RECHTSANWÄLTE

SCHELLENBERG WITTMER

SEPTEMBER 2015

Newsletter

Autor:
Roland Mathys

INFORMATION TECHNOLOGY / DATA PROTECTION

Zunehmende Bedeutung der Datenschutz-Compliance – eine praktische Anleitung für Compliance-Programme

Die Relevanz datenschutzrechtlicher Fragen und Themen hat sich in den vergangenen Jahren stark erhöht. Entsprechend wird auch der Datenschutz-Compliance im Unternehmen mehr Beachtung geschenkt. Viele Betriebe tun sich bei der Einführung von Compliance-Programmen aber noch schwer – eine praktische Anleitung zum Vorgehen kann hier Abhilfe schaffen.

1 EINFÜHRUNG

Der **Stellenwert des Datenschutzes** hat in den letzten Jahren massiv zugenommen: Noch vor relativ kurzer Zeit fristete der Datenschutz ein Schattendasein, während heutzutage datenschutzrechtliche Fragen und Themen prominent beleuchtet werden.

Diese Entwicklung geht auf verschiedene **Ursachen** zurück: Neue Technologien mit starkem Bezug zu Personendaten (z.B. soziale Netzwerke, tragbare Geräte wie Fitnesstracker oder Big Data Analysen) haben sich etabliert; Aktivitäten von Behörden und Gerichten haben das Augenmerk vermehrt auf den Datenschutz gelenkt (z.B. Entscheide betreffend Google Street View in der Schweiz oder das "Recht auf Vergessen" in der EU); einzelne Vorfälle, bei denen der Datenschutz im Zentrum stand, wurden in den Medien breit wiedergegeben (z.B. die "NSA-Affäre").

Dieser Trend wird auch in Zukunft anhalten. Jedenfalls deuten die **gesetzgeberischen Bestrebungen** in der EU mit dem demnächst finalisierten Entwurf zu einer Datenschutz-Grundverordnung wie auch entsprechende Revisionsbestrebungen im schweizerischen Datenschutzrecht in diese Richtung. Beispielsweise können unter der neuen EU-Verordnung gegen fehlbare Unternehmen Sanktionen ausgesprochen werden, die bis 5% des weltweiten Jahresumsatzes oder (falls höher) bis EUR 100 Mio. betragen sollen.

Entsprechend hat auch die **Datenschutz-Compliance** für Unternehmen massiv an Bedeutung gewonnen: Während vor wenigen Jahren die Einhaltung datenschutzrechtlicher Bestimmungen noch primär als geschäftsverhindernd und kostengenerierend empfunden wurde, stellt sie heute einen zentralen Pfeiler der Unternehmens-Compliance dar. Dabei bildet die Einhaltung der anwendbaren gesetzli-

chen und sonstigen regulatorischen Vorschriften nicht mehr nur Selbstzweck, sondern zielt oft auch darauf ab, dem Unternehmen ein datenschutzrechtliches "Gütesiegel" zu verleihen, das für Reputationszwecke und als Verkaufsargument proaktiv genutzt werden kann.

"Während der Datenschutz bis vor kurzem noch primär als geschäftsverhindernd und kostengenerierend empfunden wurde, stellt er heute einen zentralen Pfeiler der Compliance dar."

Datenschutz-Compliance stellt für viele Unternehmen juristisches Neuland dar. Entsprechend fällt ihnen die **Entwicklung und Einführung angemessener Compliance-Programme** nicht immer leicht. Es stellen sich Fragen, wie ein solches Programm strukturiert werden kann, wo begonnen werden soll, in welchem Bereich der dringendste Handlungsbedarf besteht, oder was in einem globalen Konzern oder generell im internationalen Umfeld besonders zu beachten ist. Dieser Newsletter versucht, auf solche und weitere Fragen Antworten zu geben und eine praktische Vorgehensanleitung für Datenschutz-Compliance Programme zu vermitteln.

2 BESTANDESAUFNAHME ZU BEGINN

Am Anfang des Compliance-Programms steht die Aufnahme des **datenschutzrechtlichen Ist-Zustands**. Hierbei gilt es einerseits zu analysieren, welche Personendaten überhaupt bearbeitet werden; andererseits soll erfasst werden, welche datenschutzbezogenen Instrumente (Regelungen, Prozesse, Strukturen) innerhalb eines Unternehmens bereits bestehen.

2.1 DATENBEZOGENE ANALYSE

Zunächst wird erhoben, **welche Personendaten** im Unternehmen gesammelt und bearbeitet werden. Typische Kategorien von Personendaten bilden Mitarbeiterdaten, Kunden- oder Lieferantendaten. Hierbei ist zu beachten, dass einzelne Länder (wie etwa die Schweiz) nicht nur die Daten natürlicher, sondern auch juristischer Personen schützen. Die Datenbestände sollten darauf geprüft werden, ob sie besonders schützenswerte Personendaten (z.B. gesundheitsbezogene Daten) oder Persönlichkeitsprofile umfassen, wo erhöhte Schutzanforderungen gelten. Die Daten sind auch darauf zu untersuchen, ob und in welchen Bearbeitungsphasen eine Anonymisierung oder Pseudonymisierung stattfindet, auf die das Datenschutzrecht keine oder nur beschränkte Anwendung findet.

Für jeden Datenbestand stellt sich die Frage, ob das Unternehmen als **Inhaber der Datensammlung** ("Controller") agiert oder die Daten lediglich im Auftrag eines Dritten bearbeitet ("Processor"). In diesem Zusammenhang ist auch zu erheben, welche Datenbearbeitungsaktivitäten auf ein Drittunternehmen (z.B. im Rahmen eines Outsourcings) übertragen wurden. Ebenso muss für jede Datensammlung geklärt werden, ob sie beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ("**EDÖB**") registriert ist.

Zentrale Bedeutung kommt der **Erfassung der Bearbeitungszwecke und -handlungen** zu. Aufgrund des datenschutzrechtlichen Grundsatzes der Zweckbindung dürfen Personendaten nur für bestimmte, dem Einzelnen mitgeteilte oder für ihn erkennbare Zwecke bearbeitet werden. Die Aufnahme der einzelnen Bearbeitungsaktivitäten kann entlang dem Lebenszyklus der Daten von der Erhebung über die Auswertung, Verwendung, Veränderung, Speicherung, Bekanntgabe, Aufbewahrung bis hin zur Löschung vorgenommen werden. Hierbei empfiehlt sich, typische Bearbeitungsszenarien der einzelnen Unternehmenseinheiten näher zu analysieren (im HR-Bereich z.B. Stellenbewerbung, Qualifikation, Absenzenverwaltung, private Internet- und E-Mail-Nutzung, Mitarbeiterauswertung, Austritt).

Die **Datensicherheit** bildet eine wichtige Komponente des Datenschutzes, weshalb entsprechende Überlegungen in die Analyse einzubeziehen sind. Regelmässig werden Personendaten nach Vertraulichkeit klassifiziert und durch entsprechende technische (z.B. Verschlüsselung) oder organisatorische (z.B. Zugangsbeschränkung) Massnahmen vor Veränderung oder unbefugtem Zugriff geschützt.

Kaum je beschränkt sich der Datenverkehr im globalisierten wirtschaftlichen Umfeld noch auf die Schweiz. **Grenzüberschreitende Datenflüsse** stellen die Regel dar, insbesondere für international tätige Konzerne. Aufgrund der unterschiedlichen Datenschutzniveaus in verschiedenen Rechtsordnungen ist zu untersuchen, in welchen Ländern Personendaten gespeichert werden bzw. von wo aus darauf zugegriffen wird und welche Daten zwischen welchen Staaten konzernintern und -extern transferiert werden.

"Grenzüberschreitende Datenflüsse stellen die Regel dar, insbesondere für international tätige Konzerne."

2.2 UNTERNEHMENSBEZOGENE ANALYSE

Im **organisatorischen Bereich** stellt sich die Frage, ob das Unternehmen über einen betriebsinternen Datenschutzbeauftragten verfügt, was zwar gesetzlich nicht vorgeschrieben ist, aber mit gewissen administrativen Erleichterungen verbunden sein kann. Weiter ist abzuklären, welche Abteilungen innerhalb des Unternehmens für Datenschutzthemen und -fragen zuständig sind (z.B. Recht, Compliance, HR, IT).

Unter dem Aspekt bereits verwendeter Instrumente sollte ein Inventar aller im Bereich Datenschutz **relevanter Dokumente** erstellt werden. Dazu zählen Richtlinien (z.B. im Bereich HR oder IT), Reglemente für einzelne Datensammlungen, vertragliche Vereinbarungen (z.B. bei Auftragsdatenverarbeitung oder Datentransfer), Zustimmungserklärungen oder konzernweite Datenschutzregeln ("Binding Corporate Rules").

Schliesslich sollten auch die unternehmensintern bestehenden **Prozesse** durchleuchtet werden: Welche Vorkehrungen zur Qualitätssicherung wurden getroffen (z.B. Audits, Zertifizierung), wie werden datenschutzrechtliche Vorfälle und Vorgänge abgewickelt (z.B. Meldung von "Data Leaks", Auskunfts- oder Berichtigungsgesuche), welche Anstrengungen werden im Bereich Ausbildung unternommen (z.B. interne oder externe Schulungen)?

3 IDENTIFIKATION, PRIORISIERUNG UND BEHEBUNG VON SCHWACHSTELLEN

Nach erfolgter Aufnahme des Ist-Zustands geht es darum, diesen dem **Soll-Zustand bei umfassender Compliance** gegenüber zu stellen und Problembereiche mit datenschutzrechtlichem Handlungsbedarf zu identifizieren. Die erkannten Schwachstellen sind nach Priorität zu ordnen.

3.1 IDENTIFIKATION TYPISCHER PROBLEMBEREICHE

In welchen Bereichen datenschutzrechtlicher Handlungsbedarf konkret besteht, kann nur im Einzelfall nach erfolgter Bestandsaufnahme beurteilt werden. Aus allgemeiner Erfahrung können die **nachfolgenden Unternehmensfunktionen als neuralgisch** eingestuft werden:

- **IT:** Bei der IT eines Unternehmens treten Lücken im Datenschutz oft dann auf, wenn einzelne Dienste intern zentralisiert oder an externe Provider ausgelagert werden. Akzentuiert zeigt sich das bei der Verlagerung von Daten in die Cloud, wo das Unternehmen oft nicht mehr weiss (geschweige denn beeinflussen kann), in welchem Staat die Daten letztlich gespeichert werden. Handlungsbedarf besteht zudem regelmässig im Bereich der IT-Sicherheit (z.B. fehlende Abstufung von Autorisierungen zum Datenzugriff).

- **HR:** Im gesamten Personalbereich werden meist besonders schützenswerte Daten (z.B. Gesundheitsdaten bei Krankheit oder Unfall) oder Persönlichkeitsprofile (z.B. Bewerbungsdossier mit Zeugnissen, Assessments) erhoben und bearbeitet. Entsprechend sind hier die Anforderungen an die Datenschutzkonformität höher. Häufige Schwachstellen finden sich im Rekrutierungsprozess (z.B. Aufbewahrung von Personaldossiers abgelehnter Bewerber), bei der Regelung der Nutzung von Geschäftsinfrastruktur (Internet, E-Mail) für private Zwecke oder von privater Infrastruktur für geschäftliche Zwecke ("Bring Your Own Device"), bei der Frage der Zulässigkeit von Mitarbeiterüberwachungen sowie beim Umgang mit Personendaten bei Abwesenheit oder Austritt eines Mitarbeitenden.

- **Marketing / Verkauf:** In Marketing und Verkauf finden umfassende Datenbearbeitungen statt, beispielsweise zum Zwecke der Auswertung von Personendaten und Clusterbildung oder für Direktwerbemassnahmen. Hierbei werden häufig zentrale datenschutzrechtliche Grundsätze wie Transparenz (Weiss der Einzelne, wozu seine Daten verwendet werden?), Zweckbindung (Ist ein Bearbeitungszweck legitim?) und Verhältnismässigkeit (Werden nur so viele Daten wie notwendig bearbeitet?) strapaziert.

- **Records Management:** Die Datenaufbewahrung stellt ein Stiefkind in der Datenschutz-Compliance dar. Oft fehlen klare Vorgaben zur Datenarchivierung (z.B. Dauer, Form), oder es wird von unzutreffenden Voraussetzungen ausgegangen (z.B. ausschliessliche Orientierung an der handelsrechtlichen Aufbewahrungspflicht).

- **Kommunikation:** Unter dem Oberbegriff der Kommunikation werden alle Unternehmensaktivitäten im Bereich der Offline- und Online-Medien verstanden, insbesondere Websites, soziale Netzwerke, Posts und Blogs. Datenschutzhinweise sind auf Websites inzwischen zwar weit verbreitet, werden jedoch oft unreflektiert von anderen Quellen übernommen und sind entsprechend nicht mit dem konkreten Onlineauftritt des Unternehmens abgestimmt.

> "In welchen Bereichen datenschutzrechtlicher Handlungsbedarf konkret besteht, kann nur im Einzelfall nach erfolgter Bestandsaufnahme beurteilt werden."

Weitere Gebiete, die einer vertieften Beurteilung unterzogen werden sollten, ergeben sich aus der Branche und den spezifischen Geschäftsfeldern des jeweiligen Unternehmens (z.B. Sensibilität der Daten in der Gesundheitsbranche, umfassendes Data Mining im Einzelhandel).

3.2 PRIORISIERUNG DER AKTIVITÄTEN

Die mögliche Vielzahl von Bereichen mit Handlungsbedarf wird häufig eine parallele Umsetzung nicht zulassen. Zur Bündelung der Ressourcen sollten die einzelnen Defizite somit **gestaffelt beseitigt** werden, womit sich die Frage nach der Rangfolge stellt.

Zur Priorisierung der Massnahmen empfiehlt sich die analoge Anwendung einer **Risikomatrix**: Als Kriterien stehen hierbei die Eintrittswahrscheinlichkeit eines Datenschutzverstosses und die Auswirkungen im Falle einer Verletzung im Zentrum (z.B. Anzahl betroffener Personen, Schwere der Verletzung, negative Publizität und mögliche Reputationsschäden, Gefahr von zivilrechtlichen Forderungen, eines vom EDÖB initiierten Verwaltungsverfahrens oder gar strafrechtlicher Sanktionen).

Die Rangfolge kann durch **zusätzliche Faktoren** beeinflusst werden, wie etwa die Gelegenheit zur Integration konkreter Massnahmen in bereits laufende oder unmittelbar bevorstehende Projekte oder die Möglichkeit, mit Überbrückungslösungen zu arbeiten.

Unter dem Aspekt der Priorisierung haben international tätige Konzerne auch zu entscheiden, wie sie die **Compliance in einer Vielzahl von Staaten** sicherstellen. Hierbei bewährt sich ein gestaffeltes Vorgehen, bei dem die Umsetzung in einem Staat (meist am Ort der Konzernzentrale oder im wichtigsten Markt) initiiert wird und auf dieser Basis anschliessend auf weitere Länder (unter Involvierung dortiger interner Rechtsabteilungen oder externer Berater) ausgedehnt wird.

3.3 UMSETZUNG VON MASSNAHMEN

Welche Massnahmen im konkreten Fall zur Herstellung der Datenschutz-Compliance umgesetzt werden sollen, lässt sich nicht allgemein beantworten. Das **Spektrum möglicher Massnahmen** ist sehr breit und umfasst im Wesentlichen die folgenden Elemente:

- Gänzliche **Einstellung oder Anpassung** einer nicht konformen Datenbearbeitung;

- **Information** der Betroffenen, evtl. gekoppelt an die Einholung von deren **Zustimmung** zu einer konkreten Bearbeitung;
- Erstellung oder Anpassung **vertraglicher Regelungen**, von **Richtlinien oder Bearbeitungsreglementen**;
- **Registrierung** von Datensammlungen beim EDÖB;
- organisatorische Massnahmen wie die Ernennung eines **internen Datenschutzbeauftragten**;
- Einrichtung bzw. Anpassung und Dokumentation der erforderlichen **Prozesse**;
- interne und externe **Information und Kommunikation**;
- **Schulung und Kontrolle**.

4 SCHLUSSBEMERKUNGEN

Die obigen Ausführungen zeigen, dass der Datenschutz heutzutage ein **bedeutendes Element der unternehmerischen Compliance** darstellt. Compliance-Programme tragen dazu bei, die Konformität mit den jeweils anwendbaren rechtlichen Bestimmungen sicherzustellen und dem Unternehmen ein gutes datenschutzrechtliches Prädikat zu verleihen.

Damit ein Compliance-Programm das verfolgte Ziel erreicht, muss es umsichtig geplant werden und von Beginn weg mit der erforderlichen "**Management Attention**" ausgestattet und juristisch begleitet werden.

Kontakte

Der Inhalt dieses Newsletter stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an Ihre Kontaktperson bei Schellenberg Wittmer oder an eine der folgenden Personen:

In Zürich:

Roland Mathys

Partner
roland.mathys@swlegal.ch

Andrea Mondini

Partner
andrea.mondini@swlegal.ch

In Genf:

Philippe Ducor

Partner
philippe.ducor@swlegal.ch

Virginie A. Rodieux

Rechtsanwältin
virginie.rodieux@swlegal.ch

SCHELLENBERG WITTMER AG / Rechtsanwälte

ZÜRICH / Löwenstrasse 19 / Postfach 1876 / 8021 Zürich / Schweiz / T +41 44 215 5252
GENF / 15bis, rue des Alpes / Postfach 2088 / 1211 Genf 1 / Schweiz / T +41 22 707 8000
SINGAPUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapur 049909 / www.swlegal.sg

www.swlegal.ch