

## Modernes Datenschutzmanagement – eine lohnende Investition?

Die Anforderungen an ein modernes Datenschutzmanagement zu formulieren ist schwierig aber wichtig um das Thema in einem Unternehmen überhaupt in Gang zu bringen.

Ausgangspunkt für ein Datenschutzmanagement kann die Festlegung wichtiger Ziele sein, die dann zunächst pragmatisch umgesetzt werden. Dieser zwar nicht unbedingt wissenschaftliche Weg erleichtert den Start und führt relativ schnell zu einem gewissen Datenschutzniveau. Der Weg zu einem „perfekten“ System wird dadurch nicht verbaut. Eine leistungsfähige Softwarelösung unterstützt diesen Prozess. Die Kosten sind im Vergleich zu dem erzielbaren Nutzen gering.

### Ausgangslage

Das BDSG ist im Bezug auf die Aufgaben des Datenschutzbeauftragten recht eindeutig : Er hat auf die Einhaltung relevanter Gesetze hinzuwirken, insbesondere hat er die Ordnungsmäßigkeit von DV-Programmen zu überwachen und den Mitarbeitern das Thema Datenschutz näher zu bringen. Es ist geregelt, dass der DSB rechtzeitig über Projekte im Unternehmen zu informieren ist und in welchen Fällen er vorab eine Prüfung durchführen muss. Klar ist auch, welche Informationen ihm zur Verfügung gestellt werden müssen. Auch daran, dass bestimmte Arten von Daten und der Einsatz moderner Technik ein besonderes Augenmerk verlangen, hat der Gesetzgeber gedacht. Dass sich die Eindeutigkeit der gesetzlichen Regelung auf eine sehr abstrakte Ebene beschränkt, hat jeder, der einmal angefangen hat sich mit dem Thema Datenschutz zu beschäftigen schnell erkennen müssen.

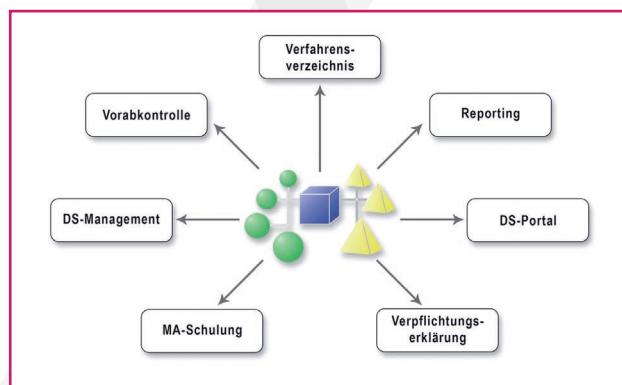
Schon allein die Anzahl der Aufgaben mit unterschiedlichsten Anforderungen ist enorm. Die gut gemeinten Hilfestellungen des Gesetzgebers (...die verantwortliche Stelle hat zur Verfügung zu stellen..., ...der DSB ist zu unterrichten..., ...der DSB nimmt in Empfang...) beschreiben aber die anspruchvollste Aufgabe: die Einführung eines Datenschutzmanagements (oder einer "Datenschutzorganisation") im Unternehmen! Alle Bereiche oder Prozesse eines Unternehmens müssen überprüft werden. Kontrollmechanismen müssen implementiert werden. Verantwortlichkeiten und Schnittstellen sind festzulegen. Ohne ein entsprechendes "Commitment" mit allen Konsequenzen der Unternehmensleitung kann dies nicht funktionieren .

### Vorgehensmodell

Die Schaffung der Rahmenbedingungen ist ein unternehmensweites Projekt und dabei abhängig von der Unternehmensstruktur, vorhandenen Abläufen oder Prozessen, gewählten Managementsystemen und auch der Unternehmensphilosophie. Ein einheitliches Vorgehensmodell kann es daher nicht geben. Zudem fehlen oft die Ressourcen für eine strategische und "korrekte" Projektplanung und -durchführung.

Ausgangspunkt für eine Grobplanung dieses Projekts kann die Festlegung von Zielen sein, die durch das Datenschutzmanagement erreicht werden sollen (Abb. 1):

- Es muss eine Verfahrensübersicht geben, die alle wesentlichen Informationen für eine datenschutzrechtliche Beurteilung enthält.
- Daraus wird das Verzeichnis abgeleitet.
- Die Vorabkontrolle baut ebenfalls darauf auf und muss nachvollziehbar sein.
- Nicht zu vergessen der technische Aspekt : Die IT-Security muss erkennen können, welche datenschutzrechtlichen Anforderungen zu erfüllen sind.
- Die Mitarbeiter müssen einbezogen werden können: Hierzu gehören Sensibilisierung, Schulung und Verpflichtungserklärung mit der entsprechenden Nachweisbarkeit.
- Es werden Mechanismen benötigt, um gegenüber internen und externen Stellen Auskünfte erteilen zu können und Transparenz zu gewährleisten.



### Die Umsetzung

Mit den Zielen als Meilensteine könnte jetzt begonnen werden, das Projekt in Phasen zu gliedern, verschiedene Teilprojekte zu definieren, Aufgaben und Zuständigkeiten zu verteilen und einen Zeitplan festzulegen. Mit den entsprechenden Ressourcen im Hintergrund ein lohnender Ansatz.

Ein pragmatischer Ansatz könnte dagegen so aussehen:

- Die überzeugte Unternehmensleitung teilt mit, dass das Projekt Datenschutzmanagement gestartet wird.

- Der Datenschutzbeauftragte informiert alle Beteiligten über Sinn und Zweck des Datenschutzes und des Projekts. (Bedenken und Vorbehalte sollten ernst genommen und zerstreut bzw. abgebaut werden. Wenn an dieser Stelle wichtige Entscheidungsträger und Meinungsbildner im Unternehmen nicht ins Boot geholt werden, wird das Projekt scheitern.)
- Es wird geprüft und festgelegt, welche Werkzeuge zum Erreichen der Ziele verwendet werden sollen (Anforderungen hierfür werden im Anschluss noch gezeigt).
- Die ausgewählte Lösung wird implementiert und es wird mit der Dokumentation bestehender Verfahren begonnen - ohne Rücksicht auf Vollständigkeit oder übermäßige Genauigkeit. Wichtiger ist es, überhaupt einmal zu erfahren, wo denn überall personenbezogene Daten verarbeitet werden. Zu Beginn wird der DSB die Fachabteilung erheblich unterstützen müssen, mit der Zeit werden Kenntnisse und Fähigkeiten jedoch wachsen und zu einer Entlastung des DSB führen.
- Der DSB sensibilisiert alle Mitarbeiter, die mit personenbezogenen Daten umgehen.
- Alle Mitarbeiter, die mit personenbezogenen Daten umgehen werden geschult und auf das Datengeheimnis verpflichtet.
- Der DSB überprüft die erfassten Verfahren und führt eine Qualifizierung und Priorisierung durch. Daraus kann er jederzeit ablesen, wo weitere "Datenschutzressourcen" investiert werden müssen.
- Der DSB führt Vorabkontrollen für neue Verfahren (und besonders sensible, bestehende Verfahren) durch.
- Die Fachabteilungen arbeiten fortlaufend an der Vervollständigung und Aktualisierung der Verfahrensdokumentationen.

## Welche Tools?

Als Werkzeuge kommen grundsätzlich Vorlagen, Checklisten und Tabellen die mit Word oder Excel editiert werden oder Softwarelösungen in Frage.

Als Softwarelösungen kann eine Standardanwendung erworben werden oder es wird eine eigene Lösung entwickelt. Wichtiges Kriterium für den Einsatz ist die Frage, ob das Tool unternehmensweit von unterschiedlichsten Anwendergruppen genutzt werden soll oder nur vom DSB selber.

Wurde die Entscheidung zur Einführung eines Datenschutzmanagements getroffen, kann konsequenter Weise die Entscheidung nur für eine unternehmensweit verfügbare Softwarelösung fallen. Textdokumente und Tabellen können eine Datenbank nicht ersetzen.

Die Entscheidung "make or buy" wird angesichts vorhandener Lösungen am Markt mit sehr gutem Preis-/Leistungsverhältnis in der Regel zu Gunsten von "buy" ausfallen.

## Anforderungen

Welche Anforderungen eine Lösung erfüllen muss, hängt von

zahlreichen Faktoren ab. Unternehmensgröße und -struktur sind dabei sicher entscheidend. Als Anhaltspunkte können folgende Kriterien dienen:

### Technische Anforderungen

- Zentrale Installation, einfach zu administrieren
- Zugriff über Standardbrowser ohne weitere Software auf den einzelnen Clients
- Schnittstelle zu vorhandenen Benutzerverzeichnissen
- Benutzerverwaltung mit rollenbasiertem Berechtigungskonzept
- Benutzerfreundliche, einfache Dateneingabe (z.B. Fragebogen zur Datenerfassung)

### Inhaltliche Anforderungen

- Verfahrensverzeichnis (interne Verfahrensübersicht mit allen Informationen, die für eine datenschutzrechtliche Beurteilung notwendig sind und externes Verzeichnis für Jedermann)
- Vorabkontrolle (mit abschließender "Freigabe")
- Mitarbeiterschulung als webbasiertes Training (mit Protokollierung der Durchführung)
- Verpflichtungserklärung (online mit Protokollierung)
- Flexible Reportingfunktion (für interne und externe Berichte)
- Todo-Liste, Übertragung von Aufgaben an andere Benutzer
- Für jeden Mitarbeiter zugängliches Informationsportal

### Der Nutzen

"Schön, aber was kostet mich so eine Lösung und wo sind die Vorteile?" wird der (bereits für das Thema Datenschutz sensibilisierte) Chef fragen. Die Antwort des DSB auf diese Frage wird entscheiden, ob sich die Investition aus Sicht der Unternehmensleitung lohnt.

Der Nutzen liegt zunächst einmal im optimierten Einsatz vorhandener Ressourcen:

- Aufgaben werden verteilt und dort erledigt, wo es am effizientesten ist.
- Dabei sichern die einfache, intuitive Handhabung und zahlreiche Hilfestellungen die hohe Qualität der erfassten Daten.
- Jeder kann auf das Tool zugreifen, wobei sichergestellt ist, dass jeder nur das zu sehen bekommt, was auch für ihn bestimmt ist!
- Das Ausdrucken oder auch das Versenden von Dokumenten kann entfallen.
- Die Mitarbeiter werden an ihrem Arbeitsplatz geschult, ohne Störung des gewohnten Arbeitsablaufs.
- Auswertungen, Reports und übersichtliche Listen mit einer Qualifizierung vorhandener Verfahren stellen sicher, dass der Status des Datenschutzmanagements jederzeit erkennbar ist (Abb. 2).