswertungen sind auch dann zulässig, wenn sie laufend erfolgen. Sodann gibt es die pseudonyme Auswertung, bei welchen bestimmten Personen oder Personengruppen Pseudonyme zugeteilt werden, die eine Identifikation verhindern. Der Identifikationsschlüssel, der es erlaubt, die Personen hinter den Pseudonymen zu identifizieren, muss natürlich streng vertraulich gehandhabt werden. Diese Auswertungsform darf ebenfalls systematisch durchgeführt werden. Die personenbezogene namentliche Auswertung ist dagegen nur stichprobeweise erlaubt oder dann, wenn ein konkreter Verdacht oder gar Gewissheit über einen Missbrauchtatbestand besteht.

6. DER ERNSTFALL

Wie soll nun unser Geschäftsführer vorgehen, um herauszufinden, wer hochvertrauliche Informationen an die Presse weitergegeben hat? Als Teil der Untersuchung bietet sich gewiss die Überprüfung der E-Mail Korrespondenz an.

Zunächst ist sorgfältig zu prüfen, ob ein konkreter und begründeter Verdacht über einen Missbrauch vorliegt. Ein solcher Verdacht darf nicht vorschnell angenommen werden. Nicht jeder Fehltritt eines Mitarbeitenden rechtfertigt den Zugriff auf sein E-Mail Konto. In Frage stehen muss eine Verletzung des Nutzungsreglements, des Arbeitsvertrags oder des Gesetzes. Aus unserer Erfahrung lohnt es sich, die Verdachtsmomente sauber zu dokumentieren. Unser Geschäftsführer dürfte keine Probleme haben, die Verdachtsmomente zu benennen.

Bei aller Dringlichkeit und Aufregung, die sich in solchen Situationen meistens einstellen, ist unserem Geschäftsführer zu raten, das Monitoring sorgfältig vorzubereiten. Bereits vor Beginn des Monitoring ist ein klar definierter Suchplan festzulegen. Im Suchplan wird festgelegt, was der Gegenstand und die Ziele der Untersuchung sind, welche Personen in das Monitoring einzubeziehen sind, welche Absender, Empfänger und Stichworte relevant und welche Stichworte ausdrücklich von der Suche auszunehmen sind. Der Suchplan hat vorzugsweise flexibel zu bleiben und muss laufend angepasst werden. Eine sorgfältige Dokumentation des Monitoring ist somit unerlässlich.

Aus datenschutzrechtlicher Sicht empfiehlt es sich, mit engen Suchläufen zu beginnen und diese erst in einem zweiten Schritt auszudehnen, wenn keine oder nur unbefriedigende Resultate erzielt werden. Im Fall unseres Geschäftsführers würde es sich etwa anbieten, zuerst nur nach E-Mails zu suchen, die

an die betreffende Zeitung oder an den verantwortlichen Redaktor dieser Zeitung gerichtet waren.

Schliesslich gilt es, die Resultate, welche das Monitoring hervorbringt, sorgfältig zu analysieren. Dabei ist äusserst wichtig, die Fakten bei der Auswertung streng objektiv zu betrachten.

7. SCHLUSSWORT

Zusammengefasst empfiehlt es sich immer, klare Regelungen aufzustellen und diese transparent zu kommunizieren.

Im Ernstfall sollten ein Monitoring immer gut vorbereitet und die Ergebnisse objektiv betrachtet werden.

Im manchmal verwirrenden Wust der geltenden Gesetze und Regelungen kann es hilfreich sein, sich immer wieder selber die Testfrage zu stellen, ob man als Betroffener es zulassen würde, dass ein Dritter mit den eigenen Personendaten in der fraglichen Art umgeht.

III. AUSTAUSCH VON PERSONALDATEN IM IN- UND AUSLAND

Dr. iur. Conradin Cramer, LL.M.

1. WAS IST BEI DER WEITERGABE VON PERSONALDATEN AN DRITTE IM INLAND ZU BEACHTEN?

Datenauslagerung entspricht einem praktischen Bedürfnis: Unternehmen lassen zum Beispiel die Bearbeitung von Spesenbelegen oder die Erstellung der Lohnabrechnungen durch Dritte besorgen. Gründe für ein solches klassisches "Outsourcing" sind in der Regel Kostenersparnis, Effizienzgewinn und Qualitätssteigerung.

Dritte im Sinne des Datenschutzrechts sind allerdings nicht nur "fremde" Dienstleister. Als Dritte gilt jede nicht mit der Arbeitgeberin identische Person. Auch die Datenübertragung im Konzern an eine Mutter-, Schwester- oder Tochtergesellschaft – zum Beispiel zur Führung eines konzernweiten Mitarbeiterverzeichnisses – gilt als Weitergabe von Personaldaten an Dritte.

Der Begriff der *Weitergabe* von Daten ist weit auszulegen: Bereits die blosse Zugangsgewährung gilt als Weitergabe, d.h. es genügt, dass der Dritte die Möglichkeit hat, auf Daten in der Schweiz zuzugreifen. Dies gilt unabhängig davon, ob der Dritte von dieser Möglichkeit Gebrauch macht.

Die Weitergabe von Daten an Dritte ist aus Sicht des Datenschutzrechts grundsätzlich zulässig, sofern die folgenden Voraussetzungen erfüllt sind:

- *Es bestehen keine gesetzlichen oder vertraglichen Geheimhaltungspflichten*: Bei Personaldaten bestehen grundsätzlich keine gesetzlichen Geheimhaltungspflichten und arbeitsvertragliche Datenweitervergabeverbote gibt es kaum je.
- *Die Arbeitgeberin muss und kann gewährleisten, dass die Daten beim Dritten sicher sind*: Die Arbeitgeberin muss sich vergewissern, dass der Dritte die gleiche Datensicherheit gewährleistet, wie die Arbeitgeberin es selbst müsste.
- *Es liegt kein Verstoss gegen die allgemeinen Datengrundsätze vor*: Die Daten müssen rechtmässig beschafft worden sein, also nicht etwa durch Täuschung oder unter Zwang (Rechtmässigkeit). Die Mitarbeiter müssen wissen, dass und welche Daten über sie bearbeitet werden (Transparenz). Die Daten müssen aktuell und dürfen nicht wissentlich falsch sein (Richtigkeit). Die Daten dürfen nur zum ursprünglich mitgeteilten Zweck bearbeitet werden (Zweckgebundenheit). Es dürfen nur so viele Daten

bearbeitet werden, wie es für den konkreten Zweck erforderlich ist (Verhältnismässigkeit).

Unter diesen Voraussetzungen ist die Datenbearbeitung durch einen Dritten zulässig – aber nur in demjenigen Umfang, in dem die Arbeitgeberin die Daten selbst bearbeiten dürfte (sogenannte *Auftragsdatenbearbeitung*).

Zu beachten ist also immer, was der Datenempfänger mit den Personendaten tut: Sobald der Dritte mit der Datenbearbeitung auch eigene Interessen oder Interessen von anderen Konzerngesellschaften verfolgt, liegt nicht mehr nur eine reine Auftragsdatenbearbeitung vor. In diesem Fall gilt der Dritte als neuer *Dateninhaber*. Die Datenbearbeitung durch den Dritten als neuen Dateninhaber bedarf eines Rechtfertigungsgrunds. Verlangt sind eine angemessene Information des Mitarbeiters und seine klare, aktuelle und konkrete Einwilligung.

Vieles, was innerhalb eines Konzerns auf den ersten Blick nach Auftragsdatenbearbeitung aussieht, entpuppt sich bei näherer Prüfung als Weitergabe an einen neuen Dateninhaber. Oft werden nämlich zusätzlich zur möglichst effizienten Datenbearbeitung auch weitere Ziele verfolgt, wie etwa ein Abgleich der Kosten innerhalb des Konzerns. Schon wenn Daten für ein konzernweites Mitarbeiterverzeichnis weitergegeben werden, erfolgt die Datenbearbeitung nicht nur im Interesse der schweizerischen Arbeitgeberin, sondern auch im Interesse anderer Konzerngesellschaften.

Ob jemand als Dateninhaber oder als Auftragsdatenbearbeiter gilt, ist auch deshalb relevant, weil dem Inhaber einer Datensammlung im Gegensatz zum Auftragsdatenbearbeiter verschiedene datenschutzrechtliche Sonderpflichten (Informations-, Anmelde- und Auskunftspflichten) auferlegt werden. Ausserdem kann die regelmässige Weitergabe an neue Dateninhaber – anders als die regelmässige Weitergabe von Daten an Auftragsdatenbearbeiter – eine Pflicht zur Registrierung der Datensammlung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auslösen.

Sofern verhindert werden soll, dass der Dritte neuer Dateninhaber wird bzw. die weitergegebenen Personaldaten auch im eigenen Interesse nutzt, empfiehlt sich eine Absicherung der Auftragsdatenbearbeitung im Vertrag mit dem Dritten. Eine solche Vertragsklausel kann beispielsweise wie folgt lauten:

> *Der Datenbearbeiter verpflichtet sich, (i) die erhaltenen Personendaten nur für die Zwecke des Auftraggebers und nur wie vom Auftraggeber angeordnet zu verwenden; und (ii) alle vom Auftraggeber erhaltenen Personendaten sowie alle Bearbeitungen davon auf schriftliche Aufforderung des Auftraggebers nach Wahl des Auftraggebers sofort und vollständig an diesen zurück zu geben oder zu löschen und die vollständige Rückgabe oder Löschung dem Auftraggeber schriftlich zu bestätigen.*

Das Vorschlagen einer solchen Vereinbarung über die Auftragsdatenbearbeitung ist ein guter Test dafür, ob der Dritte sich wirklich mit der Rolle als Auf-

tragsdatenbearbeiter begnügt oder ob er nicht vielleicht doch beabsichtigt, die Daten auch für eigenen Zwecke zu nutzen. Sperrt sich der Dritte gegen eine Pflicht zur sofortigen und vollständigen Rückgabe aller Daten, verfolgt er vermutlich mit diesen Daten auch noch weitere, eigene Zwecke.

2. ZUSÄTZLICHE VORAUSSETZUNGEN DER DATENÜBERTRAGUNG AN DRITTE IM AUSLAND

Sofern sich die Personalverwaltung eines Konzerns im Ausland befindet, müssen Personaldaten aus der Schweiz exportiert werden. Selbstverständlich lässt sich mit der Auslagerung einer Datenbearbeitung ins Ausland die Anwendung des Schweizer Datenschutzgesetzes nicht umgehen. Der Begriff der Datenbearbeitung ist sehr weit gefasst und schliesst jeden Umgang mit Personendaten ein.

Eine Weitergabe von Daten ins Ausland ist nur dann zulässig, wenn die Persönlichkeit des betroffenen Mitarbeiters nicht schwerwiegend gefährdet ist. Eine solche Gefährdung liegt vor, wenn Personendaten in ausländische Staaten bekannt gegeben werden, deren Datenschutzregulierung nach schweizerischen Standards ungenügend ist. Bei grenzüberschreitenden Datenbearbeitungen ist deshalb zu klären, ob ein angemessener Datenschutz im Empfängerstaat gewährleistet ist. Der EDÖB veröffentlicht eine Liste der wichtigsten Staaten, in der er deren Datenschutz-Gesetzgebung würdigt (http:// www.edoeb.admin.ch). Falls der EDÖB einem Staat einen angemessenen Schutz zuspricht, ist der Export von Daten ins Ausland grundsätzlich erlaubt. Ist hingegen der angemessene Schutz nicht gewährleistet, ist eine Datenbekanntgabe grundsätzlich rechtswidrig. Keinen ausreichenden Datenschutz gewähren China, Russland, Länder in Afrika und insbesondere auch die USA.

Unter den folgenden Bedingungen ist die Bekanntgabe von Personaldaten ins Ausland trotz grundsätzlich mangelhafter Datenschutzregelung im Ausland zulässig:

- Die Bekanntgabe erfolgt zwischen juristischen Personen unter einheitlicher Leitung (Konzerne) mit *konzernweiten Datenschutz-Regeln*. Diese konzerninterne Regelung ist dem EDÖB zur Kenntnis zu bringen.
- In einem *Datenbearbeitungsvertrag* zwischen dem schweizerischen Datenexporteur und dem ausländischen Datenbearbeiter ist ein angemessenes Datenschutzniveau vereinbart.
- Der Mitarbeiter hat im konkreten Einzelfall der Datenbearbeitung *zugestimmt* und dem Mitarbeiter ist bewusst, dass die Daten im Ausland einem geringeren Schutzniveau unterstehen. Zu beachten ist, dass der Mitarbeiter seine Einwilligung jederzeit gültig widerrufen kann.
- Die Daten werden an einen Datenbearbeiter in den USA exportiert, der sich dem "*Safe-Harbor*-Übereinkommen" unterworfen hat. Die Schweiz vereinbarte mit den USA ein Rahmenübereinkommen zum personenbezogenen Datentransfer aus der Schweiz in die USA. US-amerikanische

Unternehmen können sich diesem Übereinkommen unterstellen und sich verpflichten, für aus der Schweiz übermittelte Daten den schweizerischen Bedürfnissen genügende Datenschutzregeln anzuwenden. Es gibt eine öffentlich zugängliche Liste der "International Trade Administration", die alle US-amerikanischen Unternehmen aufführt, die sich dem Safe-Harbor-Übereinkommen unterworfen haben (abrufbar unter https://safeharbor.export.gov/swisslist.aspx).

Häufig wollen internationale Konzerne nicht nur Daten von Mitarbeitern, sondern auch *Dossiers von Stellenbewerbern* international austauschen. Konzerne haben häufig das Bedürfnis, Bewerbungsdossiers, die einer Landesgesellschaft zugestellt werden, auch anderen Gruppengesellschaften zugänglich zu machen. Bei Kaderpositionen entscheidet nicht selten die Konzernleitung im Ausland bei der Selektion des Personals der schweizerischen Ländergesellschaft mit.

Das Bewerbungsdossier enthält klarerweise Personendaten. In der Regel beinhaltet das Dossier einen ausführlichen Lebenslauf mit Ausbildungs- und Arbeitszeugnissen. Solche Unterlagen erlauben eine Beurteilung wesentlicher Aspekte der Persönlichkeit des Stellenbewerbers und stellen ein Persönlichkeitsprofil im Sinn des Datenschutzgesetzes dar, für das besondere Schutzbestimmungen anwendbar sind.

Ein Stellenbewerber, der eine Bewerbung auf ein Stelleninserat hin oder im Rahmen einer Blindbewerbung einreicht, muss grundsätzlich nicht davon ausgehen, dass eine Konzerngesellschaft im Ausland sein Dossier bearbeitet. Konzerngesellschaften, die Informationen über Stellenbewerber anderen Konzerngesellschaften zugänglich machen, müssen in einem ersten Schritt die ausdrückliche Einwilligung der Stellenbewerber einholen. Die Einwilligung ist nur gültig, wenn sie nach angemessener Information freiwillig erfolgt. Die Stellenbewerber müssen mindestens darüber informiert werden, welche Daten zu welchem Zweck ins Ausland weitergeleitet werden.

Bei Online-Bewerbungen empfiehlt sich die Verwendung einer klaren Datenschutzerklärung. Die Webseite ist sinnvollerweise so zu konzipieren, dass eine Bewerbung nur dann abgeschickt werden kann, wenn der Bewerber sein Einverständnis zur Weitergabe der Daten unmissverständlich zum Ausdruck gebracht hat. Dazu genügt es, dass der Bewerber eine entsprechende Einverständniserklärung anklickt, also ein "Häkchen" setzt. Muss sich der Bewerber registrieren, um seine Bewerbung eingeben zu können, so sollte das Einverständnis zur Datenschutzerklärung bereits bei der Registrierung eingeholt werden. Für "analoge" Bewerbungen muss es genügen, wenn im Stelleninserat unmissverständlich auf die Datenweitergabe hingewiesen wird und der Bewerber sich in seiner Bewerbung auf das Stelleninserat bezieht. Gerade bei Blindbewerbungen per Post ist das Einverständnis aber nach Eingang der Bewerbung separat einzuholen, bevor die Daten ins Ausland weitergeleitet werden.

3. WANN BESTEHT EINE REGISTRIERUNGSPFLICHT DER ARBEITGEBERIN BEIM EDÖB?

Unternehmen müssen ihre Datensammlungen beim EDÖB anmelden, wenn sie regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten. Personaldossiers gelten zwar als Persönlichkeitsprofile und enthalten nicht selten auch besonders schützenswerte Personendaten (wie etwa Arztzeugnisse oder Strafregisterauszüge). Dennoch führen Personaldossiers nicht zu einer Registrierungspflicht: Das Datenschutzgesetz entbindet von der Registrierungspflicht, wenn Daten aufgrund einer gesetzlichen Verpflichtung gesammelt werden. Eine solche gesetzliche Verpflichtung erstreckt sich zum Beispiel auf alle Daten, die zur Erstellung eines Arbeitszeugnisses verwendet werden. Das führt dazu, dass Personaldossiers nicht zu einer Registrierungspflicht führen. Der EDÖB hat das Bestehen dieser Ausnahme in einem Merkblatt bestätigt.

Eine Registrierung beim EDÖB ist auch erforderlich, wenn regelmässig Personendaten an Dritte bekannt gegeben werden. Keine Registrierungspflicht besteht immerhin dann, wenn Daten *nur zur Auftragsdatenbearbeitung* weitergegeben werden, der Dritte die Daten also lediglich gemäss Instruktionen so bearbeitet, wie es die Arbeitgeberin als Dateninhaberin selbst auch tun dürfte.

Ferner besteht keine Registrierungspflicht, wenn ein Unternehmen eine formelle *Datenschutzzertifizierung* erworben hat. Eine solche Zertifizierung haben aktuell erst ganz wenige Schweizer Unternehmen erworben. Wir erachten diese Möglichkeit deshalb als wenig praxisrelevant und verzichten auf weitere Informationen dazu.

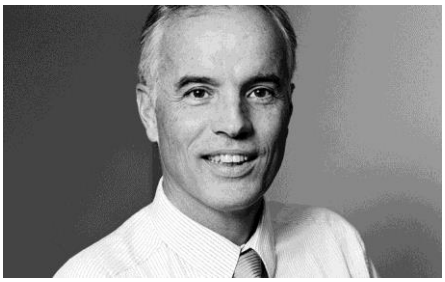
Unternehmen, die regelmässig Personaldaten an Dritte (insbesondere an Konzerngesellschaften) über die reine Auftragsdatenbearbeitung hinaus weitergeben, steht eine weitere Möglichkeit offen, sich von der Registrierungspflicht zu entbinden: Keine Registrierungspflicht besteht, wenn ein Unternehmen einen *internen Datenschutzverantwortlichen* ernennt und dies dem EDÖB mitteilt. Mehr als 800 Schweizer Unternehmen haben diese Lösung gewählt. Der EDÖB veröffentlicht auf seiner Webseite (http://www.edoeb.admin.ch) ein Verzeichnis der Unternehmen, die einen Datenschutzverantwortlichen einsetzen und somit von der Registrierungspflicht befreit sind. Wir erachten die Einsetzung eines internen Datenschutzverantwortlichen als sinnvoll und empfehlen dies grundsätzlich jedem Unternehmen.

Der Datenschutzverantwortliche kann ein Mitarbeiter oder ein Dritter (natürliche oder juristische Person im Auftragsverhältnis) sein. Er muss über die nötigen Fachkenntnisse verfügen, wobei Grundkenntnisse im Datenschutzrecht und die Vertrautheit mit der Organisation der Arbeitgeberin grundsätzlich genügen. Der Datenschutzverantwortliche muss so geschult sein, dass er sich mindestens selbständig ein Bild darüber machen kann, ob und inwieweit eine Datenbearbeitung geeignet ist, die Persönlichkeit einer Person zu verletzen. Der EDÖB empfiehlt, dass nicht juristisch ausgebildete Datenschutzverantwortliche wenigstens ein halbes Jahr im Bereich Datenschutz gearbeitet ha-

ben. Der Datenschutzverantwortliche muss seine Aufgabe fachlich weisungsunabhängig ausführen und direkt Kenntnis von allen Datenbearbeitungen erhalten. Um die organisatorische Unabhängigkeit sicherzustellen, darf der Datenschutzverantwortliche keine andere Tätigkeit ausüben, die mit seiner Funktion unvereinbar ist, wie z.B. in der Informationssystemverwaltung oder der Personalführung. Am besten eignen sich deshalb Personen aus der IT-Abteilung, der Rechtsabteilung oder des Risk Managements. Die Funktion des Datenschutzverantwortlichen kann auch von einem Mitarbeiter einer ausländischen Konzerngesellschaft übernommen werden, sofern dieser in der Lage ist, sich mit der Datenbearbeitung und der datenschutzrechtlichen Situation in der Schweiz vertraut zu machen.

ANSPRECHPARTNER

Am Standort Zürich



Felix C. Meier-Dieterle
fmd@vischer.com

Barbara Meyer
barbara.meyer@vischer.com

Am Standort Basel

Gili Fridland Svensson, LL.M.
gfridland@vischer.com

Dr. Conradin Cramer, LL.M.
ccramer@vischer.com