Erläuterungen betreffend die „Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem“

Gemäss Art. 4 Abs. 3 der Verordnung über die Datenschutzzertifizierungen (VDSZ) hat der Beauftragte Richtlinien zu erlassen, die sich hauptsächlich auf ISO/IEC 27001:2005 „Anforderungen für Informationsmanagementsysteme (ISMS)“ stützen, und gleichzeitig das **Schwergewicht Datenschutz** wahren.

Um dem zu entsprechen, ging es in einem ersten Schritt darum, von ISO 27001 die allgemeinen Anforderungen an Managementsysteme zu übernehmen, die ihrerseits aus den wichtigen Anforderungen von ISO 9001 für das Qualitätsmanagement stammen, wie sich dies aus dem informativen Anhang C von ISO 27001 ergibt. Das Schwergewicht Datenschutz ergibt sich teilweise aus zwei Einführungskapitel, d.h. „2. Normative Verweisungen“ und „3. Begriffe und Definitionen“, hauptsächlich aus dem Kapitel „**4. Managementsystem**“ insbesondere mit seinem Punkt **4.2.1** „Erstellung des Systems“ und, rein interpretativ in den beiden ersten „0. Einleitung“, „1. Anwendungsbereich“ und den vier letzten Kapiteln „5. Verantwortung des Managements“, „6. Interne Audits“, „7. Managementbewertung“ und „8. Verbesserungen“.

Die Hauptschwierigkeit bestand darin, den Akzent mehr auf den Datenschutz als auf die Informationssicherheit zu setzen. Über Art. 7, der die durch das DSG auferlegten Voraussetzungen der Datensicherheit deckt, kann man glücklicherweise den Datenschutz als Gesamtziel betrachten, das durch eine Verallgemeinerung dasjenige Ziel der in ISO 27001 verfolgten Datensicherheit. Damit zielt man darauf ab, ein Datenschutzmanagementsystem zu erstellen, das unter anderem eine Politik des ISMS, eine Auswahl von Massnahmen für die Behandlung von Nichtkonformitäten, eine Erklärung zur Anwendbarkeit der umgesetzten Massnahmen mit einer Begründung betreffend derjenigen, die ausgeschlossen wurden, einem Behandlungsplan der Nichtkonformitäten, einer Überprüfung/Nachprüfung der Datenschutz-Verletzungen oder –Zwischenfälle, und der Korrektur- oder Vorbeugungsmassnahmen zur Verbesserung des ISMS.
Der Knackpunkt dieser Schwergewichtung Datenschutz befindet sich zweifellos im Risikomanagement, das den Ausgangspunkt bildet, ein ISMS zu erstellen und zu verwalten. Wenn ein solches Risikomanagement gut an die « internen » Informationssicherheitsziele angepasst ist, ist es dagegen überhaupt nicht was die « externen » Datenschutzvoraussetzungen betrifft. Ein DSMS muss somit zwingend ein **Konformitätsmanagement** dem Risikomanagement assoziieren, wobei letzteres für die Aspekte der Datensicherheit beibehalten wird (vgl. Prinzip/Ziel/Artikel 7).

Konkret besteht die **Bewertungsmethode** der Nichtkonformität aus einer Analyse der Nichtkonformität, die nach der Identifikation der Nichtkonformitätsquellen in eine Einschätzung der Nichtkonformität mündet, in der Regel auf eine Skale mit zwei Werten: erhebliche und leichte Nichtkonformität.

Dagegen ist **keine Einschätzung der Nichtkonformität möglich**, da eine Nichtkonformität weder akzeptiert (keine restliche Nichtkonformität ab ein hypothetisches akzeptables Niveau), noch übertragen werden kann! Mit anderen Worten muss eine Nichtkonformität zwingend durch geeignete Massnahmen **behandelt** oder aber beispielsweise durch den **Verzicht** auf die betreffende Datenbearbeitung vermieden werden.

In einem zweiten Schritt ging es darum, den normativen Anhang A von ISO 27001, der aus dem Inhaltsverzeichnis der Norm ISO/IEC 27002:2005, bekannter unter dem Namen „Leitfaden zum Management von Informationssicherheit“ besteht, zu übernehmen. Dieser besteht aus 15 Kapiteln, wovon die 11 letzten die „Kontrollgruppen“ bilden, die ihrerseits in 39 „Kontrollziele“ unterteilt sind und zu insgesamt 133 „Kontrollmassnahmen“ führen. Daraus ergibt sich das **Schwergewicht Datenschutz**, da die **Massnahme 15.1.4**, die den „Datenschutz und Vertraulichkeit von personenbezogenen Informationen“ betrifft und die in der Substanz vorschreibt, dass „diese gemäss den Rechtsnormen, Reglementen und allfällig anwendbaren Vertragsbestimmungen gewahrt sein müssen.“

Im Blickwinkel einer Datenschutzzertifizierung von Organisationen oder von Verfahren, versteht sich von selbst, dass diese sehr generelle Massnahme detailliert und in Unterziele unterteilt werden muss, die ihrerseits in konkrete Massnahmen umzusetzen sind. Dies ist nun im Rahmen einem „**Leitfaden für die Umsetzung der DSMS-Richtlinien**“ erfolgt, das den Anhang der **„Richtlinien über die Mindestanforderungen an das DSMS**“ bildet. Gestützt auf das Beispiel der OZDE und anderen Ländern wie Australien, Kanada und Grossbritannien, haben wir „**9 Datenschutzgrundsätze**“ als Hauptzwecke dieses „Leitfadens für die Umsetzung der DSMS-Richtlinien“ definiert. Diese Grundsätze bestehen aus 20 konkreten Datenschutzmassnahmen, die in nicht abschliessender Art die wichtigsten Voraussetzungen, die dem Gesetz oder seiner Vollzugsverordnung entspringen. Um das Lesen zu erleichtern und zum besseren Verständnis dieses Anhangs, ist jede Massnahme gemäss dem Standard ISO 27002 strukturiert, von dem sie eine spezielle Ausweitung für den Datenschutz bildet. Gleich wie die ISMS-Massnahme 15.1.4 ihrerseits auf ein DSMS verweist, muss hier noch hervorgehoben werden, dass das 7. Ziel „Datensicherheit“ mit seinen assoziierten Massnahmen nichts anderes als ein Verweis des DSMS auf ein ISMS ist. Unter den 133 bestehenden Sicherheitsmassnahmen von ISO 27002 wurde vor allem eine Vorselektion der für den Datenschutz relevantesten Massnahmen gemacht.

Auch wenn es ausser Frage steht, für den Erhalt einer DSMS-Zertifizierung eine ISMS-Zertifizierung vorauszusetzen, so wird doch der Umfang der Anerkennung einer bestehenden ISMS-Zertifizierung, insbesondere was die Voraussetzungen gemäss Art. 7 DSG betrifft, im Einzelfall durch den Zertifizierer abgewogen und entschieden werden müssen. Was die Akkreditierung durch die SAS betrifft, ist es dagegen möglich, dass die DSMS-Akkreditierung als Ausweitung der ISMS-Akkreditierung (ISO 27001) vorgesehen werden könnte, aufgrund der engen und ausdrücklichen Beziehung zu den Voraussetzungen dieser internationalen Norm.

Für alle betroffenen Akteure (Akkreditierer, Zertifizierer, Zertifizierte, Auditierer, Kontrolleure, etc.) muss betont werden, dass das zur Zeit bestehende enge Verhältnis mit den internationalen Normen ISO 27001 et 27002 aufgrund ihrer weltweiten Anerkennung und Durchdringung auf dem Weltmarkt klug und vorteilhaft ist, sowie aufgrund ihrem wertvollen Beitrag betreffend Terminologie, Struktur und Systematik. Dieser normative Zusammenhang ist oder wird übrigens schon bald erweitert werden durch zusätzliche Leitfäden wie ISO 27003 « Umsetzung des ISMS », ISO 27004 « Metrik und Messbarkeit », ISO 27005 « Risikomanagement », ISO 27006 « Akkreditierungsvoraussetzungen » oder aber ISO 27007 « Audits von ISMS».

Schematisch kann die Hierarchie der normativen Bestimmungen wie folgt dargestellt werden: