DuD
Datenschutz und Datensicherheit

Das Protokollierungs-Dilemma

Dirk Fox

Gemäß der Anlage zu § 9 BDSG Nr. 5 ist durch technische und organisatorische Maßnahmen „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme *eingegeben*, *verändert* oder *entfernt* worden sind (Eingabekontrolle).“ Dies ist erforderlich, sofern der Aufwand in angemessenem Verhältnis zum Schutzzweck steht und soll die Kontrolle automatisierter Verarbeitungen personenbezogener Daten ermöglichen.

1 Dilemma

Die Protokollierung der automatisierten Verarbeitung personenbezogener Daten schafft ein Dilemma. Denn Protokolldaten im Sinne der Eingabekontrolle sind selbst personenbezogene Daten: Da nachvollziehbar sein muss, „von wem“ die Eingabe, Änderung oder Entfernung (Löschung) erfolgte, muss ein eindeutiges Personenkennzeichen (Name, Login-ID o.ä.) gespeichert werden. Auch die Protokollierung des Zeitpunkts ist für eine nachträgliche Überprüfung unverzichtbar.[1]

Bei Mitarbeitern, die mit der Verarbeitung personenbezogener Daten befasst sind, stellt eine solche Protokollierung ein Verfahren dar, das grundsätzlich dazu geeignet ist, „das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ – und solche Verfahren unterliegen nach § 87 Abs. 1 BetrVG der betrieblichen Mitbestimmung.

In jedem Fall ist die Protokollierung selbst als ein automatisiertes Verfahren der Verarbeitung personenbezogener Daten zu behandeln, im Verfahrensverzeichnis zu dokumentieren und mit geeigneten Löschfristen zu versehen. Etwas skurril mutet allerdings die Vorstellung an, dass auch jede Veränderung und Entfernung dieser Protokollierungsdaten wiederum zu protokollieren und diese Protokollierung selbst wieder als Verfahren zu betrachten ist – eine solche unbegrenzte Selbstbezüglichkeit war vom Gesetzgeber sicherlich nicht gewollt.

[1] Siehe auch Ernestus/Geiger in Simitis, Kommentar zum Bundesdatenschutzgesetz.

2 Schwierigkeiten

Auch stößt die Eingabekontrolle auf erhebliche Umsetzungsschwierigkeiten in der Praxis. Es beginnt damit, dass zahlreiche informationstechnische Systeme zur Verarbeitung personenbezogener Daten (wie insbesondere Datenbankanwendungen) gar keine Möglichkeit bieten, die erforderlichen Log-Informationen zu speichern (Ausnahme: SAP). In Adressdatenbanken werden immerhin oft Zeitpunkt und Bearbeiter-ID der Ersterfassung einer Adresse, manchmal auch der jeweils letzten Bearbeitung gespeichert, nicht aber eine Veränderungshistorie oder eine Löschung.

Schlimmer noch: Auf die verbreiteten handelsüblichen Datenbanken, die die jeweiligen Anwendungen nutzen, kann ein Administrator in der Regel unter Umgehung der Eingabeoberfläche direkt zugreifen. Bei einigen marktführenden Datenbanken lässt sich dieser Zugriff nicht einmal an ein Login binden, die Datenbank ist also für jeden Direktzugriff offen. Bei Änderungen im Direktzugriff erfolgt kein automatischer Log-Eintrag.

Eine besondere Herausforderung stellen Datenlöschungen dar: Will man die Löschung eines Datensatzes nachvollziehbar speichern, muss man das gelöschte Datum ebenfalls aufbewahren – was den Löschvorgang selbst ad absurdum führt. Versucht man, die Protokollierungsanforderungen auf typische automatisierte Verarbeitungen, die in jedem Unternehmen vorkommen, anzuwenden, kommt man zu eigenwilligen Resultaten. Beispielsweise werden in einer CRM-Datenbank, in der ein Unternehmen (wie heute üblich) alle Kundenkontakte dokumentiert, ununterbrochen Datensätze korrigiert (Adressänderungen, neue Telefonnummern, andere E-Mail-Adresse, geänderte Firmierung, neuer Tätigkeitsbereich oder Abteilungswechsel des Ansprechpartners, neuer Vertreter, Tippfehler in Name oder Adresse etc.). Kaum ein Datensatz in einem gepflegten CRM-System, der nicht im Laufe eines Jahres viele Male modifiziert wird. Hinzu kommen die Kontakteinträge: Telefonate, Vertriebsbesuche, E-Mailings, Post-Mailings. Für jede dieser Änderungen sind Zeitpunkt, Bearbeiter und Veränderung zu speichern. Die entstehende Log-Datei würde schnell den Umfang der eigentlichen Datenbank übersteigen. Ähnliches gilt für einen unternehmensweiten Kalender: Hier werden permanent Termine verschoben, Teilnahmen bestätigt oder abgelehnt, Räume oder Geräte umgebucht. Eine nachvollziehbare Protokollierung müsste die Rekonstruktion jeder Eintrags-Historie erlauben.

Schließlich müsste der betriebliche Datenschutzbeauftragte die Protokolle regelmäßig prüfen – zu welchem Zweck aber? Nach welchen Kriterien?

Fazit

Die Forderung einer nachvollziehbaren „Eingabekontrolle“ im BDSG erscheint überzogen und in der Datenschutzpraxis weder umsetzbar noch zielführend. Diese Anforderung geht deutlich über die entsprechende Bestimmung des BDSG 1990 hinaus – danach war lediglich „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme *eingegeben* worden sind (Eingabekontrolle).“

Weniger wäre hier mehr. Denn zweifellos wichtig ist die Nachvollziehbarkeit von Datenänderungen oder Löschungen mit datenschutzrechtlichem Hintergrund, wie beispielsweise von Betroffenen veranlasste Korrekturen. Die Protokollierung üblicher Korrekturvorgänge (Umfirmierung, Adressänderung etc.) sowie zulässige Ergänzungen oder Vervollständigungen sind für eine wirksame Datenschutzkontrolle hingegen verzichtbar. Viel wichtiger wäre vielmehr, Sperrungen und Übermittlungen nachvollziehbar zu protokollieren.

Die „Eingabekontrolle“ des BDSG führt in der Praxis zu Datensammlungen, die den Kern des Datenschutzes, den Schutz der Persönlichkeit vor unkontrollierter Speicherung und Verarbeitung, in sein Gegenteil zu verkehren drohen.