



Datenschutzgerechte Protokollierung

Orientierungshilfe
und
Fragenkatalog

Rel. 1.0.1
20.08.2010



Der Landesbeauftragte für den Datenschutz Niedersachsen

Problemstellung

Auch für die Informations- und Kommunikationstechnik gilt die alte Lebensweisheit „**Vertrauen ist gut, Kontrolle ist besser**“. Um eine nachträgliche Kontrolle zu ermöglichen, ist es erforderlich Nutzer- und Systemaktivitäten aufzuzeichnen. Enthält eine solche Aufzeichnung mindestens den Zeitpunkt, die ausgeführte Handlung und den Handelnden spricht man allgemein von Protokollierung.

Einerseits dient ...

die Protokollierung von Verarbeitungsaktivitäten dazu, die Informations- und Kommunikationstechnik nachprüfbarer, sicherer und transparenter zu gestalten. Um sowohl die Nachvollziehbarkeit gewünschter und geplanter Prozesse, als auch die Prävention und Ahndung missbräuchlicher Verwendungen gewährleisten zu können, stellen Protokolle ein probates Mittel dar und kommen auf den verschiedensten Ebenen der Hard- und Softwarenutzung zum Einsatz.

Andererseits entstehen ...

durch Protokollierungen aber auch neue Sammlungen personenbezogener Daten über die Nutzer der Verarbeitungssysteme. Datenfriedhöfe mit unzureichenden Zugriffsberechtigungen laden häufig zu zweckfremder und damit unzulässiger Nutzung ein. Hiervon kann jeder persönlich betroffen sein! ... Ob als Bürger, der eine EDV-gestützte Verwaltungsleistung in Anspruch nimmt oder als Mitarbeiter, der als Anwender eines Verfahrens seine Spuren hinterlässt.

Diese beiden Aspekte bilden das Spannungsfeld, in dem sich jede Protokollierung bewegt, soweit dabei personenbezogene Daten aufgezeichnet werden. Dieses Dokument soll dem Leser bei der Realisierung eines datenschutzkonformen Einsatzes von Protokollierung praxisorientierte Hilfestellung geben.

Erscheinungsformen von „Protokollen“

Grundsätzlich können Protokolldaten verschiedenen Aufgaben dienen:

- (1) sie stellen einen funktionalen Inhalt der betreffenden Anwendung dar
(z.B. Aufzeichnung der anweisenden Personen im Rahmen eines Haushaltswirtschaftssystems)
Hierbei sind sie elementarer Bestandteil des Verfahrens und unterliegen dessen datenschutzrechtlicher Gesamtwürdigung.
- (2) sie sind für die Erfüllung der originären Fachanwendung nicht erforderlich
(z.B. Erfassung lesender Zugriffe auf den Datenbestand eines Verfahrens oder Aufzeichnung von Systemzuständen zur Fehleranalyse)
Ihre Auswertung ist nur im Rahmen ihrer konkreten Zweckbestimmung zulässig; soweit es sich um Protokolldaten handelt, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, unterliegen sie nach § 31 BDSG bzw. § 10 Abs. 4 NDSG einem besonderen gesetzlichen Schutz.

Für eine Reihe von automatisierten Verfahren der öffentlichen Verwaltung (z.B. im Meldewesen) gelten darüber hinaus **spezifische Protokollierungsvorschriften**, die vorrangig heranzuziehen sind.

Grundsätze datenschutzgerechter Protokollierung

Die im Folgenden aufgeführten Grundsätze sollen als Richtschnur für eine datenschutzgerechte Protokollierung dienen; sie sind durch geeignete technische oder organisatorische Sicherungsmaßnahmen zu realisieren.

- ***Zweckbindung***

Keine Protokollierung ohne vorherige ausreichende Definition einer Zweckbestimmung

Protokolle dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Bereits das allgemeine Datenschutzrecht verpflichtet hier zu einer strikten Zweckbindung!

Insbesondere ist es nicht zulässig, Daten, die zur Datenschutzkontrolle, Datensicherung oder Sicherstellung des ordnungsgemäßen Betriebs gespeichert wurden, für andere Zwecke zu verarbeiten (§ 31 BDSG, § 10 Abs. 4 NDSG).

- ***Erforderlichkeit***

Protokollierung nur in dem für die Aufgabenerledigung erforderlichen Umfang

Für Art und Umfang der Protokollierung gilt der Grundsatz der Erforderlichkeit. Es dürfen nur die Daten erhoben werden, die im Rahmen der Zweckbestimmung für die Aufgabenerledigung unerlässlich sind. Eine nicht näher bestimmte Protokollierung auf Vorrat ist unzulässig.

Soweit technisch möglich und für den jeweiligen Zweck ausreichend sollte bei der Protokollierung auf personenbezogene Daten verzichtet werden; technische Möglichkeiten hierzu bieten die Anonymisierung oder Pseudonymisierung der Daten (Prinzip der Datenvermeidung/Datensparsamkeit).

- ***Verhältnismäßigkeit / Angemessenheit***

Nicht mit Kanonen auf Spatzen schießen

Je sensibler die Daten der zu protokollierenden Anwendung und je höher die Eintrittswahrscheinlichkeit einer abzuwendenden Gefährdung sind, desto größere Ansprüche sollten aus datenschutzrechtlicher und systemtechnischer Sicht an eine ausreichende Kontrolle gestellt werden. Bei der Erzeugung von Protokollen nach § 10 Abs. 4 NDSG ist stets abzuwägen, ob die Sensitivität der entstehenden Protokolldaten in einem angemessenen Verhältnis zum Schutzbedarf der überwachten Verfahren steht.

Während bei der Verarbeitung frei zugänglicher personenbezogener Daten auf eine Protokollierung weitgehend verzichtet werden kann, sollten Veränderungen schutzbedürftiger personenbezogener Daten grundsätzlich aufgezeichnet werden. Bei einem besonders hohen Schutzbedarf kann auch die Aufzeichnung lesender Zugriffe erforderlich sein.

- ***Umfang***

Der Kontrollzweck bestimmt den Protokollumfang

Der Inhalt der Protokollierung sollte so gewählt sein, dass Verfahrensfehler oder unbefugte Handlungen möglichst frühzeitig erkannt oder zumindest nachträglich verifiziert werden können. Je nach Erforderlichkeit können hierfür neben reinen Systemzuständen auch Änderungen der Zugriffsrechte, der Zugang zum Betriebssystem (Login) oder Administratoraktivitäten festgehalten werden.

Unzureichend sind Protokolle, die lediglich das Starten und Beenden der Anwendung aufzeichnen. Bei Massenprotokollierungen kann auch die Aufzeichnung einer Stichprobe bzw. eine stichprobenartige Auswertung in Frage kommen.

- **Auswertung**

Protokolle müssen auswertbar sein und ausgewertet werden

Protokollierung ist kein Selbstzweck, sondern nur sinnvoll und datenschutzrechtlich vertretbar, wenn die Protokolldaten auch tatsächlich ausgewertet werden. Protokolldaten, die im Rahmen ihrer Zweckbestimmung anfallen, sind in einem vorher festzulegenden Zyklus zumindest stichprobenartig auszuwerten. Ungenutzte „Datenhalden“, deren Entstehungsgründe womöglich in Vergessenheit geraten, sind zu vermeiden.

Je nach Protokolldatenanfall ist es im Rahmen einer sinnvollen und zielgerichteten Auswertung unabdingbar, zeit-, ereignis- oder benutzerorientiert zugreifen zu können. Niemandem kann über längere Zeit das „Lesen“ umfangreicher Dateien im Textformat (o. ä.) zugemutet werden; der Einsatz von automatisierten Recherchehilfen ist anzustreben.

- **Vertraulichkeit**

Protokolldaten sind gegen unberechtigte Nutzung zu schützen

Nur wenige vorher bestimmte Berechtigte dürfen auf Protokolldateien zugreifen. Für die regelmäßige Prüfung von Daten die zum Zwecke der Datenschutzkontrolle und der Datensicherung erhoben wurden, sollten Datenschutzbeauftragte und Revisoren verpflichtet werden. Protokolle zur Sicherung des ordnungsgemäßen Betriebs sind zweckmäßigerweise zeitnah durch die Systemadministration durchzusehen. Die Wahl eines gesicherten Speicherortes und die restriktive Vergabe der Zugriffsberechtigungen sind an diesem Ziel auszurichten.

Je nach Sensitivität der Daten kann es geboten sein, die Kontrollen nach dem 4-Augen-Prinzip durchzuführen.

- **Integrität**

Protokolldaten dürfen nachträglich nicht verändert werden

Nur manipulationssichere Protokollierungen können ihren Schutzzweck in vollem Umfang erfüllen. Insbesondere bei sensiblen Anwendungen ist die Unveränderbarkeit von Protokolldaten durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten. Dabei richtet sich der zu treibende Aufwand im wesentlichen nach dem Schutzbedarf der verarbeiteten Daten.

Technische Maßnahmen sind organisatorischen vorzuziehen.

- **Aufbewahrungsdauer / Löschfristen**

Protokolldaten sind nach ihrer Zweckerfüllung zeitnah zu löschen

Für die Aufbewahrung der Protokolle gelten die allgemeinen Lösungsregeln 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 (z.B. § 35 Abs. 2 BDSG, § 17 Abs. 2 NDSG).

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. Die Aufbewahrung von Protokolldaten für mehr als ein halbes Jahr wird sich in der Regel schwer begründen lassen.

- **Transparenz**

Existenz und Verwendungszweck von Protokolldaten dürfen kein Geheimnis sein

Sowohl das Transparenzgebot als auch der Präventionsgedanke bringen gewisse Informationspflichten mit sich. So sollte jeder Beteiligte Kenntnis von der Art, dem Umfang, der Zweckbindung und den Auswertungsmodalitäten einer Protokollierung haben und sich möglicher Konsequenzen bei festgestellten Verstößen gegen Datenschutz und Datensicherheit bewusst sein.

- **Beteiligungen**

Betriebs- und Personalräte sowie Datenschutzbeauftragte sind rechtzeitig einzubinden

Wie bei allen Verarbeitungen personenbezogener Daten ist der betriebliche oder behördliche Datenschutzbeauftragte (bDSB) bereits in der Planungsphase rechtzeitig zu beteiligen.

Soweit Protokolldateien Beschäftigtendaten enthalten, ist der Betriebs- bzw. Personalrat zu informieren, um ihm die Wahrnehmung seiner Beteiligungsrechte zu ermöglichen (§ 87 Abs. 1 Nr. 6 BetrVG, § 67 Abs. 1 Nr. 2 NPersVG).

Hinweise für die Praxis

Die Praxis zeigt, dass es bei der Übertragung der vorstehenden Grundsätze in die alltägliche Arbeit eine Vielzahl von Schwierigkeiten zu überwinden gilt. Wichtig ist, diese nun nicht zu ignorieren, sondern offen zu diskutieren, die Risiken eines Zuviel oder Zuwenig abzuwägen und zu dokumentieren. Letzteres ist unerlässlich um die Entscheidungsfindung transparent und überprüfbar zu gestalten und bei sich ändernden technischen Rahmenbedingungen ohne allzu viel Aufwand nachjustieren zu können.

Durch eine formale Regelung sollte gewährleistet sein, dass hinsichtlich der Protokollierung für jedes Verfahren Festlegungen getroffen werden, die für alle Betroffenen dokumentiert und nachvollziehbar zur Verfügung stehen. Die wesentlichsten Regelungsbereiche sind hierbei jeweils:

- Zweckbestimmung
- Inhalt und Umfang
- Auswertung (wann und durch wen)
- Aufbewahrungsdauer
- Zugriffsberechtigung
- Zuständigkeit für die Überprüfung dieser Regelungen

Um Datenschutzbeauftragten, die vor dieser Aufgabe stehen die ersten Schritte zu erleichtern, haben wir einen **Fragenkatalog** zusammengestellt. Er ist in wenige Bereiche gegliedert, in denen an Hand konkreter Fragestellungen die benötigten Informationen beschafft, bewertet und die erforderlichen und realisierbaren Maßnahmen abgewogen werden können. Dieser Katalog kann naturgemäß nicht alle denkbaren Fälle berücksichtigen; er weist aber einen systematischen und gangbaren Weg, sich im Rahmen der gegebenen Möglichkeiten einer rechtlich haltbaren und praktikablen Lösung anzunähern. Dabei stellt er kein starres Korsett dar, sondern ist stets an die konkrete Situation anzupassen.

Fragenkatalog

Bestandsaufnahme der Verfahren	
Welche Verfahren befinden sich im Einsatz?	
Zu welchen Verfahren erfolgen Protokollierungen?	
Erfolgt die Protokollierung durch das Verfahren selbst oder wird (auch) auf der Systemebene protokolliert?	
Enthalten die Protokolle personenbezogene Daten?	
Hinweis: Ein aktuelles Verzeichnissesverzeichnis kann als mögliche Quelle für eine Bestandsaufnahme dienen. Hieraus können sich auch Hinweise auf bestehende Protokollierungen ergeben. zu beachten: Evtl. existieren Verfahren, die selbst keine personenbezogenen Daten verarbeiten, in deren Protokolldaten aber personenbezogene Daten enthalten sind.	

Feststellung des Schutzbedarfs der innerhalb von (Fach-) Verfahren verarbeiteten personenbezogenen Daten	
Welcher Schutzstufe sind die Daten zuzuordnen, deren Verarbeitung protokolliert werden soll? Hier wird das maximal mögliche Schadensausmaß ermittelt; als Hilfe kann das Schutzstufenkonzept unter www.lfd.niedersachsen.de / Service-Angebote / Technische Hilfen / Schutzstufen dienen.	
Welche Risikofaktoren sind zu beachten? konkret: Welche Gefährdungen können auftreten und wie wahrscheinlich ist dies?	
Welcher Schutzbedarf ergibt sich? Als Schutzbedarf ist hier das Produkt aus Schadensausmaß und Eintrittswahrscheinlichkeit zu verstehen.	
Hinweis: Da der Schutzbedarf der Daten wichtigste Grundlage für die Bestimmung eines angemessenen Aufwandes für die Verhältnismäßigkeit des Protokollumfangs ist, muss dieser immer zuerst ermittelt werden. Zuständig für diese Festlegung ist grundsätzlich der fachlich verantwortliche Nutzer der Daten; bei Bedarf sollte der bDSB beratend unterstützen. Hinweise können sich aus der Vorabkontrolle des Verfahrens oder den Grundsatzkatalogen des BSI ergeben.	

Bestimmung der Anforderungen an die Protokollierung und Ableitung der Zweckbestimmung

Welche Anforderungen ergeben sich aus fachlicher Sicht?	
z.B. rechtliche oder sonstige Anforderungen aus fachlicher Sicht ... aus systemtechnischer Sicht?	
z.B. Sammlung von Informationen zur Fehleranalyse etc. ... aus Sicht des Datenschutzes?	
gestaffelt nach Schutzbedarf der Daten und Umfang und Detaillierung der Protokolle; Wahrung der Verhältnismäßigkeit ... aus Sicht des Betriebs- bzw. Personalrats	
z.B. Sicherstellung von Beteiligungsrechten	
Sollen die gleichen Protokolldaten verschiedenen Zweckbestimmungen dienen?	
Wer übernimmt die vorgesehene Auswertung?	
Ist sichergestellt, dass die Protokolle im Sinne der Zweckbestimmung in angemessener Zeit ausgewertet werden können?	
Hinweis: Die sich aus verschiedenen Ansprüchen ergebenden Anforderungen sind aufzunehmen und bzgl. ihrer Zweckbestimmungen zu präzisieren.	

Ermittlung der Konfigurationsmöglichkeiten der Protokollierung

Lässt sich die Protokollierung getrennt von anderen Funktionalitäten des Verfahrens aktivieren bzw. deaktivieren?	
Ist der Umfang der Protokollierung konfigurierbar?	
Lässt sich der Speicherort der Protokolldateien beeinflussen?	
Welche Standardeinstellungen sind nach einer Installation aktiv?	
Enthalten die Protokolle Daten verschiedener Zweckbestimmungen?	
Es soll sichergestellt werden, dass die Daten für jede Zweckbestimmung getrennt verfügbar gemacht werden können.	

Wie wird die Manipulationssicherheit gewährleistet? Optimal wären geeignete technische Vorkehrungen (direktes Schreiben auf CD/DVD-ROM; Speicherung auf besonders gesicherten, zentralen Log-Servern, o. ä.); alternativ sind organisatorische Regelungen zu treffen und die Zugriffsrechte rigide zu handhaben.	
Hinweis: Sicherlich wird immer die fachliche Funktionalität bei der Auswahl eines Verfahrens im Vordergrund stehen. Bestehende Unzulänglichkeiten bei der Konfigurierbarkeit der Protokollierung sollten allerdings nach Ausschöpfen aller vertretbaren technischen Möglichkeiten durch zusätzliche organisatorische Regelungen (Erlass, Kontrolle und Durchsetzung geeigneter Dienstanweisungen etc.) weitestgehend ausgeglichen werden.	

Besonderheiten für Protokolle auf System- und Netzebene	
Welche Protokolle werden auf System- und Netzebene geführt?	
Ist die Personenbeziehbarkeit der Protokolldaten hinreichend geklärt? Wurde die mögliche Verwendung von Zusatzinformationen aus dem Bereich der Administration einbezogen?	
Dienen diese Protokolle tatsächlich ausschließlich Zwecken nach §10 Abs. 4 NDSG / § 31 BDSG?	
Ist eine Nutzung zu Zwecken der Verhaltens- und Leistungskontrolle tatsächlich wirksam ausgeschlossen ?	
Wie lange werden die Protokolldaten aufbewahrt?	
Hinweise: Neben den Protokollen in abgegrenzten (Fach-)Verfahren werden häufig Zustands- und Nutzungsdaten auf System- oder Netzebene erfasst; dabei ist verstärkt die Frage nach deren Zweckbestimmung zu stellen. Häufig werden diese Daten einfach erst mal erhoben, ohne vorher eine konkrete Nutzung festzulegen. Zum Einen, weil die Systeme diese Einträge eben standardmäßig erfassen, zum anderen weil man ja nicht wissen kann, ob man die Angaben zur Fehlerbehebung oder für den Nachweis eines Fehler verursachenden oder sonst wie unerwünschten Nutzerverhaltens noch mal gebrauchen könnte. Auch eine solche Protokollierung ist generell nur dann zulässig, wenn im Vorfeld klar definiert wird, welchen Zwecken die erhobenen Daten dienen sollen; häufig wird in diesem Umfeld die „Sicherstellung eines ordnungsgemäßen Betriebs“ eine wesentliche Rolle spielen. Diese Zweckbestimmung hat dann allerdings zur Folge, dass die entsprechenden Protokolldaten den besonderen Bestimmungen des §10 Abs. 4 des NDSG bzw. § 31 BDSG unterliegen. Weiterhin sollte für diese Daten eine wirksame und akzeptierte Zugriffs- und Auswertungsbeschränkung realisiert werden. Sinnvoll wäre es, entsprechende Regelungen in einer Dienstanweisung für die Systemverwaltung zu hinterlegen; sie schützen nicht zuletzt den/die Administratoren vor unzulässigen Auswertungersuchen. Die Aufbewahrungsfristen sollten i.d.R. 14 Tage nicht übersteigen, da ältere Daten meist keinen Wert mehr für die Betriebssicherheit haben. Aus diesem Grund ist anzustreben, die Daten von regelmäßigen Datensicherungen mit längeren Aufbewahrungsfristen auszunehmen. Werden bestimmte Systemvorgänge aus Gründen der Systemsicherheit oder der Datenschutzkontrolle protokolliert, sind diese Daten möglichst getrennt zu erfassen und aufzubewahren; hier kann eine längere Aufbewahrungsfrist gerechtfertigt sein. Allerdings reicht auch hier die Feststellung „man komme aus zeitlichen Gründen eben nicht eher zu einer Auswertung“ ganz sicher nicht aus. Sinnvoll ist es, die Zweckbestimmung, die vorgesehene Aufbewahrungsfrist und die Begründung für längere Fristen nachvollziehbar zu dokumentieren.	

weitere, lokal bedeutsame Fragen	
Fragestellungen mit Erläuterung	
Hinweise zur Auswertung und Umsetzung der Ergebnisse	

Zum guten Schluss

Die mit Hilfe des Fragenkatalogs gesammelten Informationen geben zum Einen ein gutes Bild der aktuellen Situation und weisen zum Anderen mögliche Wege, erkannte Defizite auszugleichen. Als notwendig erachtete Maßnahmen werden sich allerdings nicht immer bestmöglich und zeitnah realisieren lassen.

Neben allen sich ergebenden internen technischen, organisatorischen, personellen oder finanziellen Schwierigkeiten, sollte der Bedarf an optimierten Protokollierungsfunktionalitäten verstärkt an die Hersteller der jeweiligen Verfahrenssoftware herangetragen werden.

Zumindest langfristig könnte die wiederholte Artikulation derartiger Kundenwünsche am besten geeignet sein, an dieser Stelle eine positive Veränderung herbeizuführen.