Die Datentrennung – ein altes Leid?

Das achte Gebot: Die Datentrennung

Die Anlage zu § 9 BDSG wirft in der Nummer acht viele Fragen für die Unternehmen auf: Wie steht es um die Trennung von Test- und Echtdaten in Entwicklungsumgebungen? Erfolgt eine technische und räumliche Trennung von pseudonymisierten Daten und Pseudonymbrücken? Wie ist es um die Mandantentrennung bestellt? Verarbeitet der Konzernverbund Daten nach dem Prinzip der Datentrennung? Heikle Fragen – Datenschutz PRAXIS zeigt Lösungen.

Im letzten Beitrag zur Serie der sogenannten acht Gebote aus der Anlage zu § 9 BDSG geht es um die Trennung der Daten. Das achte Gebot besagt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden müssen.

Mitarbeiterdaten aus der Zutrittskontrolle, die z.B. an den Türsicherungsanlagen erfasst werden, dürfen nach dem BDSG für keine anderen Zwecke Verwendung finden. Ein Abgleich zwischen Zutrittsdaten und Daten aus einer separaten Zeiterfassung verbietet sich somit.

Daten dürfen nur zweckgebunden erhoben werden

Dementsprechend spielt die Zweckbindung eine entscheidende Rolle bei der Datentrennung. Erlischt beispielsweise der Zweck, zu dem personenbezogene Daten erhoben, verarbeitet oder gespeichert wurden, sind die Daten zu löschen. Das gilt zumindest, sofern dem keine andere gesetzliche Verpflichtung oder übergeordnete Regelung nach Betriebsverfassungsgesetz als Betriebsvereinbarung entgegensteht.

Die Trennung sollte bereits bei der Planung berücksichtigt werden

Speichert ein Unternehmen also Daten etwa aus Zutrittskontrolle und Zeiterfassung zusammen, obwohl sie unterschiedlichen Zwecken dienen, ist es meist schwierig, Teile der Daten, deren Nutzungsberechtigung abgelaufen ist, zu löschen oder zu sperren.

Um späteren Problemen vorzubeugen, sollten Sie als Datenschutzbeauftragter darauf hinwirken, dass die Beteiligten bereits bei der Planung von Anwendungen und deren Datenspeicherung nach dem Gebot der Datentrennung vorgehen.

Reale personenbezogene Daten müssen mit fiktiven Informationen überschrieben werden, bevor sie in Entwicklungs- oder Testumgebungen zum Einsatz kommen, um die Anonymität ausreichend zu gewährleisten

Die gängige Praxis ist nicht immer legitim

Nicht immer unterliegt die Datenverarbeitung von personenbezogenen Informationen der legitimierten Praxis für die Verwendung von Daten. Zusätzliche Aufgaben, insbesondere zur Entwicklung oder Neugenerierung von Anwendungen, fordern „realitätsnahe“ Datenbestände. Doch Vorsicht – nicht selten werden dabei die gesetzlichen Vorgaben aus der gesamten Palette der acht Gebote ad absurdum geführt.

Das übliche Leid bei Test- und Produktivsystemen

Sofern Eigenentwicklungen in der IT-Umgebung getestet oder Anwendungsverfahren durchgeführt werden, steht grundsätzlich die Frage nach der Trennung von Test- und Echtdaten im Raum. Meist findet jedoch keine Trennung statt.

Üblicherweise bedienen sich Systementwickler und Programmierer bei den Produktivdaten, um möglichst reale Testszenarien durchspielen zu können. Dass dabei eine Kopie der aktuellen Produktivdaten eins zu eins

Pseudonymisierte Daten

Bei der Pseudonymisierung geht es um Identitätsverschleierung. Sie dient dem Ziel, weitere Daten über eine Person zu sammeln, ohne ihre Identität zu kennen.

Von der Pseudonymisierung zur Anonymisierung

Die Pseudonymisierung kann auf rücknehmbare Weise anhand von Referenzlisten für Identitäten und ihre Pseudonyme oder anhand von Zwei-Wege-Verschlüsselungsalgorithmen für die Pseudonymisierung erfolgen.

Identitäten können auch so verschleiert werden, dass eine Reidentifizierung nicht mehr möglich ist. Durch die dabei angewendete Einweg-Verschlüsselung entstehen gewöhnlich anonymisierte Daten.

Weitere Hinweise zur Begriffserklärung finden sich im Working Paper WP136 der Artikel-29-Datenschutzgruppe (*http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf*).

übernommen wird, halten viele für selbstverständlich.

Der Datenschutzbeauftragte rät zur Vorsicht!

Für Inhouse-Entwicklungen werden Sie als Datenschutzbeauftragter in der Regel kaum gegen oben genannte Praxis ankommen. Doch Vorsicht ist geboten, sofern die personenbezogenen Datensätze Feldinhalte nach § 3 Abs. 9 – sogenannte sensible Daten – oder meldepflichtige Daten entsprechend § 42a BDSG enthalten.

Verfälschung der Daten kann einen strengen Schutz gewährleisten

Gerade bei Entwicklungen in Personalsystemen muss zwingend der Schutz von Mitarbeiterdaten gewährleistet sein. In diesen Fällen empfiehlt es sich, die Testdaten mit zufälligen Zeichen- oder Zahlenfolgen im Namens- und Adressfeld sowie in den Daten zur Bankverbindung zu überschreiben.

Problematisch sind vor allem externe Entwicklungen

Weit gefährlicher kann unter Umständen die vollständige Weitergabe von Echtdaten an externe Dienstleister werden, die die Daten dann in sogenannten Testumgebungen einsetzen.

Eine Anonymisierung der personenbezogenen Daten wie im Kasten vorgestellt ist oberstes Gebot. Sind gar Sozialdaten im Sinne des § 80 SGB X (zehntes Sozialgesetzbuch) betroffen, müssen Sie ein besonderes Augenmerk auf die Testdaten haben. Aufgrund des besonderen Schutzbedarfs von Sozialdaten gelten noch strengere Anforderungen als nach dem BDSG.

Halten Sie die Pseudonymisierungsschlüssel unter Verschluss

Lassen sich Datensätze nach den Regeln der Pseudonymisierung verarbeiten, ist dies ein weiterer Weg, um eine Datentrennung zu gewährleisten. Dabei stehen die Pseudonymzuordnungen unter besonderer Aufsicht des Datenschutzbeauftragten. Die Nutzer der pseudonymisierten Datensätze dürfen dabei auf keinen Fall Zugriff auf die Zuordnungsschlüssel erhalten, damit sie die zugehörigen Personen nicht identifizieren können.

IT-Systeme sollten von Haus aus eine Mandantentrennung mitbringen

Insbesondere für Dienstleister, die für verschiedene Auftraggeber arbeiten, ist eine Mandantentrennung obligatorisch. Systeme wie die klassische Finanzbuchhaltung, Personalabrechnungssysteme oder SAP bieten von Haus aus eine wirkungsvolle Mandantentrennung an.

Achten Sie auch im Konzernverbund auf Datentrennung

Problematisch stellt sich oftmals eine datenschutzkonforme Datentrennung im Konzernverbund dar. Dabei landen nicht selten personenbezogene Daten, insbesondere von Kunden und Mitarbeitern, in einem gemeinsamen Topf. Die Praxis zeigt, dass dieser Fehler sehr häufig auftritt.

Optimal ist die physische Trennung

Die beste Basis einer wirksamen Datentrennung ist eine physische Trennung, also separate IT-Systeme mit entsprechenden Speichermedien.

Alternativ dazu lässt sich eine organisatorische Trennung einführen

Bedeutet dieser Schritt zu großen Aufwand, lässt sich oftmals zumindest eine rein organisatorische Trennung umsetzen. Dazu benötigen Sie allerdings eine saubere Berechtigungsstruktur mit eindeutiger Kennung auf die Herkunft der Daten. Unter Umständen ist daneben zusätzlich eine datenschutzrechtliche Zustimmung des Betroffenen notwendig.

Die acht Gebote auf einen Blick

Unter *www.datenschutz-praxis.de* finden Sie alle Beiträge zu den acht Geboten auf einen Blick. Einfach über die Suche gehen und „Gebot“ eingeben.

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (*www.keck-dsb.de*).

Prüffragen zur Datentrennung	Ja	Nein
Werden Daten, die für einen bestimmten Zweck erhoben wurden, auch für andere Zwecke verwendet?	☐	☐
Sind Daten in Testsystemen entsprechend anonymisiert?	☐	☐
Werden Pseudonyme und personenbezogene Daten strikt getrennt?	☐	☐
Sind Daten für verschiedene Auftraggeber getrennt?	☐	☐
Wird die Mandantentrennung in den Systemen konsequent angewendet?	☐	☐
Ist ein Backup- und Restore-Verfahren entsprechend den unterschiedlichen Speicherzwecken vorhanden?	☐	☐
Lässt sich im Archivsystem sauber nach den verschiedenen Datenquellen trennen?	☐	☐

Prüfbogen zur Datentrennung mit den wichtigsten Kontrollfragen für den Datenschutzbeauftragten. Die Checkliste finden Sie als Abonnent auch unter www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten.