„Kasus knaxus“ Protokollierung

Das fünfte Gebot: Die Eingabekontrolle

Die Eingabekontrolle zielt auf die Revisionsfähigkeit der Eingabe von personenbezogenen Daten ab, wobei dazu auch nicht vernetzte Einzelarbeitsplätze gehören. Die Eingabekontrolle soll dokumentieren, wer für eine unzuverlässige oder falsche Dateneingabe verantwortlich ist. Der „Kasus knaxus“ oder springende Punkt ist dabei die Protokollierung.

Die datenschutzrechtliche Regelung zur Eingabekontrolle findet sich in den technisch-organisatorischen Maßnahmen zum § 9 BDSG.

Nach Nr. 5 der Anlage gilt es Maßnahmen zu treffen, die „gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)“.

Das Gebot der Verhältnismäßigkeit

Ergänzend präzisiert § 9 Satz 2 BDSG: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“. Das ist vielleicht einer der Gründe, weshalb die Eingabekontrolle von vielen Datenschutzbeauftragten vernachlässigt wird …

Die vier Elemente der Eingabekontrolle

In der Regel funktioniert eine wirksame Eingabekontrolle durch die Protokollierung folgender vier Elemente:

1. Welcher Datensatz ist betroffen?
2. Welche Aktivität wurde durchgeführt (Neuanlage, Veränderung, Löschung)?
3. Wann war der Zeitpunkt der Aktivität?
4. Wer war die ausführende Person (Benutzeraccount)?

Zentral für die Eingabekontrolle ist die Nachvollziehbarkeit. Es muss also immer klar sein, durch wen die Eingabe, die Änderung oder die Löschung von Daten erfolgte.

Wer hat denn jetzt bitte schon wieder die Daten unbefugt verändert? Die Eingabekontrolle macht‘s nachvollziehbar.

Kasus knaxus ist der Datenschutz

Das setzt jedoch ein eindeutiges Personenmerkmal (Name, Login-Daten etc.) voraus. Die Protokollierung schafft also personenbezogene Daten, die der Datenschutzkontrolle unterliegen.

Schwierigkeiten bei der Umsetzung: Oft keine Änderungshistorie vorhanden

Vielfach stößt die Eingabekontrolle auf erhebliche Umsetzungsschwierigkeiten. Es beginnt damit, dass die Systeme zur Verarbeitung personenbezogener Daten in der Praxis häufig keinerlei Nachvollziehbarkeit bieten.

Viele Systeme speichern bei der Ersterfassung von Daten lediglich einen Zeitstempel mit Bearbeiter-ID. Eine Historie der nachfolgenden Änderungen am Datensatz oder gar die Dokumentation der Datenlöschung fehlt oft gänzlich.

Herausforderung Datenlöschung

Eine besondere Herausforderung für alle Systeme stellt die Datenlöschung dar. Die Protokollierungsanforderungen stoßen hierbei oft an ihre Grenzen, müsste man doch den Löschvorgang an sich aufbewahren.

Unkontrollierbare Hintertür für Admins

Allen Anwendungen gemeinsam ist die Tatsache, dass Entwickler oder Administratoren in der Regel unter Umgehung der üblichen Eingabeoberfläche direkt auf personenbezogene Daten zugreifen können. Bei vielen Datenbanken lässt sich dieser Zugriff nicht an eine wirksame Protokollierung binden. Jeder Direktzugriff über diese Hintertür ist also unkontrollierbar.

Datengrab Protokollierung

Eine nachvollziehbare Protokollierung müsste idealweise die Rekonstruktion jeder Eingabe oder Änderung erlauben. Aber wer will in einem umfangreichen Customer-Relationship-Management-System noch wissen, dass der Ansprechpartner eines Unternehmens einen neuen Tätigkeitsbereich bekam? Kommen noch Änderungen in den Kontaktdaten sowie Änderungen durch Tippfehler hinzu, entstehen Protokollinformationen, die niemanden interessieren. Zudem bläht sich die Log-Datei zum Datengrab auf.

Eingabekontrolle scheint überzogen

Die Forderung nach einer überprüfbaren Eingabekontrolle erscheint vielen DSBs überzogen. Zudem ist sie aufgrund der oben genannten Ausführungen oft schwer umsetzbar. Schließlich sollte der DSB die Logfiles regelmäßig prüfen – zu welchem Zweck, ist jedoch vielen unklar.

Schritt 1: Bestimmen Sie die betroffenen Anwendungen

Identifizieren Sie zuerst die Anwendungen zur Verarbeitung personen-

bezogener Daten. Welche Programme sind im Einsatz und erlauben eine Protokollierung? Wo ist die Eingabekontrolle wirklich erforderlich? Beispiele aus der Praxis sind üblicherweise:

- Zutritts- und Zeitkontrolle
- Personal-Informations- und Abrechnungssysteme
- SAP/ERP-Anwendungen
- CRM zur Kundenpflege
- Web-Shopsysteme
- Anlagen zur Videokontrolle
- Betriebssysteme
- Werkzeuge zur Fernwartung und zur Systemüberwachung

Schritt 2: Überprüfen Sie die Zugriffskontrolle

Basis einer wirksamen Eingabekontrolle ist eine funktionierende Zugriffskontrolle. Hilfestellung dazu finden Sie im Beitrag zum zweiten Gebot in der Dezember-Ausgabe 2010 der Datenschutz PRAXIS.

Schritt 3: Definieren Sie den Schutzzweck

Als Nächstes muss der jeweilige Schutzzweck festgelegt werden. Was ist in der Änderungshistorie eines Datensatzes entscheidend? Beispiele sind:

- Datum und Anwender-ID bei Neuanlage
- Historie zur Datensatzsperrung
- nachvollziehbare Übermittlung
- Änderung sensibler Daten nach § 3 Abs. 9 oder nach § 42a BDSG

Die Aufzeichnung von üblichen Korrekturvorgängen sowie zulässigen Ergänzungen sind für eine Datenschutzkontrolle hingegen oft verzichtbar.

Schritt 4: Lassen Sie Kontrollmaßnahmen festlegen

Als Letztes sollte die oder der Verantwortliche in der Fachabteilung Kontrollmaßnahmen festlegen. Das Änderungsprotokoll aus der Entgeltabrechnung z.B. ist sicherlich am besten bei der Personalleitung aufgehoben.

Schritt 5: Definieren Sie Zugriffsregeln

Grundsätzlich ist es notwendig, einen Dateiverantwortlichen mit fest definierten Zugriffsberechtigungen auf die Logfiles zu bestimmen. Einen allzu freien Zugang durch Benutzer gilt es aufgrund der Sensibilität von Logdaten auf jeden Fall zu vermeiden.

An die Übersicht als automatisiertes Verfahren denken!

Wie bereits erwähnt fallen im Rahmen der Eingabekontrolle erneut personenbezogene Daten an. Aus Sicht des Datenschutzes ist dazu eine entsprechende Übersicht als automatisiertes Verfahren zu erstellen.

Definieren Sie zwingende Löschfristen

Leider wird in der Praxis oft vergessen, Löschfristen zu definieren. Denn vom Grundsatz des Datenschutzes her dürfen personenbezogene Daten nur so lange aufbewahrt werden, wie ein Grund für ihre Speicherung besteht.

Der Betriebsrat ist tangiert

Logdaten stehen üblicherweise im Rahmen der Mitbestimmung nach § 87 Abs. 1 BetrVG im besonderen Fokus der Betriebsräte, eignen sich die Protokolldaten doch grundsätzlich dazu, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Umsetzungsvorschlag der Landesdatenschutzbeauftragten Brandenburg

Als Zusammenfassung ein Vorschlag der LDA Brandenburg, wie sich die Eingabekontrolle realisieren lässt:

- Einsatz von Sicherheitssoftware
- Transaktionsprotokolle
- Festlegung, wer Daten eingeben darf
- Kennzeichnung von Erfassungsunterlagen mit Name und Datum nach Vollzug der Eingabe
- Protokollierung der Netzverwaltung, der Zugriffsrechte auf Dateien, der gescheiterten Zugriffsversuche und der Programmaufrufe
- Auswertung der Protokolle und Festlegung, zu welchen Zwecken sie verwendet und wie lange sie aufbewahrt werden dürfen
- Festlegung zu Veränderungen von Zugriffsrechten
- Festlegung Dateiverantwortlichkeit

Fazit: Kein Datenschutz-Dilemma!

Die Eingabekontrolle muss also kein Protokollierungs-Dilemma sein, wenn das Unternehmen die Regeln des Datenschutzes beachtet.

Hermann Keck

Prüfansatz	Erfüllt	Nicht erfüllt
Ist die Führung schriftlich erteilter, nachvollziehbarer Zugriffsberechtigungen geregelt?		
Wird eine Protokollierung von Eingabe, Veränderungen oder Löschung personenbezogener Daten durchgeführt?		
Sind der Veranlasser, der Grund einer Eingabe, einer Veränderung oder einer Löschung von personenbezogenen Daten nachvollziehbar?		
Gibt es Regelungen zu den Zugriffsbefugnissen auf erstellte Protokolldaten?		
Sind Löschungsregelungen für Protokolldaten vorhanden?		

Prüfen Sie die Eingabekontrolle anhand dieser Checkliste. Abonnenten finden die Checkliste im Word-Format unter www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten.