ZIK

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Datenschutz-Managementsysteme im Aufwind?

Schulthess §

62

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Datenschutz-Managementsysteme im Aufwind?

Schulthess § 2016

62

Das 1998 geschaffene «Zentrum für Informations- und Kommunikationsrecht» an der Rechtswissenschaftlichen Fakultät der Universität Zürich (Lehrstuhl Prof. Dr. Rolf H. Weber, Rämistrasse 74, 8001 Zürich) dient als Forschungsstelle sowie als Anlauf- und Kontaktstelle für an diesem Rechtsgebiet interessierte Personen und Gruppen.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7255-7469-8

www.schulthess.com

Inhaltsverzeichnis

DAVID ROSENTHAL*

Datenschutz-Compliance im Unternehmen: Eine etwas andere Anleitung …[1]

Inhaltsverzeichnis

I. Ausgangslage

Es gibt niemanden in der Schweiz, der den Datenschutz vollumfänglich einhält, nicht einmal der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte. Das ist auch gar nicht möglich, doch mehr dazu später. Angesichts der wachsenden Bedeutung und Präsenz dieses Themas in der Öffentlichkeit und angesichts der wachsenden Sanktionsrisiken – die kommende Datenschutz-Grundverordnung der EU (DSGV) lässt grüssen – nimmt das Interesse an Datenschutz-Compliance allerdings laufend zu, ganz besonders in der Wirtschaft. Denn bei den meisten Unternehmen ist es darum nicht gut bestellt, und die verantwortlichen Personen wissen das auch.

---

* Lic. iur., Konsulent in einer Wirtschaftskanzlei in Zürich, Lehrbeauftragter an der Eidg. Technischen Hochschule Zürich und Universität Basel, Sekretär des Vereins Unternehmens-Datenschutz (VUD).

1 Dies ist die schriftliche Fassung eines Vortrags des Autors vom 28. Oktober 2015.

Jeder kann mit den folgenden zwölf Fragen den Selbsttest machen:

1. Sind bei Ihnen alle Datensammlungen und Bearbeitungsverfahren sauber dokumentiert?
2. Haben Sie überall dort, wo Daten bearbeitet werden, eine für den Datenschutz verantwortliche Person mit entsprechendem Know-how und Ressourcen?
3. Sind alle grenzüberschreitenden Datenflüsse in Länder ohne angemessenen Datenschutz vertraglich oder analog abgesichert, auch konzernintern?
4. Sind alle konzerninternen und -externen Auftragsdatenbearbeitungen vertraglich geregelt?
5. Ist jede relevante Datenbearbeitung durch eine passende Weisung geregelt?
6. Sind die Massnahmen zur Sicherstellung der Datensicherheit im Betrieb auf dem Stand der Technik?
7. Sind alle Mitarbeiter in Sachen Datenschutz ausgebildet und sensibilisiert?
8. Wird die Einhaltung der erforderlichen Datensicherheit und der Bestimmungen des Datenschutzes intern und von extern überprüft?
9. Sind alle nötigen Meldungen und Registrierungen erfolgt und alle Bewilligungen eingeholt?
10. Sind alle Datenbearbeitungen, wo erforderlich, transparent kommuniziert?
11. Verfügen alle Verträge mit Dritten über angemessene Datenschutzklauseln?
12. Sind alle Prozesse zur Sicherstellung des Datenschutzes definiert, insbesondere bezüglich der Rechte der betroffenen Personen, bezüglich neuer Projekte, bezüglich Verträge mit Providern und für den Fall von Data Breaches?

Die Frage 6 werden viele Unternehmen erfahrungsgemäss mit mehr oder weniger gutem Gewissen mit Ja beantworten können. Bei den Fragen 9, 10 und 11 werden manche Unternehmen mindestens teilweise positiv antworten können. In allen anderen Punkten wird die Mehrheit der Unternehmen nach meiner Erfahrung passen müssen. Das mag erschreckend erscheinen, wird so manche Leser meines Beitrags aber zugleich beruhigen, weil es bedeutet, dass es vielen so ergeht. Und geteiltes Leid ist halbes Leid. Datenschutz wird vielerorts nach wie vor *ad-hoc* betrieben. Nach meiner Erfahrung aus der Beratung ist das selbst in manchen internationalen Grosskonzernen über weite

Strecken noch so. Ein koordiniertes, langfristig angelegtes und flächendeckendes Vorgehen zur Sicherstellung von Datenschutz-Compliance fehlt häufig. Ein Grund dafür ist, dass bislang andere Themen wie Massnahmen zur Einhaltung des Kartellrechts oder zur Verhinderung von Korruption mehr Gewicht hatten und die Ressourcen belegten. In regulierten Branchen wie etwa der Finanzindustrie gibt es Themen, die das Kerngeschäft wesentlich fundamentaler betreffen als der Datenschutz und daher die volle Aufmerksamkeit des Managements erfordern. Damit will ich den Datenschutz nicht abwerten, aber wenn sich ein Unternehmen in Bezug auf seine Datenbearbeitung einigermassen "anständig" und transparent verhält und nicht mehr als das tut, was alle anderen auch tun, waren die Datenschutzrisiken bisher *de facto* beschränkt. Bisher jedenfalls.

Doch auch im Datenschutz ändern sich die Zeiten. Die Regulierung nimmt massiv zu, die Risiken ebenfalls, und zwar nicht nur wegen der neuen Bussen für Datenschutzverstösse, die in einigen Jahren auch in der Schweiz eingeführt werden (die Schweiz wird dazu völkerrechtlich verpflichtet werden, um weiterhin als Land mit angemessenem Datenschutz gelten zu können). Ein Beispiel ist die DSGV mit ihren 91 Artikeln, die auch von vielen Unternehmen in der Schweiz zu beachten sein wird, weil sie – grob gesagt – nicht nur Datenbearbeitungen auf dem Territorium der EU erfasst, sondern Datenbearbeitungen weltweit, sobald sie auch Bürger der EU in relevanter Weise betreffen.

In der Praxis werde ich von Unternehmen oft gebeten aufzuzeigen, was sie tun müssen, um datenschutzkonform oder eben neu-deutsch "compliant" zu werden, und zwar ohne, dass diesbezüglich nennenswerte Vorarbeiten bestehen würden, auf denen aufgebaut werden kann. Die übliche Erwartung an diesem Punkt ist dann jeweils, dass hierzu einige Weisungen und Reglemente verfasst werden müssen, der eine oder andere Prozess zu definieren ist und vielleicht die Datenschutzklauseln auf der Website und in gewissen Verträgen anzupassen sind.

Doch so einfach ist das leider nicht. Im Gegensatz zu anderen Themen wie etwa der Korruptionsbekämpfung spielt der Datenschutz in so gut wie *jedem* Bereich des Unternehmens eine Rolle, betrifft so gut wie *jeden* Prozess und *jede* IT-Anwendung, die ein Unternehmen einsetzt, denn überall dort, wo personenbezogene Daten bearbeitet werden, ist auch Datenschutz zu beachten. Und schon an dieser Stelle bricht die Hoffnung auf eine rasche Lösung des Problems meist ein: Die meisten Unternehmen wissen gar nicht, welche

Daten sie wo, wie und vielleicht auch warum bearbeiten, oder genauer gesagt: Irgendjemand weiss es im Betrieb zwar immer, aber eben nur irgendjemand. Einen Plan gibt es nicht.

Nun könnte ich in solchen Fällen einen umfangreichen Aktionsplan vorlegen, ein komplexes Netz an Massnahmen vorschlagen, mit dem Ziel, ein Unternehmen "compliant" zu machen. Doch weder würde ich (und die im Unternehmen zur Umsetzung zuständigen Stellen) das Budget hierfür erhalten, noch wäre das Unternehmen bereit, sich derart umfassend neu zu erfinden, "nur" um den Datenschutz einzuhalten. Die Übung wäre von vornherein zum Scheitern verurteilt.

So habe ich im Laufe der Jahre eine andere Vorgehensweise entwickelt, die wesentlich erfolgsversprechender ist, weil sie darauf ausgerichtet ist, wie Unternehmen und ihre Entscheidungsträger tatsächlich funktionieren und wozu sie bei allem guten Willen tatsächlich in der Lage sind. Diese Vorgehensweise besteht aus sechs Schritten, die nachfolgend erläutert werden. Allerdings möchte ich an dieser Stelle warnen: Meine Aussagen mögen den einen oder anderen provozieren, unkonventionell oder gar befremdlich erscheinen, und sie entsprechen nicht der üblichen Rhetorik von Management-Beratern und Unternehmensanwälten. Aber das Feedback, das ich erhalte, bestätigt mich, die Dinge beim Namen zu nennen und denen, die sich unternehmensintern für mehr Mittel zur Einhaltung des Datenschutzes einsetzen, eine praktische Hilfe zu bieten.

II. Sechs Schritte zur Datenschutz-Compliance im Unternehmen

A. Schritt 1: Für Demut sorgen

Ich habe es bereits erwähnt: Niemand kann die Anforderungen des Datenschutzes vollständig erfüllen. Die Regeln des Datenschutzes sind zu kompliziert, zu vielschichtig. Zwar lässt sich das heutige Datenschutzgesetz so anwenden, dass sich konkrete Fälle vernünftig lösen lassen. Aber dabei sind so viele Parameter zu berücksichtigen und so viele Abwägungen zu treffen, dass es unmöglich ist, dies andauernd zu tun.

Der Datenschutz betrifft wie erwähnt alle Bereiche eines Unternehmens, weil in der Regel überall Personendaten bearbeitet werden (wozu in der Schweiz

ja auch Daten über andere Unternehmen zählen, sofern ermittelt werden kann, um welche Unternehmen es sich handelt). Daher kann ein Unternehmen mit den Anforderungen des Datenschutzes nur dann einigermassen zu Recht kommen, wenn es alle – wirklich alle – Prozesse einzeln durchdefiniert und im Hinblick auf den Datenschutz anpasst und für die Durchsetzung der definierten Prozess sorgt. Aber das ist so aufwendig, dass es kaum ein Unternehmen tun wird, ohne sich dem Vorwurf auszusetzen, Datenschutz als Selbstzweck zu betreiben oder es schlicht zu *über*treiben, indem es vor lauter Bäumen den Wald nicht mehr sieht.

Auch Datenschutz-Compliance ist ein Gebiet, in welchem *Risikoentscheide* erforderlich sind, d.h. eine Fokussierung der Ressourcen und Compliance auf jene Dinge, die wichtig sind und dem Unternehmen, seine Mitarbeiter oder Dritte wirklich schaden können. Viele Datenschutzverstösse im Alltag sind – bei gesundem Menschenverstand betrachtet – von untergeordneter Relevanz.

Hinzu kommt, dass die rechtsanwendenden Behörden – insbesondere der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte und die Gerichte – jedenfalls in der Schweiz manche Entscheide zur Umsetzung des Datenschutzgesetzes rein ergebnisorientiert und unabhängig davon treffen, was das Gesetz wirklich vorsieht. Sie mögen damit oftmals auch keine Falschen treffen und "gefühlt" richtig entscheiden. Weil diese Entscheide aber in der Folge auf eine Art und Weise begründet werden, die weder konsistent noch gesetzeskonform ist, werfen sie für den Datenschutzrechtler, der es richtig machen will, mehr Fragen auf, als sie lösen. Sie stellen die Systematik des Datenschutzgesetzes kurzerhand auf den Kopf und sorgen dementsprechend für Rechtsunsicherheit, weil auf Basis des Gesetzes nicht mehr vorhersehbar ist, wie die Gerichte entscheiden werden.

Als Beispiel sei hier nur ein Entscheid des Obergerichts Zürich vom März 2015 erwähnt, der wohl aus falschverstandenen Gründen der Einzelfallgerechtigkeit das Auskunftsrecht nach Art. 8 DSG für Dokumente bejahte, die gar keine Personendaten enthalten (vgl. dazu David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 592). Der Entscheid führte selbst bei hartgesottenen Datenschützern für Kopfschütteln und Erklärungsnöte, trug und trägt aber mit dazu bei, dass die Datenschützer in den Unternehmen nicht mehr verstehen, was denn nun dem Auskunftsrecht unterliegen soll und was nicht. Mit dem ursprünglichen Sinn und Zweck von Art. 8 DSG haben dieser und diverse andere Entscheide – auch des Bundesgerichts – längst nichts mehr zu tun.

Entsprechend ratlos lassen sie in den Unternehmen jene zurück, die sich um die Einhaltung des Datenschutzes kümmern sollen.

Doch um ein Unternehmen – oder genauer: dessen Management – dazu zu bringen, der Datenschutz-Compliance die nötige Aufmerksamkeit zu widmen, muss diese Realität für den Moment zurückstehen; sie hätte den gegenteiligen Effekt, nämlich dass die Entscheidungsträger in ihrem Gefühl bestärkt würden, Compliance im Bereich Datenschutz sei eine derart diffuse Sache, dass sie ohne Weiteres zur Klärung zurückgestellt werden könne. Oder aber: Im Datenschutz ist nach wie vor alles grau, und grau ist nicht verboten.

Wichtiger ist es stattdessen, in einem ersten Schritt eine *gesamtheitliche* Wahrnehmung der "Missstände" des Unternehmens im Bereich Datenschutz herzustellen. Die zwölf Fragen im Eingang zu diesem Beitrag eignen sich bestens dafür. Jedes "Nein" ist ein datenschutzrechtliches Compliance-Defizit. Wenn Sie sich für mehr Compliance im Datenschutz einsetzen wollen, müssen Sie zuerst aufzeigen, dass es – wie es regelmässig der Fall sein wird – nicht nur an einigen kleinen Dingen fehlt, sondern die Datenschutz-Compliance in ihrem Grundsatz nicht gewährleistet ist. Sinn und Zweck dieser Übung ist vor allem eines: Den Entscheidungsträgern die Erkenntnis vermitteln, dass das Unternehmen in Sachen Datenschutz-Compliance noch so gut wie *nichts* erreicht hat, ganz unten ist, es ganz schlecht darum steht. In einem ersten Schritt müssen Sie mit anderen Worten für die nötige Demut sorgen. Die Botschaft soll also sein: Es geht nicht nur um Retuschen, etwas Optimierung hier und da, sondern es sind fundamentale Anpassungen nötig, um den gesetzlichen Vorgaben zu entsprechen.

Hierbei hilft es erfahrungsgemäss, dass die Entscheidungsträger überhaupt verstehen, worum es beim Datenschutz geht (nämlich eine Rechtspflicht mit ganz konkreten Vorgaben) und realisieren, wie viele Bereiche des Unternehmens davon wirklich betroffen sind (nämlich alle). Hierzu sind keine langen Ausführungen nötig und das Rad muss auch nicht neu erfunden werden. So gibt es im Internet zum Beispiel diverse, ausgezeichnet aufgemachte Video-Tutorials, die auch einem Laien in wenigen Minuten die Essenz des Datenschutzes vermitteln können, ohne sie zu langweilen (Beispiel: http://bit.ly/1KouAXr).

Ist diese Essenz klar, ist es erfahrungsgemäss sinnvoll aufzuzeigen, dass Datenschutz-Compliance sich im Wesentlichen mit drei Bereichen auseinandersetzen muss, damit sich die Entscheidungsträger der Vielschichtigkeit der

Angelegenheit bewusst werden – auch dies mit dem Ziel, für die nötige Demut gegenüber der Herausforderung zu sorgen:

1. Formale Erfordernisse: Gemeint sind Notifikationen und Registrierungen bei Behörden, aber auch Verträge, die zur Sicherstellung des Datenschutzes abgeschlossen werden müssen.
2. Materielle Restriktionen: Hier geht es darum, wer welche Daten wie und wann bearbeiten darf, also um die Anforderungen in der Sache. Gemeint sind Regeln wie der Zweckbindungsgrundsatz, das Gebot der Verhältnismässigkeit und der Transparenz.
3. Governance: Hierbei geht es um Vorkehrungen, mit welchen die materiellen und formalen Anforderungen sichergestellt werden. Gemeint sind Massnahmen wie der Erlass von Richtlinien, Schulungen, Dokumentation, Regeln wie "Privacy by Default", die Durchführung von "Privacy Impact Assessments", Rechte der Betroffenen und Audits.

Sie sollten schliesslich verdeutlichen, worum es bei Compliance überhaupt geht, nämlich das Treffen von Massnahmen, um die Verstösse gegen intern und extern vorgegebene Regeln zu verhindern, zu erkennen und darauf zu reagieren ("Prevent, Detect, Respond"). Auch in dieser Hinsicht muss also klargestellt werden, dass das Thema mit dem Erlass einiger Weisungen nicht getan ist. Compliance geht – auch im Bereich des Datenschutzes – wesentlich weiter.

B. Schritt 2: Leidensdruck schaffen

Demut alleine genügt nicht. Unternehmen wollen nicht gegen den Datenschutz verstossen, jedenfalls die Mehrheit hat nicht diese Absicht und will auch nicht die Grenzen des Datenschutzes austesten. Unternehmen müssen sich jedoch nicht nur an den Datenschutz halten, sondern eine Vielzahl von gesetzlichen und anderen Regelungen einhalten. Sind sie international tätig, vervielfältigen sich die Vorgaben im Bereich der Compliance noch. Tatsache ist auch, dass es bisher "wichtigere" Dinge als den Datenschutz gab – wichtiger deshalb, weil Regelverstösse in anderen Bereichen wesentlich gewichtigere Konsequenzen für ein Unternehmen haben konnten. Gemeint sind die beiden bereits erwähnten Bereiche des Kartellrechts und der Korruptionsbekämpfung, aber auch die Vorschriften zur Buchführung, des Gesellschaftsrechts und ganz generell des Aufsichtsrechts in regulierten Branchen. Da die Ressourcen eines Unternehmens endlich sind, müssen Prioritäten gesetzt und

dementsprechende "risikobasierte" Entscheide punkto Compliance gefällt werden.

Hinzu kommt, dass viele Entscheidungsträger mit Fug und Recht sagen können, dass bisher ja auch "nichts passiert" sei und sich niemand wirklich beschwert habe über die Art und Weise, wie das Unternehmen im Datenschutz unterwegs war. Vor diesem Hintergrund wird denn auch verständlich, warum dem Datenschutz jedenfalls bisher eine oft untergeordnete Priorität eingeräumt worden ist. Er soll zwar nicht vernachlässigt werden, aber so richtig ernsthaft betreiben und entsprechend viele Mittel und "*management attention*" dafür aufbringen wollte auch niemand.

Um dem Abhilfe zu schaffen, müssen Sie daher in einem zweiten Schritt Leidensdruck aufbauen. Hierbei besteht die Botschaft, die Sie vermitteln müssen, im Wesentlichen aus vier Aussagen:

1. Erklären Sie, dass es *reiner Zufall* war, dass bisher noch nichts passiert ist. Das wird in aller Regel nicht schwer fallen. Auch hier helfen die zwölf Fragen aus der Einleitung zu diesem Beitrag weiter. In der Tat ist es so, dass jedenfalls in der Schweiz die Datenschutzaufsicht nicht flächendeckend arbeitet, sondern sich aufgrund ihrer beschränkten Ressourcen einzelne Unternehmen herauspickt, diese dann aber in aller Konsequenz verfolgt. Dazu genügen Beschwerden von Mitarbeitern, Kunden oder Konkurrenten, oder schon ein kritischer Zeitungsbericht zu den Geschäftsgebahren des Unternehmens im Bereich des Datenschutzes, selbst wenn dieser an den Tatsachen vorbeigeht.
2. Zeigen Sie, dass sich die Zeiten ändern. Auch das wird Ihnen kein Problem bereiten: Die EU hat soeben ihr Datenschutzrecht generalrevidiert und in vielen Bereichen verschärft. Auch Unternehmen aus der Schweiz werden sich in vielen Fällen der DSGV und ihrer extraterritorialen Wirkung nicht entziehen können. Das geht so weit, dass manche Schweizer Unternehmen inskünftig sogar eine Kontaktperson in der EU bezeichnen müssen. Das Schweizer Datenschutzgesetz befindet sich ebenfalls in Revision; ein Vorentwurf wird noch 2016 vorgelegt werden. Dass es diese neuen gesetzlichen Anforderungen gibt, ist nach meiner Erfahrung mittlerweile selbst in den obersten Führungsetagen bekannt, was nicht zuletzt an den drakonischen Bussenandrohungen liegt, mit welchen die DSGV von sich reden macht. Aber auch die betroffenen Personen üben mittlerweile ihr Recht aus und gehen dafür sogar – mit Erfolg – vor Gericht. Hier sei exemplarisch der US-Steuerstreit der Schweizer Banken

zu erwähnen, in dessen Rahmen zahlreiche Daten zum US-Geschäft geliefert werden mussten, was wiederum zu Hunderten von Gerichtsverfahren von Mitarbeitern führten, die fürchteten, dass sie aufgrund der Datenlieferungen von den US-Behörden verfolgt würden. Datenschutzverfahren sind somit keine exotische Erscheinung mehr.

3. Zeigen Sie, dass Datenschutz nicht nur eine Frage von unklaren Rechtsfragen oder von Interessenabwägungen ist, die je nach Betrachtungsweise so oder so ausfallen können, sondern es in bestimmten Bereichen schlicht keine Grauzonen gibt: Entweder trifft ein Unternehmen in einer bestimmten Situation eine gewisse Massnahme, oder es handelt rechtswidrig. Die Bekanntgabe von Personendaten in ein Land ohne angemessenen Datenschutz ist so ein Beispiel. Hier bewegen sich manche international tätige Konzerne in der datenschutzrechtlichen Illegalität, weil sie den konzerninternen Datenfluss nicht sauber geregelt haben.
4. Zeigen Sie, dass fehlende Compliance zu immer höheren Kosten und einem wachsenden Bussenrisiko führt. In der DSGV sind zwischenzeitlich Verwaltungsstrafen von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes vorgesehen. Zahlreiche Staaten in Europa aber auch ausserhalb sehen heute schon Bussen und teils sogar Freiheitsstrafen für Datenschutzverstösse vor (vgl. die Länderberichte unter https://goo.gl/EC1Dgh). Hinzu kommen die Kosten zur Umsetzung neuer oder veränderter Anforderungen. Das EuGH-Urteil, welches in der EU zur Ungültigerklärung der Safe-Harbor-Regelung bei Datenexporten in die USA führte, ist ein gutes Beispiel zur Veranschaulichung der Problematik, da dieses Urteil weit über Datenschutzkreise hinaus zur Kenntnis genommen wurde. Unternehmen mussten sich in der Folge des Entscheids innerhalb von kürzester Zeit einen Überblick darüber verschaffen, wie sie allfällige Datenbekanntgaben in die USA mit den betreffenden Empfängern datenschutzrechtlich geregelt hatten. Das war für viele Unternehmen ein Ding der Unmöglichkeit oder mit erheblichen Aufwänden verbunden, weil sie es vorgängig verpasst hatten, die Regelung solcher Datenexporte zu systematisieren. Mindestens eine meiner Klientinnen hatte deswegen anfangs sogar schlaflose Nächte (ich konnte sie beruhigen, denn auch im Datenschutz wird weniger heiss gegessen als gekocht wird, aber das muss an dieser Stelle nicht betont werden). Unternehmen mit funktionierender Datenschutz-Compliance sahen diese Entwicklung hingegen kommen und waren entsprechend vorbereitet, ohne dass hierfür nennenswerte Kosten angefallen sind.

C. Schritt 3: Der Strohhalm

Aus Schritt 1 und 2 ergibt sich in der Kombination normalerweise ein mindestens leichtes Ohnmachtsgefühl: Der Datenschutz ist im Unternehmen in unterschiedlichster Hinsicht nicht eingehalten, und es besteht nicht einmal ein klares Bild, wie schlimm die Situation tatsächlich ist. Und dabei kommen laufend neue Anforderungen hinzu – einschliesslich einer komplett neuen Regulierung in der EU mit saftigen Bussen. Wie sollen diese Probleme sinnvoll gelöst werden? Und vor allem, wo soll damit begonnen werden? Was braucht es dazu?

Der erste Reflex ist in solchen Fällen meist derselbe: Die Stellen, die im Betrieb für den Datenschutz zuständig sind oder hier als ersten Handlungsbedarf erkannt haben und nun versuchen, das Management zu überzeugen, denken an einen "*big bang approach*", d.h. sie wollen auf einen Schlag die Datenschutz-Compliance auf unterschiedlichsten Ebenen und in diversen Bereichen auf Vordermann bringen. Nicht "kleckern, sondern klotzen" heisst da oftmals die Devise, vor allem, wenn der Datenschutz im Unternehmen bisher ein nicht zu rechtfertigendes Schattendasein fristete.

Diese Herangehensweise ist nach meiner Erfahrung normalerweise weder sinnvoll noch zielführend. Ich habe das in einigen Fällen schon so erlebt: Da wird – meist mit Hilfe eines externen Beraters – eine umfassende Planung all jener Schritte unternommen, die das Unternehmen umsetzen muss, um datenschutzkonform zu werden, es werden gigantische Budgets zusammengestellt, um jeden Bereich mit Weisungen zu regeln, alle Prozesse zu definieren, alle Leute auszubilden und so weiter. Das mag für bestimmte Fälle sinnvoll sein, zum Beispiel in sehr sensitiven, klar definierten Bereichen eines Unternehmens. In gewissen Fällen mag das sogar gesetzlich vorgeschrieben und in der Umsetzung auch praktisch zwingend sein, wie etwa im Falle der Datenannahmestellen der Krankenkassen im Bereich der Grundversicherung: Wenn diese punkto Datenschutz-Governance nicht "in Ordnung" sind, werden sie nicht zertifiziert, und ohne Zertifizierung dürfen sie gemäss einschlägigem Aufsichtsrecht nicht betrieben werden. Das sind aber Ausnahmefälle. In den meisten Betrieben führen überambitionierte Datenschutzprojekte hingegen dazu, dass sie in ihrer eigenen Flut versinken, sie zum Selbstzweck werden, viel Geld kosten und ins Stocken geraten, weil bildlich gesprochen die Bissen zu gross waren: Es wird dann erfahrungsgemäss vieles angefangen, aber nichts richtig zu Ende gebracht. Vor allem aber lässt sich auf diese Weise die für nachhaltigen Datenschutz erforderliche Kultur im Betrieb nicht

bilden; diese ergibt sich nicht aus Weisungen oder Aktivismus einiger weniger, sondern aus einer Vielzahl von Menschen, die den Datenschutz-Gedanken kennen und schätzen lernen und ihn im Alltag nebst ihrer sonstigen Tätigkeit umsetzen und dadurch von innen her zum Durchbruch verhelfen.

Datenschutz-Compliance muss mit anderen Worten in einem Unternehmen heranwachsen können, um akzeptiert zu werden, sich dauerhaft zu etablieren und systematisch, statt reaktiv betrieben zu werden, und zwar auch dann, wenn das Unternehmen sich kein formalisiertes, zertifizierbares Datenschutz-Managementsystem (DSMS) leisten will oder muss.

Wo aber anfangen? Hier hat sich in der Praxis bewährt, dem Management des Unternehmens einen einfachen, ersten, aber effektiven Schritt auf dem Weg zur Datenschutz-Compliance anzubieten, einen ersten Schritt, der sich gut verkaufen lässt und Leidensdruck nimmt. Es ist mit anderen Worten der "Strohhalm", den Sie finden und dem Management reichen müssen, um sich aus der mindestens gefühlt miserablen Datenschutz-Compliance retten zu können. Es geht um eine Massnahme, die zwar nicht das ganze Problem löst, die es aber dem Management ermöglicht zu sagen, dass es die Herausforderung auch tatsächlich anpackt.

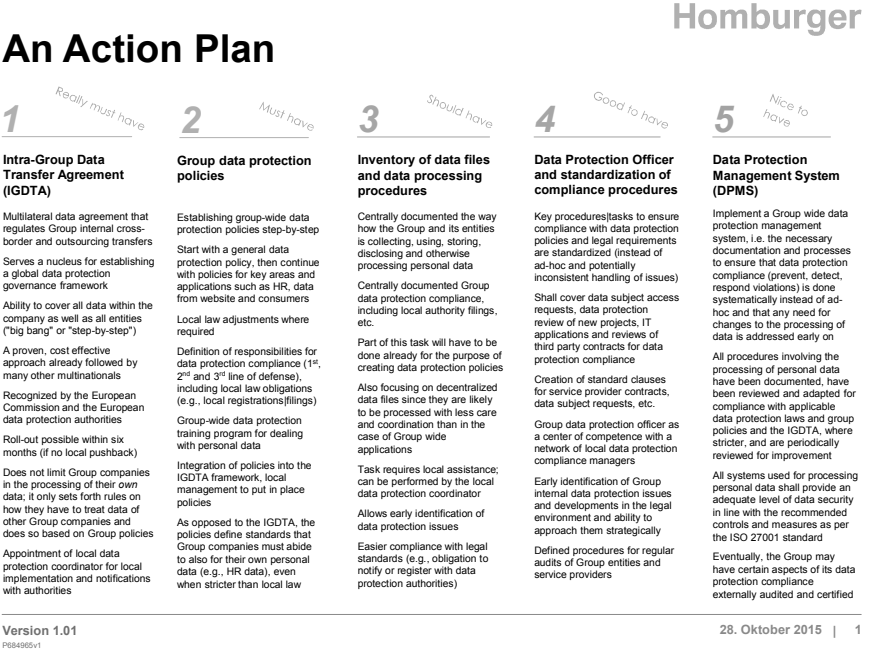
Der Strohhalm soll und darf etwas kosten, denn sonst ist er nichts wert, er sollte aber nicht zu teuer sein, denn sonst sind die Hürden zur Genehmigung seines Einsatzes zu hoch. Der Strohhalm darf nicht zu kontroversen Diskussionen im Management führen, denn sonst droht die Diskussion zu versanden, weil sie zur Klärung auf später verschoben werden muss. Es muss sich vielmehr um einen Lösungsansatz handeln, für den das Management dankbar ist, weil es einen ersten Schritt in die richtige Richtung ist und den Leidensdruck etwas lindert. Es muss schliesslich eine sehr konkrete Massnahme sein mit anerkannter Compliance-Wirkung, auch wenn das obere Management ihre Wirkung letztlich nicht versteht. Hier hilft es erfahrungsgemäss eine Massnahme zu wählen, die auch Mitbewerber und andere Unternehmen bereits erfolgreich umgesetzt haben – ein Argument, dass immer wirkt. Kein Entscheidungsträger will in solchen Dingen, die er nicht freiwillig, sondern gezwungenermassen tut, Experimente machen.

Es bringt nichts, diese erste Massnahme allzu lange vorzubereiten und zu prüfen, wo in der Sache die Datenschutzrisiken im Betrieb am grössten sind. Dazu müsste ein Unternehmen in aller Regel zuerst einmal verstehen, wer intern welche Daten wie bearbeitet, und dies wissen wie gezeigt die wenigs-

ten Unternehmen. Es ist daher jedenfalls in grossen, multinationalen Unternehmen mit unterentwickelter Datenschutz-Compliance eine reine Geld- und Zeitverschwendung, in einem ersten Schritt zum Beispiel eine Gap-Analyse vorzunehmen und zu analysieren, wo genau das eigene Unternehmen im Datenschutz nicht das tut, was es sollte. Die resultierende Liste wird lang sein und nicht mehr Anhaltspunkte wie eine Priorisierung der zu treffenden Massnahmen bringen, wie sich normalerweise in einer Sitzung von zwei oder drei Stunden herausfinden lässt. Ein Workshop von einigen Stunden mit den richtigen Personen genügen jedenfalls nach meiner Erfahrung, um ein vergleichsweise gutes Bild der Datenschutz-Compliance in einem Unternehmen oder Konzern zu erhalten und einen Plan zu schmieden.

Auch auf den Plan sollten Sie nicht zu viel Zeit verschwenden. Es gibt hier keine optimale oder für alle Situationen richtige Lösung. Wesentlich ist, dass akzeptiert wird, dass sich nicht alle Probleme mit einem Schlag lösen lassen, dass stattdessen schrittweise vorgegangen wird und alle sich einig sind, dass nach dem ersten Schritt weitere folgen müssen. Auch das Management muss wissen, dass die erste Massnahme, die es genehmigt, lediglich der Beginn einer Compliance-Bestrebung ist, die einen Horizont von ohne Weiteres bis zu fünf Jahren haben kann. Diese Zeit kann nämlich erfahrungsgemäss erforderlich sein, um den Datenschutz in einem Unternehmen auf Vordermann zu bringen, auch wenn erste, wirksame Schritte viel rascher umgesetzt werden können. Dies ist dem Management ebenfalls zu kommunizieren, doch wird dessen Bereitschaft, einem Compliance-Vorhaben scheibchenweise zuzustimmen, wesentlich grösser sein als es in einem Schlag zu genehmigen. Es sollte nach wie vor die Option haben, spätere Schritte, die vielleicht lediglich "good to have" oder gar "nice to have" sind, abzulehnen.

Die nachstehende Folie zeigt das Beispiel eines Aktionsplans aus dem Jahre 2015, wobei das Management in einem ersten Schritt nur über den ersten oder die beiden ersten Schritte befindet:



Erfahrungsgemäss ist es am sinnvollsten, mit Massnahmen im Bereich der formalen Anforderungen des Datenschutzes zu beginnen. Sie sind aus meiner Sicht ein "quick win", ein schnell zu realisierender Gewinn: Sie lassen sich oft relativ einfach umsetzen, helfen aber zugleich, das rechtliche Risiko im Bereich des Datenschutzes deutlich zu reduzieren. Behörden können die Einhaltung formaler Anforderungen wesentlich einfacher nachprüfen als materielle Anforderungen, und sie bieten oft nicht wirklich Spielraum in der Frage, ob sie erforderlich sind. Sie wirken zudem teilweise bereits durch ihr Vorhandensein, und zwar gleichgültig, ob und wie sehr dem Datenschutz im Betrieb sonst nachgelebt wird. Viele der formalen Anforderungen sind auch bussenbewehrt, während Sanktionen aufgrund einer in der Sache unkorrekten Datenbearbeitung schwieriger zu fällen sind, da sie Wertentscheide voraussetzen.

Eine typische erste Massnahme ist die Vornahme von zwingenden Behördenmeldungen. In der Schweiz gibt es nur wenige solche Pflichten, weshalb

viele Unternehmen gar nicht meldepflichtig sein werden, doch im europäischen Ausland unterliegen Unternehmen mitunter vergleichsweise weitgehenden Melde- und Bewilligungspflichten.

Meine persönlich bevorzugte "erste Massnahme" in einem Konzern ist der Abschluss eines konzerninternen Datentransfer- und Outsourcing-Vertrags, in der Fachsprache auch als Intra-Group-Data-Transfer-Agreement ("IGDTA") bezeichnet. Es regelt alle relevanten Aspekte des konzerninternen Flusses von Personendaten, sei es vor dem Hintergrund der Exportregelungen (in der Schweiz: Art. 6 DSG), sei es vor dem Hintergrund der Auftragsdatenbearbeitung (in der Schweiz: Art. 10a DSG). Dieser Vertrag wiederum muss in diversen Staaten – so auch der Schweiz – den lokalen Datenschutzbehörden notifiziert werden. Er wird Ihnen allerdings auch beim nächsten Schritt zur Datenschutz-Compliance gute Dienste leisten.

D. Schritt 4: Die Hidden Agenda

Datenschutz lässt sich natürlich nicht nur mit formalen Massnahmen wie etwa einer Datenschutzmeldung bei der Behörde oder dem Abschluss eines IGDTA betreiben. Datenschutz muss im Betrieb gelebt werden. Daher genügt es auch nicht, dass das Management mit gutem Willen alle möglichen Weisungen erlässt, wie mit Personendaten umzugehen ist. Solche Weisungen sind zwar nötig, da das Datenschutzrecht zu generisch ist, um den Mitarbeitern als konkrete Handlungsanweisung im betrieblichen Alltag zu dienen.

Es genügt somit nicht, den Datenschutz nur zu *verordnen*. Damit Datenschutz im Betrieb gelebt wird, muss ein Unternehmen im eigenen Betrieb Personen aufbauen, die sich dafür einsetzen und sich damit auskennen, die zum Beispiel ihren Kollegen in der Praxis bei datenschutzrechtlichen Fragen zur Seite stehen, ein Auge auf diese Dinge haben und für Verständnis sorgen. Gelebter Datenschutz erfordert viel Fleiss, Disziplin und damit auch Akzeptanz, denn Datenschutz ist zwar auch in der Sache sinnvoll, erfüllt ein natürliches Bedürfnis der meisten von uns und kann geschäftlich ein Gewinn sein, aber wir sollten uns nichts vormachen: Datenschutz macht uns allen die Arbeit letztlich ein deutliches Stück schwerer als wenn es ihn nicht geben würde. Denn Datenschutz erfordert bereits in materieller Hinsicht, dass Rücksicht genommen werden muss, dass aktiv kommuniziert wird, dass laufend hinterfragt wird, ob eine bestimmte Datenbearbeitung in der Tat gerechtfertigt ist. Die dafür erforderliche Unterstützung im eigenen Betrieb aufzubauen, die eigene Organisation an Datenschutz-Compliance zu gewöhnen und

für die nötige Akzeptanz zu sorgen, ist wesentlich anspruchsvoller als der Abschluss eines Vertrags wie etwa dem IGDTA. Doch auch hier gibt es Lösungsansätze aus der Praxis.

Damit sind wir auch schon beim vierten Schritt auf dem Weg zur Datenschutz-Compliance: Hat das Management den Strohhalm erst einmal ergriffen und kommt er zum Einsatz, sollten Sie ihn als "trojanisches Pferd" für ihren Masterplan nutzen.

Das IGDTA ist für mich ein wunderbares Beispiel, wie das in einem internationalen Konzern geht: Der Abschluss eines solchen Vertrags zwischen den einzelnen Konzerngesellschaften ist relativ simpel zu bewerkstelligen. Ein solcher Vertrag besteht im Wesentlichen aus den beiden, von der Europäischen Kommission genehmigten Mustervertragsklauseln für grenzüberschreitende Datenübermittlungen in Länder ohne angemessene Datenschutzgesetze. Das Schöne daran ist, dass sie für einen Laien kompliziert ausschauen, sie nicht verändert werden dürfen, sie aber trotzdem weltweit als Standard akzeptiert sind, selbst bei Unternehmen aus den USA. Darüber hinaus enthält das IGDTA im Prinzip nur noch Rahmenbestimmungen, die dafür sorgen, dass diese Musterklauseln, wo erforderlich, zwischen den einzelnen Konzerngesellschaften zum Einsatz kommen und gewisse weitere Fälle (wie etwa Auftragsdatenbearbeitungen) abgedeckt sind. Gegen ein IGDTA lässt sich rechtlich eigentlich so gut wie gar nichts einwenden: Wenn in einem Konzern beispielsweise HR-Daten aus Europa einer Konzerngesellschaft in den USA zugänglich gemacht werden sollen, braucht es in aller Regel einen solchen Vertrag. Hat ein Unternehmen nichts Vergleichbares, verhält es sich rechtswidrig. Ein IGDTA ist dabei die einfachste Methode, diesen Rechtsverstoss, der in gewissen Ländern auch bussenbewehrt ist, zu heilen. Immer mehr Konzerne schliessen daher ein solches Vertragswerk konzernintern ab. Es ist – wie der Amerikaner sagen würde – praktisch ein "*no brainer*", falls ein Konzern nicht aufwendigere Ansätze wie etwa "Binding Corporate Rules" verfolgen will.

Das Spannende an einem IGDTA ist allerdings, wie es sich – wird es konsequent genutzt – in einem Konzern weit über seinen Kernzweck hinaus auswirken kann. An dieser Stelle seien nur drei solcher Nebeneffekte erwähnt:

– Erster Nebeneffekt: Eigentlich dient ein IGDTA nur dazu, den teilnehmenden Konzerngesellschaften vorzuschreiben, wie sie die Daten *anderer* Konzerngesellschaften bearbeiten dürfen, wenn sie auf diese nutzen wollen. In der Bearbeitung ihrer eigenen Daten schränkt das IGDTA sie

nicht ein. Darum ist der interne Widerstand normalerweise gering, und die Konzerngesellschaften sind mehr oder minder bereit, sich gewissen Datenschutzregeln zu unterwerfen, auch wenn sie dies aufgrund ihrer eigenen Rechtsordnung nicht tun müssen. Das Argument, dass das ausländische Recht dies eben verlangt, wirkt in solchen Fällen. Die Erfahrung zeigt allerdings auch, dass die Grenzen zwischen den Datentöpfen der einzelnen Konzerngesellschaften zusehends verschwinden und die Regeln, die eigentlich gemäss IGDTA nur bei Zugriffen auf *fremde* Datentöpfe beachtet werden müssen, zusehends auch für die Bearbeitung eigener Daten zum Standard werden, obwohl das IGDTA dies nicht vorsieht. Um die Aufwendungen zur Einhaltung des IGDTA tief zu halten, wird sich ganz von selbst ein Trend zur Vereinheitlichung der Regeln durchsetzen, und dieser Konzernstandard wird sich oft an den strengsten Vorgaben ausrichten. Auf diese Weise entstehen über Zeit konzernweite Standards, deren zwangsweise Einführung auf einen Schlag mit grosser Wahrscheinlichkeit an internen Widerständen gescheitert wäre.

– Zweiter Nebeneffekt: Ein IGDTA sieht sinnvollerweise lokale Ansprechpersonen für Fragen zur Umsetzung des IGDTA vor. Das Pflichtenheft dieser Personen kann sehr schlank gehalten werden, geht es im IGDTA doch streng genommen nur um den Zugriff auf Daten anderer Konzerngesellschaften und umgekehrt. Die Bearbeitung eigener Daten – das Kernthema der Datenschutz-Compliance – ist davon nicht erfasst. Das ist wichtig, denn wenn die teilnehmenden Gesellschaft den Eindruck haben, dass ihnen die Umsetzung des IGDTA zuviel Aufwand verursacht und ihnen personelle Ressourcen wegfrisst, werden sie sich dagegen wehren. Doch auch hier erweist sich ein IGDTA als trojanisches Pferd für die Datenschutz-Compliance: Es zwingt nämlich erstens die Ansprechpersonen sich mit den Fragen des Datenschutzes auseinanderzusetzen, und zweitens drückt es ihnen innerhalb ihrer eigenen Firma den "Datenschutz-Stempel" auf. Auch wenn sie sich formell nur um das IGDTA kümmern müssen, zeigt die Erfahrung, dass diese Personen über Zeit auch im eigenen Hause mit allen weiteren Fragen zum Datenschutz betraut werden ("Da war doch einer, der dieses Datenschutzding der Konzernzentrale umsetzen musste?!"). Sie entwickeln sich so über Zeit zwangsläufig zu Spezialisten in diesem Bereich, und mit der Spezialisierung kommen auch die Ambitionen und das Verantwortungsgefühl, dem Datenschutz auch über das IGDTA Nachachtung zu schenken. Das IGDTA wiederum sorgt für die internationale, konzerninterne Vernetzung dieser Leute. Für die Konzernzentrale, die sich um den Datenschutz

auch in den Tochtergesellschaften kümmern muss, werden sie zu idealen Ansprechpartnern weit über die Belange des IGDTA hinaus. Dies alles ergibt sich mit der Zeit praktisch von alleine aufgrund der Macht der Gewohnheit.

– Dritter Nebeneffekt: Die lokalen Ländergesellschaften, die dem IGDTA beitreten, müssen selbständig prüfen, ob das IGDTA ggf. den lokalen Behörden notifiziert werden muss. Dies wird darin mit Vorteil explizit festgehalten. Diverse Staaten kennen solche Meldepflichten. Viele Unternehmen sind sich dessen jedoch nicht bewusst. Ist das Vertragswerk aber erst einmal unterschrieben, werden sie sich zwangsläufig mit der Frage auseinandersetzen. Hat ein Unternehmen seine diesbezüglichen Pflichten im Griff, wird das keinen grösseren Aufwand mit sich bringen. Die Erfahrung zeigt allerdings, dass manche Gesellschaften ihre Meldepflichten überhaupt erst dann realisieren, wenn sie konkret darauf angesprochen werden und entsprechende Abklärungen tätigen. Im Rahmen einer solchen Abklärung kommen freilich regelmässig weitere Fragen auf, die bei dieser Gelegenheit ebenfalls geklärt werden müssen. Schreibt ein Land vor, dass ein Vertrag wie das IGDTA der Datenschutzbehörde gemeldet werden muss, dann wird es häufig auch die Anmeldung bestimmter Datensammlungen oder -bearbeitungen vorsehen. Meldet das Unternehmen nur das IGDTA, muss es mit kritischen Rückfragen der Behörde rechnen. Die Gesellschaft wird somit in vielen Fällen faktisch gezwungen sein, auch die anderen, mit dem IGDTA nicht unmittelbar zusammenhängenden Meldungen nachzuholen, was wiederum weitere Compliance-Massnahmen wie etwa die Erhebung der von der Gesellschaft geführten Datensammlungen zur Folge haben kann. So kann das IGDTA eine ganze Reihe von Folgemassnahmen auslösen.

Diese Nebeneffekte legen Sie selbstverständlich den betroffenen Gesellschaften nicht offen. Sie sind quasi ihre "Hidden Agenda", um unnötige Diskussionen zu vermeiden. Diese Nebeneffekte sind aus Sicht der Compliance aber ebenso wertvoll wie die unmittelbare Wirkung des IGDTA. Hinzu kommt, dass ein IGDTA zu Beginn mit einem sehr engen Anwendungsbereich eingeführt werden kann, indem es beispielsweise auf HR-Daten beschränkt wird. Ist ein IGDTA aber erst einmal im Konzern etabliert, kann es sehr viel einfacher auf andere Bereiche ausgedehnt werden und auch bei den materiellen Regeln, zu deren Einhaltung die einzelnen Gesellschaften sich verpflichten, können zusehends "die Schrauben angezogen" werden. Dazu sogleich mehr.

E. Schritt 5: Gewinnen Sie die Early Adopters

Sie mögen selbst vielleicht erkannt haben, wie wichtig es ist, dass Ihr Unternehmen sich für eine funktionierende Datenschutz-Compliance einsetzt. Sie sehen die möglichen negativen Folgen für Ihr Unternehmen, wenn es sich nicht darum kümmert (Stichwort "Leidensdruck") und sehen auch, welchen Gewinn Datenschutz der Firma einbringen kann – etwa in Form eines erhöhten Kundenvertrauens und zufriedeneren Mitarbeitern.

Aber: Nicht jeder im Betrieb wird Verständnis für Datenschutz haben, und er wird sich darauf berufen, dass es "bisher ja auch ging". Der Mensch ist zudem ein Gewohnheitstier, und er mag Veränderung normalerweise nicht. Das gilt auch im Bereich des Datenschutzes und erschwert dessen Umsetzung naturgemäss, jedenfalls wo zur Datenschutz-Compliance Anpassungen in den Abläufen erforderlich werden und wo es zu Einschränkungen kommt, weil gewisse Informationen für einen Mitarbeiter plötzlich "aus Gründen des Datenschutzes" nicht mehr verfügbar sind. Der Hinweis, dass dies eben gesetzlich so vorgeschrieben sei, wird nichts zu einer besseren Stimmung beitragen. Auch für viele der Entscheidungsträger ist Datenschutz wenig greifbar und zu abstrakt, um ihn zu verstehen, ganz im Gegensatz zu anderen Compliance-Themen wie etwa die Bekämpfung von Korruption: Jeder Manager hat ein klares Verständnis, worum es bei Korruption geht, oder er glaubt dies zumindest. Im Bereich des Datenschutzes ist das nicht der Fall. Datenschutz ist ein Nebelthema und dies führt leider allzu oft dazu, dass Sie es schwer haben werden, für ihre Pläne entsprechende Verbündete im Unternehmen zu finden.

Ohne hinreichend starke Verbündete in den relevanten Stellen im Unternehmen werden Sie Ihre Massnahmen zur Datenschutz-Compliance jedoch nicht durchsetzen können. Ohne Verbündete wird auch eine von der Unternehmensführung verordnete Datenschutzweisung toter Buchstabe bleiben und nicht in allen Bereichen können Sie persönlich dafür sorgen, dass die darin enthaltenen Vorgaben ernst genommen werden.

In der Praxis lässt sich dieses Problem dadurch lösen, indem die folgenden drei Punkte beachtet werden:

1. Projekte zur Datenschutz-Compliance müssen interdisziplinär durchgeführt werden. Es nützt nichts, wenn sich nur die Rechts- oder Compliance-Abteilung um entsprechende Massnahmen kümmert. Hat sie keine Verbündeten im Bereich der IT-Sicherheit und der IT, wird sie mit ihren

Vorgaben gegen eine Mauer laufen. Die Interdisziplinarität ist auch sachlich erforderlich, ist Datenschutz doch selbst eine Mischung verschiedener Disziplinen: Da gibt es Aspekte der technischen Datensicherheit, Aspekte der Datenverarbeitung, rechtliche Aspekte und – etwa im Bereich der Interessenabwägung oder Verhältnismässigkeit – fachliche und geschäftliche Fragen. Diese kann weder ein Jurist alleine beantworten, noch ein Informatiker oder ein Ökonom. Werden Datenschutz-Compliance-Projekte von Anfang an interdisziplinär betrieben, kann auch den zwei weiteren, in jedem Unternehmen bekannten Phänomenen "Not Invented Here" und "Not In My Backyard" wirkungsvoll begegnet werden. Nicht verhindern kann die Interdisziplinarität allerdings Diskussionen zur Frage, über wessen Budget die Kosten der Massnahmen zur Datenschutz-Compliance laufen sollen.

2. Projekte zur Datenschutz-Compliance müssen intern oder quasi-intern betrieben werden, denn sie sollen auch intern etwas verändern. Es spricht nichts dagegen, sich gerade zu Beginn eines Aktionsplans "Datenschutz" etwas Hilfe von externen Beratern zu holen. Sind sie wirklich erfahren, haben sie den Vorteil, dass sie entsprechende Vorhaben bereits mehrfach in anderen Unternehmen umgesetzt haben und mit ihrem Wissen und ihrer Erfahrung helfen können, gewisse Fehler zu vermeiden und zur Effizienz beitragen. Externe Berater können auch wichtig sein, wenn es darum geht, die eigenen Entscheidungsträger zu überzeugen, denn auch in Sachen Datenschutz gelten die Propheten im eigenen Lande oft wenig. Allerdings ist es wichtig, das Know-how im Bereich des Datenschutzes zu internalisieren; das Unternehmen muss in Sachen Datenschutz-Compliance auf den eigenen Beinen stehen können. Das gilt umso mehr, je grösser das Unternehmen ist, und ist nicht nur eine Kostenfrage, sondern auch eine Frage der Effizienz. Datenschutz-Compliance verlangt weitaus mehr als Kenntnisse im Bereich des Datenschutzes; diese lassen sich relativ leicht aneignen oder solange erforderlich von aussen einkaufen. Die wirkliche Herausforderung ist die Kenntnis der internen Verhältnisse und der Umgang mit den diversen innerbetrieblichen "Stakeholdern", wenn es darum geht, den Datenschutz auch gegen deren Willen durchzusetzen, wo dies nötig ist.
3. Gerade zu Beginn eines Projekts zur Datenschutz-Compliance ist es wichtig, intern die richtigen Partner zu identifizieren, die sich als "Early Adopters" gewinnen lassen und mit Ihnen am selben Strick ziehen, weil sie sich von der Sinnhaftigkeit und Notwendigkeit des Projekts besonders leicht überzeugen lassen. Solche Early Adopters finden sich typi-

scherweise am häufigsten im Bereich Compliance, Recht, Informatik, interne Revision bzw. Controlling, Informationssicherheit und Personalwesen. Der letztgenannte Bereich ist vorliegend besonders interessant, da Daten über die eigenen Mitarbeiter in den meisten Unternehmen zu einem für die Datenschutz-Compliance wichtigen Bereich zählt. Da Personalverantwortliche oft eine hohe Affinität zu Datenschutzthemen aufweisen, sind sie regelmässig ideale Verbündete für ein Datenschutzprojekt wie etwa die Einführung eines IGDTA. Manche meiner multinationalen Klienten entschieden sich aus genau diesem Grund, ihr IGDTA – wie vorstehend erwähnt – zunächst nur mit Bezug auf HR-Daten einzuführen. Den Personalverantwortlichen musste in der Regel nicht erst erklärt werden, warum Datenschutz wichtig und das IGDTA daher eine sinnvolle Sache ist. Diskussionen mit anderen, weniger einsichtigen Geschäftsbereichen, welche die Einführung des IGDTA massiv verzögert hätten, konnten so vermieden werden. Sie nahmen davon erst Kenntnis, als es bereits etabliert und nicht mehr wegzudenken war – zu spät, um sich noch dagegen zu wehren, bin ich versucht zu sagen.

F. Schritt 6: Mut zur Lücke

Ich habe es bereits zwei Mal erwähnt: Niemand kann die Anforderungen des Datenschutzes vollständig erfüllen. Das wird sich auch in Zukunft nicht ändern. Aus diesem Grund sollten auch Massnahmen zur Datenschutz-Compliance nicht danach streben, alle Anforderungen des Datenschutzes abzudecken, sondern sich auf wesentliche Punkte fokussieren. Mut zur Lücke lautet das Credo. Es bedeutet nicht, dass sich ein Unternehmen in den von einem Compliance-Vorhaben nicht erfassten Bereichen gegen den Datenschutz entscheidet oder Regelverstösse bewusst in Kauf nimmt. Wenn jedoch mehrere Häuser brennen und nur eines gelöscht werden kann, muss eine Wahl getroffen werden. Wird das Feuer in allen Häusern nur ein bisschen bekämpft, werden alle Häuser niederbrennen. Auch im Datenschutz hat es sich als effektiver und effizienter erwiesen, wenn Unternehmen ihre Ressourcen zielgerichtet einsetzen und Prioritäten festlegen, statt nach dem Giesskannenprinzip vorzugehen.

Hinzu kommt, dass Datenschutz-Compliance im Betrieb erlernt werden muss und die Umsetzung entsprechender Massnahmen viele Fallstricke mit sich bringt. Gewisse Prozesse spielen sich in jedem Unternehmen in ähnlicher Form ab, andere sind firmenspezifisch. Auch aus diesem Grund ist es erfahrungsgemäss sinnvoll, sich bei der Umsetzung grösserer Compliance-

Vorhaben zunächst auf einen Bereich zu beschränken und die Aktivitäten erst danach auf die weiteren Bereiche auszudehnen, um sie dort mit Hilfe der gesammelten Erfahrungen umso rascher, besser und effizienter umsetzen zu können. Die Fokussierung auf einen Bereich hat den nützlichen Nebeneffekt, dass sich auch die innenpolitische Unterstützung und die nötigen Budgets leichter beschaffen lassen und sich sehr viel schneller Resultate erzielen lassen, als wenn Massnahmen an breiter Front eingeführt werden müssen.

Welchen Bereich ein Unternehmen als "Pilot" oder prioritäres Ziel für ein Datenschutz-Compliance-Projekt auswählt, ist vor allem eine taktische Frage. Manche werden hierfür den Bereich mit den gefühlt grössten Datenschutzrisiken wählen, andere wiederum den Bereich, in welchem intern die wenigsten Widerstände zu erwarten oder schon besonders viele Vorarbeiten vorgenommen wurden.

Hierzu müssen die einzelnen Bereiche, in denen Datenbearbeitungen im Unternehmen stattfinden, nach Risiko und Verantwortlichkeiten unterschieden werden. Unternehmen im industriellen Bereich, die nach Risiko priorisieren, beschränken sich bei ihren Massnahmen zur Datenschutz-Compliance zum Beispiel zu Beginn normalerweise auf die Bearbeitung von Mitarbeiterdaten, bevor sie sich (falls überhaupt) den Kundendaten, den Daten von Lieferanten und etwaigen anderen Daten widmen. Ein Unternehmen, das mit Konsumenten verkehrt, wird seine Priorität vermutlich auf die Bearbeitung von Daten seiner privaten Endkunden festlegen. Ein anderer Ansatz ist die Unterscheidung zwischen den zentral koordinierten Datenbearbeitungen und jenen, für welche dezentrale Verantwortungen bestehen und daher schwieriger zu erfassen sind.

Grössere IT-Projekte haben sich in der Praxis ebenfalls als sehr gute Gelegenheit zur Einführung von Datenschutz-Massnahmen erwiesen. Die Compliance ist hier quasi Trittbrettfahrerin: Wird beispielsweise eine neue Software zur Verwaltung von HR-Daten eingeführt oder die Aufbewahrung von Daten im Konzern zentralisiert oder neu organisiert, können begleitend dazu sehr leicht neue Weisungen, Verträge, Schulungen und anderen Vorkehrungen zur Datenschutz-Compliance implementiert werden. Solche IT-Projekte haben für den Datenschutz erhebliche innenpolitische Vorteile: Es bestehen in der Regel separate Budgets, über die auch die Massnahmen zum Datenschutz finanziert werden können. Zudem werden in diesen Fällen die innenpolitischen Widerstände gegen solche Massnahmen in aller Regel gering sein. Voraussetzung ist allerdings, dass sie vom Management als rechtlich

zwingende Voraussetzung zur rechtskonformen Umsetzung der betreffenden Vorhaben positioniert und entsprechend gestützt werden. Sie dürfen mit anderen Worten kein "Wunschkonzert" sein. Die Gelegenheit solcher IT-Projekte hat auch noch einen anderen Vorteil: Soweit die Datenschutz-Massnahmen gegenüber den Behörden gemeldet werden müssen, kann unter Hinweis auf die Einführung eines neuen Systems ohne Weiteres begründet werden, warum eine Meldung gerade zu diesem Zeitpunkt erfolgt und nicht schon viel früher. Lästige Fragen und Erklärungsnöte bleiben so oft erspart.

Ist der Bereich für einen Pilot identifiziert, werden die geplanten Anstrengungen wie etwa das Formulieren entsprechender Weisungen, definieren von Prozessen, Durchführen von Schulungen und Prüfungen, der Realisierung technischer Massnahmen, den Abschluss von Verträgen, etc. zunächst nur auf einen Bereich konzentriert werden. Versuchen Sie es allerdings auch hier nicht, es perfekt zu machen und so das Vorhaben zu gefährden. Die Fokussierung auf das Wesentliche ist das Ziel, denn selbst wenn sich eine geplante Compliance-Massnahme nur zu 80 Prozent umsetzen lässt oder befolgt wird, wird dies im Bereich des Datenschutzes normalerweise eine erhebliche Verbesserung gegenüber dem früheren Zustand darstellen. An den restlichen 20 Prozent kann zu einem späteren Zeitpunkt gearbeitet werden.

III. Schlusswort

Die Schwierigkeit der Datenschutz-Compliance ist nicht, dass nicht klar wäre, was die rechtlichen Anforderungen des Datenschutzrechts an das Unternehmen sind, welche Massnahmen diesbezüglich ergriffen werden müssen und wie sie korrekt und optimal umzusetzen wären. Die Herausforderung liegt in der Praxis darin, den Datenschutz in einer Organisation so weit zu verankern und zu etablieren, dass er nicht mehr nur *ad-hoc* und reaktiv, sondern möglichst durchgängig systematisch und pro-aktiv betrieben wird. Die in meinem Beitrag dargelegte Vorgehensweise kann erheblich zur Erreichung dieses Ziels beitragen und einem Unternehmen helfen, auf den "richtigen Weg" zu kommen. Die Vorgehensweise erscheint auf den ersten Blick zwar unkonventionell, ist aber praxiserprobt. Die genannte Herausforderung vermögen allerdings, wenn überhaupt, nur wenige Unternehmen vollumfänglich zu meistern. Meine Erfahrung zeigt auch, dass diese Chancen je kleiner sind, je grösser ein Unternehmen ist, auch wenn es theoretisch absolut betrachtet mehr Geld in Datenschutz-Compliance investieren kann. Formali-

sierte DSMS haben dieses Ziel im Übrigen auch. DSMS, Datentransferverträge und all die weiteren Massnahmen zum Datenschutz sind jedoch im Ergebnis nur Hilfsmittel auf dem Weg zur Datenschutz-Compliance. Am Ende zählt schlicht, wie "anständig" ein Unternehmen seine Daten in der Perzeption der betroffenen Personen und der Öffentlichkeit bearbeitet. Tut es das nicht, wird ihm auch das ausgeklügelste System zur Sicherstellung der Datenschutz-Compliance nichts nutzen.