Orientierungshilfe „Protokollierung“

Herausgegeben vom
Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand 2. November 2009

Inhalt

1 Einleitung

Sowohl die Datenschutzgesetze der Länder als auch das Bundesdatenschutzgesetz enthalten Regelungen, aus denen sich die Pflicht zur Protokollierung ergibt oder zumindest ableiten lässt. In einigen Landesdatenschutzgesetzen findet man das Regelungsziel Revisionsfähigkeit, das insbesondere durch die Maßnahme der Protokollierung umgesetzt werden kann. Das Bundesdatenschutzgesetz (BDSG) und andere Landesdatenschutzgesetze normieren Kontrollziele wie Eingabekontrolle oder Verantwortlichkeitskontrolle, aus denen sich ebenfalls die Pflicht zur Protokollierung ableiten lässt. Im BDSG zeigt sich am Beispiel der Anlage zu § 9, dass praktisch keine der dort konkret aufgeführten technisch-organisatorischen Maßnahmen ohne das Vorsehen einer Nachweismöglichkeit, die typischerweise in Form eines Protokolls geschieht, umsetzbar ist. Für eine Reihe von Verwaltungsverfahren gelten zudem bereichsspezifische, vom Datenschutzrecht des Bundes bzw. des betreffenden Landes abweichende, oft wesentlich konkretere Protokollierungsvorschriften (Beispiele: Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze usw.).

Obwohl die Datenschutzgesetze von Bund und Ländern Regelungen enthalten, aus denen sich die Pflicht zur Protokollierung ableiten lässt, gibt es nur wenige Vorgaben für die konkrete Ausgestaltung der Protokollierung. Dennoch haben sich auf Basis der Anforderungen erprobte Vorgehensweisen entwickelt, die in diesem Text als grundlegende Empfehlungen dargestellt werden.

2 Grundsätze

Die Zweckbindung von Protokolldaten ist in den Datenschutzgesetzen von Bund und Ländern explizit geregelt (z. B. § 31 BDSG oder § 10 Abs. 6 DSG M-V). Die Protokollierung dient allein dem Zweck der Aufrechterhaltung von Datenschutz und Datensicherheit und darf grundsätzlich nicht für eine automatisierte Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden.

Alle Protokolldaten unterliegen also einer strikten Zweckbindung. Diese strikte Zweckbindung ist die Konsequenz aus dem Umstand, dass Protokollierungsdaten einen

umfassenden Einblick in die Tätigkeiten der Administratoren, Nutzer bzw. Anwender ermöglichen, sie aber auch für die genannten Kontrollzwecke erforderlich sind.
Für die Gestaltung der Protokollierungsverfahren gilt der **Grundsatz der Erforderlichkeit**. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderlichen Maß zu beschränken.

Für die technische Ausgestaltung und Auswahl der Verfahren der Protokollierung ist das Gebot der **Datensparsamkeit und Datenvermeidung** zu befolgen. Hierbei sind insbesondere die Möglichkeiten zur Pseudonymisierung oder Anonymisierung zu berücksichtigen. Im Falle der Pseudonymisierung ist das Verfahren darzustellen, mit dem die Zuordnung zwischen Person und Pseudonym geregelt ist.

3 Zweck und Anforderungen an eine Protokollierung

Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Entsprechend den allgemeinen Anforderungen an Datensicherheit und Datenschutz - oder allgemeiner: an Beweissicherheit und Revisionsfestigkeit – und der gleichzeitig auszuschließenden automatisierten Leistungs- und Verhaltenskontrolle der an der Datenverarbeitung beteiligten Personen, müssen Protokolldaten mit Personenbezug **zweckgebunden**, **vollständig** und **datensparsam** eingerichtet sein. Sie müssen die tatsächlich erfolgten Operationen, die beteiligten Anwendungen, Maschinen und Personen mit Zeitbezug korrekt dokumentieren. Dabei besteht regelhaft ein Zielwiderspruch zwischen der Vollständigkeit und der Datensparsamkeit. Dieser Konflikt lässt sich nur vor dem Hintergrund der verfahrensspezifischen Bedingungen so weit auflösen, um so einen bestmöglichen Ausgleich der Ziele zu erreichen. **Protokolldaten dürfen nicht nachträglich verändert werden können und nur Berechtigten zugänglich sein.**

Die ordnungsgemäße Funktion des Protokollierungsverfahrens und die Gültigkeit von Protokolldaten muss durch geeignete Tests sichergestellt werden. Diese sollten ein gezieltes Durchführen von zu protokollierenden Ereignissen und eine darauf folgende Überprüfung, ob diese Ereignisse sich in den Protokolldaten wiederfinden lassen, umfassen. Solche Tests sind immer dann notwendig, wenn die protokollierenden Systeme oder Systemteile verändert werden. Dies gilt insbesondere, wenn die Änderung am System einer datenschutzrechtlichen Freigabe bedarf.

Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptologischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden.

4 Arten von Protokolldaten

Bei der Protokollierung ist zwischen den Aktivitäten der Maschinen, der Administratoren sowie der Nutzer und Anwender zu unterscheiden. Administratoren können einen besonderen Einfluss auf die Strukturen eines IT-Systems ausüben, weshalb sie bei der Nutzung

administrativer Rechte einer besonderen Kontrolle unterliegen. **Die Nutzung administrativer Rechte muss zu einem Eintrag im Protokoll führen.**

Unter Nutzung administrativer Rechte sind üblicherweise Maßnahmen zur Installation, Modifikation und Konfiguration von Hard- und Software zu verstehen.

Während die Protokollierung der Maschinen und der administrativen Tätigkeiten den Charakter einer Systemüberwachung hat, dient die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung.

Beide Protokollierungsformen dienen dazu, die Ordnungsmäßigkeit der Datenverarbeitung nachzuweisen bzw. auf Anforderung nachweisen zu können.

4.1 Protokollierung administrativer Tätigkeiten

Es müssen die Ereignisse und Tätigkeiten protokolliert werden, die die Funktionsweise der informationstechnischen Geräte sowie der Programme, der Dateien, die Speicherorganisation und die Nutzungsrechte einer automatisierten Verarbeitung personenbezogener Daten verändern.

Dabei ist auch zu beachten, dass die Protokollierung auch explizit zum Schutz der Administratoren vor unberechtigten Vorwürfen hinsichtlich eines möglichen Missbrauchs dienen kann. Ohne eine entsprechende Protokollierung administrativer Tätigkeiten könnten solche Vorwürfe gegen Administratoren nicht nachhaltig entkräftet werden.

Administrationstätigkeiten, wie bspw. die Verwaltung einer Datenbank, müssen unter einer personalisierten Administrationskennung durchgeführt werden, während die restliche nicht-administrative Arbeit mit normalen Benutzerrechten unter der allgemeinen Nutzerprotokollierung erfolgt.

Es muss verhindert werden, dass
- ein ändernder Zugriff auf die Protokolldaten durch diejenigen Personen stattfinden kann, deren Tätigkeiten durch die Protokolldaten dokumentiert werden.
- ein lesender Zugriff auf die Protokolldaten aus anderen Gründen als der Aufrechterhaltung von Datenschutz und Datensicherheit erfolgen kann.

4.2 Protokollierung der Nutzung von IuK-Systemen

Bei der Benutzung von Verfahren zur automatisierten Verarbeitung personenbezogener Daten müssen die Tätigkeiten protokolliert werden, die zum Nachweis einer korrekten, rechtskonformen Verarbeitung notwendig sind.

Die Inhalte der Protokolldaten orientieren sich hierbei an der konkret durchgeführten Datenverarbeitung und am Schutzbedarf der verarbeiteten Daten. Näheres zur inhaltlichen Ausgestaltung findet sich im folgenden Abschnitt.

Üblicherweise müssen die Tätigkeiten der
- Authentifizierung und Autorisierung,
- der Dateneingabe und -veränderung,
- der Dateneinsicht,

- der Datenübermittlung und
- der Datenlöschung

protokolliert werden.

5 Qualität der Protokolldaten

Entsprechend dem Zweck der Protokollierung müssen die in Protokolldaten aufgeführten Aktionen so aggregiert werden können bzw. sein, dass sie der kontrollierenden Instanz helfen, einen Sachverhalt zu rekonstruieren und zu bewerten.

5.1 Inhalt

Protokolldaten müssen Auskunft geben über

- den Zeitpunkt einer Tätigkeit bzw. eines Ereignisses,
- die zutreffende Bezeichnung einer Tätigkeit oder eines Ereignisses,
- die mit der Tätigkeit oder dem Ereignis befasste Person bzw. Systemkomponente und
- den Zweck der Tätigkeit.

Der Zeitpunkt sollte anhand einer zumindest innerhalb der Organisation synchronisierten Zeitquelle bestimmt werden. Art und Weise der Zeitdarstellung müssen eindeutig und zumindest sekundengenau aufgelöst sein.

Die Darstellung der Tätigkeit bzw. des Ereignisses muss eindeutig Auskunft geben, welche Tätigkeit durchgeführt wurde bzw. welche Ereignisse und Operationen auf dem System stattfanden.

Auslöser eines zu protokollierenden Ereignisses ist in der Regel eine Person. Diese muss eindeutig bestimmbar sein. Grundsätzlich sollte die Person deshalb über einen direkt zuordbaren Bezeichner - beispielsweise durch eine personenbezogene Zugangskennung - benannt werden. Als weitere Auslöser agieren darüber hinaus aber auch Server, Dienste bzw. Services, die automatisiert Protokolldaten erzeugen.

Bei einem Zugriff, bei dem Daten geändert wurden, muss die geänderte Teilmenge klar eingegrenzt benannt werden. Bei Datenbank-gestützten Systemen erfolgt dies üblicherweise durch Angabe eines oder mehrerer eindeutiger und nicht-leerer Feldinhalte - im allgemeinen Primärschlüssel. Bei einem ändernden Zugriff sollten die Daten vor und nach der Änderung protokolliert werden. Bei Datenbank-gestützten Systemen geschieht dies üblicherweise durch Benennung der geänderten Datenbankfelder und die Angabe der Feldinhalte vor und nach der Änderung.

Bei einem Zugriff, bei dem Daten nur gelesen wurden, müssen die Daten benannt werden, in die Einsicht genommen wurde. Die Darstellung erfolgt bei Datenbank-gestützten Systemen üblicherweise durch Angabe des Primärschlüssels und den Bezeichnern der übermittelten Datenfelder.

Der Zweck der Tätigkeit führt viele einzelne Operationen zu einem Vorgang zusammen. So kann beispielsweise das Anlegen eines neuen Benutzers eine Vielzahl von schreibenden und lesenden Zugriffen auf einem System auslösen. Diese einzelnen Operationen müssen dann aggregiert zu Aktionen oder Tätigkeiten zusammengeführt werden können.

5.2 Format

Die Protokolldaten müssen in einem durch gängige Analysewerkzeuge auswertbaren Format vorliegen.

Die Erfahrung hat gezeigt, dass Protokolldaten, die im CSV-Format vorliegen, zusammen mit den frei verfügbaren Tools awk oder grep die operativen Anforderungen an eine maschinell unterstützte Kontrollierbarkeit von Protokolldaten erfüllen. Das CSV-Format fasst üblicherweise einen Protokolleintrag in einer Zeile zusammen. Die Zeile wird in die abgrenzbaren Teilbereiche - beispielsweise Datum, Benutzerkennung, Tätigkeit - durch ein Trennzeichen aufgeteilt. Üblicherweise wird als Trennzeichen das Komma oder Semikolon verwendet. Sollten die Trennzeichen auch innerhalb eines abgrenzbaren Teilbereichs vorkommen, so sollten diese Teilbereiche durch Hochkomma eingeschlossen werden.

6 Technische und organisatorische Aspekte

Bei der Einführung von IuK-Technologie muss der gesamte Lebenszyklus eines Verfahrens betrachtet werden. Dieselbe Anforderung muss deshalb auch an die in diesem Verfahren anfallenden Protokolldaten gestellt werden.

6.1 Erzeugen

Für jedes Verfahren muss in einem Konzept festgelegt werden, welche Tätigkeiten im jeweiligen Verfahren zur Verarbeitung personenbezogener Daten nachzuweisen sind.

Die Notwendigkeit ergibt sich aus

- gesetzlichen Anforderungen,
- Anforderungen aus dem organisationsinternen Datenschutzmanagement und
- Anforderungen aus verbundenen oder übergeordneten Organisationen.

Üblicherweise ergibt sich aus den gesetzlichen Rahmenbedingungen bei vollständig automatisierten Verfahren der Zwang zur Protokollierung ändernder Zugriffe auf personenbezogene Daten.

Eine Protokollierung lesender Zugriffe ist ebenso aus Gründen der datenschutzrechtlichen Revisionssicherheit grundsätzlich erforderlich, insbesondere wenn ein Verfahrensschritt für den Nutzer direkt auf die Ermittlung personenbezogener Daten abzielt. Bei einem hinreichend fein differenzierten Zugriffsschutz kann der Umfang der Protokollierung reduziert werden.

Aufgrund einer Bestandsaufnahme der geltenden Anforderungen muss das Verfahren daraufhin betrachtet werden, welche Tätigkeiten durch Protokolle dokumentiert werden müssen. Für jede Tätigkeit muss der Inhalt der Protokolldaten festgelegt werden. Diese Festlegungen sollten in die Dokumentation des Verfahrens aufgenommen werden.

Die Protokolldaten müssen vollumfängliche Auskunft geben. Jede als relevant eingestufte Tätigkeit muss deshalb zu einem Protokolleintrag führen.

IuK-Systeme, die einen direkten Zugriff auf personenbezogene Daten haben, müssen eine Protokollierung durchführen. Üblicherweise wird der Zugriff auf personenbezogene Daten

über ein oder mehrere zentrale Systeme gesteuert. In diesem Fall kann die Protokollierung auf diese Systeme beschränkt werden.

Änderungen an der Konfiguration der Protokollierung müssen einen Eintrag im Protokoll erzeugen.

6.2 Übertragen

Werden Protokolldaten mit Personenbezug und/oder erhöhtem Schutzbedarf über Netze übertragen (z. B. bei zentraler Protokollspeicherung oder entfernter Auswertung), sind zur Wahrung der Vertraulichkeit, Integrität und Authentizität geeignete und für den Schutzbedarf angemessene kryptografische Verfahren nach dem Stand der Technik zu nutzen.

Voraussetzung für eine revisionssichere und datenschutzgerechte Protokollierung ist die vollständige Übertragung der Protokolldaten. Deshalb ist das verbindungsorientiert Transportprotokoll (TCP) dem verbindungslosen Transportprotokoll (UDP) vorzuziehen.

6.3 Speichern

Die Art und der Umfang der Speicherung der Protokolldaten muss festgelegt werden. Wenn eine Tätigkeit protokolliert wird, dann bedeutet dies aber auch, dass genau in diesem Moment der Erzeugung des Protokolldatums auch eine Kontrolle dieser Daten bzw. der Tätigkeiten geschehen kann. Es muss aus Gründen der Datensparsamkeit geprüft werden, ob ein derartiges, sofortiges Überprüfen von Tätigkeiten ohne Speicherung der Daten hinreicht und keine weitere, später erfolgende Kontrollmöglichkeit vorgesehen werden muss.

Die Zugriffsmöglichkeiten auf Protokolldaten sind zu minimieren, insbesondere für die Systemadministratoren, deren Tätigkeiten anhand dieser Protokolldaten kontrollierbar sein müssen. Um dieser speziellen Anforderung, sowie generell den Anforderungen an Datensicherheit und Datenschutz, gerecht werden zu können, sollten Protokolldaten nicht auf den Produktionsmaschinen sondern auf eigens vorgehaltenen Protokollservern gespeichert werden. Der Zugriff auf diese dedizierten Protokollserver ist entsprechend zu regeln. Ebenso müssen die üblichen Mechanismen zur Datensicherung, wie das Prüfen des Wiederherstellens von Backups, des Lesen- und Verarbeitenkönnens (Hardware, Formate, Zertifikatehandling) auf den Protokollservern umgesetzt sein.

Die Sammlung von Protokolldaten zu einem festgelegten Zweck ist klar zu bezeichnen.

Hat das Sicherheitskonzept (Risikoanalyse) ergeben, dass von einem erhöhten Schutzbedarf der Protokolldaten auszugehen ist, sollten diese mit kryptografischen Verfahren auf dem Protokollserver ausreichend gesichert werden.

6.4 Auswerten

Als Grundlage für eine datenschutzkonforme Auswertung muss die Art und der Umfang der Auswertung unter Beachtung der engen Zweckbindung der Protokolldaten vorab festgelegt werden („Protokollierungskonzept“). Dieses Konzept ist Teil der zu erstellenden Risikoanalyse bzw. des Sicherheitskonzepts, die im Zuge der Vorabkontrolle zu fertigen sind.

Da Protokolldaten geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sollten Mitbestimmungsrechte der Personalvertretungen berücksichtigt werden

(vgl. § 87 Abs. 1 Nr. 6 BetrVG oder § 70 Abs. 2 PersVG M-V). Die Art der Auswertung der Protokolldaten und die an der Auswertung Beteiligten sollten daher in einer Dienstvereinbarung geregelt werden.

Die Auswertung personenbezogener Protokolldaten muss also immer im Vier-Augen-Prinzip, unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung der organisationseigenen Datenschutz- und IT-Sicherheitsbeauftragten, erfolgen.

Bereits bei der Planung der Protokollinhalte sind typische Szenarien zur Auswertung betrachtet worden. Für diese Szenarien müssen geeignete Mechanismen zur Auswertung vorgehalten werden. Für die häufigsten Auswertungen sollte bereits im Verfahren selbst eine Möglichkeit zur Auswertung geschaffen werden.

Für speziellere Auswertungen muss dann unter Nutzung einheitlicher Protokollformate (vgl. Abschnitt „Inhalte“) eine auf den jeweiligen Zweck zugeschnittene Auswertung durchgeführt werden.

Für die Auswertung von Protokolldaten müssen vorab typische Szenarien geplant werden, in denen Protokolldaten entweder anlassbezogen oder regelmäßig ausgewertet werden. Die Szenarien sollten die zu erwartenden Auskunftsersuchen interner und externer Stellen berücksichtigen.

Werden Protokolldaten einer organisationsexternen Instanz zur Auswertung übergeben, so ist, durch geeignete technische und organisatorische Maßnahmen, eine Weitergabe-, Verwendungs- und Löschkontrolle für diese Daten zu etablieren.

Die Vorgehensweise zur Auswertung der Protokolldaten ist zu dokumentieren und die Durchführung ihrerseits zu protokollieren.

6.5 Löschen

Für jedes Protokolldatum ist bereits vor dem Erzeugen die **Aufbewahrungsdauer** festzulegen. Für die Aufbewahrung der Protokolle gelten die allgemeinen Löschungsregeln der Datenschutzgesetze. Ein Maßstab ist mithin die „Erforderlichkeit der Aufgabenerfüllung”. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Pflicht zur Löschung.

Somit wird die Länge der Aufbewahrungsdauer maßgeblich durch den geplanten Auswertungszyklus bestimmt. Je nach Verfahrensart können Fristen von nur wenigen Tagen bis hin zu mehreren Monaten zweckmäßig und akzeptabel sein.

Wird diese Dauer überschritten, muss das Datum gelöscht werden.

Mit Blick auf einige Landesdatenschutzgesetze, in denen die Speicherdauer für Protokolldaten selbst bei der Verarbeitung ausschließlich automatisiert gespeicherte Daten auf ein Jahr begrenzt wird (z. B. § 6 Abs. 4 LDSG S-H oder § 22 Abs. 4 DSG M-V), sollte die Speicherdauer grundsätzlich auf höchstens ein Jahr begrenzt werden, soweit nicht spezialgesetzliche Regelungen oder verfahrensspezifische Bedingungen andere Löschfristen zwingend erfordern.

Der Umgang mit Protokolldaten, insbesondere aber das Verfahren zum Löschen der Protokolldaten muss beschrieben sein. Es müssen dabei auch die Protokolldaten in die Löschung einbezogen werden, die auf Datensicherungsmedien oder bei einem Auftragsdatenverarbeiter gespeichert sind.

Bei der Protokollierung von Löschvorgängen für Protokolldaten dürfen keine personenbezogenen Daten in den Inhalten des Lösch-Protokolls enthalten sein. Stattdessen sind gegebenenfalls Hinweise auf Aktenzeichen oder Dateinamen aufzunehmen. Ferner müssen Angaben darüber, welche Person oder welche Systemkomponente die Löschung dieser Protokolldaten zu welchem Zeitpunkt vorgenommen hat, enthalten sein (Beispiel: „Gelöscht Protokolldaten_Fachverfahren_AA200_bis_ZZ620_von 200106_bis_200606, Admin_A, 20090302_1510_35“).

Soweit ein Protokoll der Verfahrensdokumentation dient, kann die erforderliche Speicherdauer identisch sein zur Dauer der Dokumentationspflicht und mehrere Jahre betragen. Dies gilt beispielsweise für die Dokumentation, wer wann welche Zugriffsrechte besaß und umfasst das Anlegen und Löschen von Benutzerkennungen und die Vergabe von Zugriffsrechten. Ein anderes Beispiel, bei dem eine langjährige Speicherung erforderlich sein kann, betrifft lesende Zugriffe die eine Datenübermittlung darstellen; dies wäre der Fall, wenn die Daten verarbeitenden Stelle einer anderen Daten verarbeitenden Stelle ein Leserecht einräumt, ohne dass eine Auftragsdatenverarbeitung vorliegt. In diesen und anderen Fällen könnten aus den Protokollen Berichte erstellt werden, um das Verfahren zu dokumentieren. Auf die Speicherung der Protokolle kann anschließend verzichtet werden, falls die Berichte gegen nachträgliche Änderungen geschützt sind und festgestellt werden kann, ob sie vollständig sind.

7 Weiterführende Literatur

- DuD - Datenschutz und Datensicherheit, 31. Jahrgang, Heft 10, Oktober 2007, Protokollierungs-Spezial
- DuD - Datenschutz und Datensicherheit, 30. Jahrgang, Heft 5, Mai 2006, Protokollierungs-Spezial
- „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“ https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/studien/logdaten/index_htm.html