Mengenlehre

Dirk Fox

Vereinigungsmenge

Wiewohl im Titel dieser Zeitschrift durch ein lapidares „und“ verbunden, stehen Datenschutz und Datensicherheit in der Praxis in einem speziellen, nicht immer gespannten Verhältnis zueinander.

So ist die Entwicklung des Datenschutzrechts einerseits geprägt von einer wachsenden Fokussierung auf die automatisierte Datenverarbeitung. Kein Wunder, bieten heute moderne Datenbank Anwendungen doch in den Anfängen des Datenschutzrechts nicht geahnte Möglichkeiten zur Verknüpfung, Auswertung und Interpretation digitaler Angaben über natürliche Personen. Auch werden in wachsendem Umfang herkömmliche Papier-Akten durch elektronische Pendanten ersetzt. Hinzu kommt die zunehmende Protokollierung von Transaktionen, beispielsweise bei Internet-Anwendungen (Online-Banking, Online-Shopping). Die Gesetzgebung trägt somit der wachsenden „Digitalisierung“ der Verarbeitung personenbezogener Daten in angemessener Weise Rechnung.

Aus dieser Entwicklung folgt konsequent, dass für personenbezogene Daten in IT-Systemen besondere Schutzmaßnahmen technischer und organisatorischer Art zu fordern sind, um diese vor unberechtigtem Zugriff, Veränderung und Löschung zu schützen. Das BDSG konkretisiert diese Anforderungen in der Anlage zum § 9 – wenn auch mit etwas verstaubt anmutender Begrifflichkeit. Datenschutz und Datensicherheit wachsen erkennbar zusammen.

Schnittmenge

Ist somit Datensicherheit als ein Spezialgebiet des Datenschutzes zu verstehen? Und sinnvoller Weise gar der Datenschutzbeauftragte in Personalunion mit dem Sicherheitsbeauftragten zu bestellen?

Nun – den Sicherheitsbeauftragten dieser Welt zur Beruhigung – so einfach ist die Wirklichkeit natürlich nicht. Klar: Der Datenschutz fokussiert auf personenbezogene Daten. Andere Arten sensibler digitaler

Informationen wie Betriebsgeheimnisse werden vom Datenschutz nicht erfasst. Auch der Missbrauch informationstechnischer Infrastrukturen – Bandbreite, Speicherbereiche, Webserver etc. – sind kein Thema des Datenschutzes, wohl aber des IT-Sicherheitsbeauftragten. Weite Bereiche der IT-Sicherheit sind datenschutzrechtlich gar nicht relevant.

Bilden Datenschutz und Datensicherheit also gewissermaßen eine Schnittmenge, in der sich der organisatorische und technische Schutz personenbezogener Daten als gemeinsames Interesse finden?

Leider greift auch dieses gerne bemühte Bild zu kurz. Denn wohl verstandene IT-Sicherheit erzeugt ihrerseits personenbezogene Daten – in Log-Files und Protokollen von Sicherheitssystemen wie Firewalls, Intrusion Detection Systemen und Virenfiltern. Damit wird die IT-Sicherheit selbst zum Gegenstand des Datenschutzes – bei Personalunion von IT-Sicherheitsbeauftragtem und Datenschutzbeauftragtem sind diesbezügliche Interessenskollisionen vorhersagbar.

Leere Menge

Schlimmer noch: Rollenmodelle für die Rechtevergabe in IT-Systemen erfordern privilegierte „Alleswisser“ – die Administratoren; datenschutzrechtlich ein Graus und, mehr noch als anfallende Logfiles, unvermeidlicher Zankapfel. Denn bisher gibt es dazu wenig Alternativen. Auch wenn sich durch personalisierte Accounts, Rollen und manipulationssichere Logfiles das Wirken der Administratoren – auch zum Schutz der Administratoren selbst – einigermaßen kontrollieren lässt, bleibt die Tatsache, dass sie in erheblichem Umfang über Zugriffsberechtigungen verfügen, die einem engen Verständnis von Zweckbindung und Erforderlichkeitsprinzip widersprechen.

Umgekehrt fordert die „Eingabekontrolle“ in der Anlage des § 9 BDSG, „dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen

eingetragen, verändert oder entfernt worden sind“ – eine Horrervorstellung für einen IT-Verantwortlichen, bedeutet dies doch, konsequent umgesetzt, einen beispiellosen Protokollierungsumfang, beispielsweise bei Datenbanken, der von marktüblichen Produkten meist nicht unterstützt wird und zudem die Speicherung und regelmäßige Kontrolle einer gigantischen Menge personenbezogener Daten nach sich zöge.

Zu diesem Heft

Für dieses Heft haben wir einen Schwerpunkt gewählt, in dem sich Datenschutz und Datensicherheit grundsätzlich einig sind: Audit und Zertifizierung als Maßnahme der Selbstregulierung, orientiert an etablierten „best practices“ und Standards. Bei diesem Thema liegt zumindest im Datenschutz noch ein Stück Weg vor uns, während sich in der IT-Sicherheit bereits internationale Standards wie ISO 2700x als Grundlage für Zertifizierungen von IT-Infrastrukturen etabliert haben. *Gerhard Weck* fasst in seinem Beitrag die Erfahrungen mit einer der ersten Zertifizierungen nach ISO 27001 zusammen. *Karin Schuler* und *Volker Hammer* skizzieren aus der Datenschutzpraxis motivierte Anforderungen an Gegenstand und Zielsetzungen eines Datenschutzaudits. *Stefan Gora* stellt im Gateway etablierte Vorgehensweisen bei der Durchführung von Security Audits vor. Einen interessanten Weg beschreitet *Claus Simon* mit der von ihm vorangetriebenen Verankerung des Datenschutzes in einem IT-Grundschutz-Baustein – Datenschutz als Teilmenge einer IT-Sicherheitszertifizierung. Dass und wie ein anderer Best-Practice-Ansatz der IT, nämlich die Prozess-Perspektive von ITIL, Gewinn bringend auf den Datenschutz übertragen werden kann, zeigt *Martin Meints* in seinem Beitrag.

Ob nun Vereinigungs-, Schnitt- oder Leere Menge – lernen können Datenschutz und IT-Sicherheit noch Einiges voneinander.