



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Version 1.0

Technische Empfehlungen für die Protokollierung gemäss Art. 4 DSV des EDÖB

vom 15. September 2023

Inhaltsverzeichnis

1.	Einleitung und Ziel des Dokuments.....	3
1.1.	Art. 4 DSV	3
1.2.	Art. 3 Abs. 3 DSV	3
1.3.	Zweck der Protokollierung	4
2.	Protokollierung.....	4
2.1.	Die drei Grundpfeiler der Protokollierung.....	4
2.1.1.	Erfassung.....	4
2.1.2.	Speicherung.....	5
2.1.3.	Analyse	5
2.2.	Konzept.....	5
3.	Technische Empfehlungen	6
3.1.	Allgemeine technische Empfehlungen zur Protokollierung	6
3.2.	Speicherung und Speichervolumen.....	7
3.3.	Protokollierung bei bestehenden Anwendungen.....	8
4.	Konkrete Fragen zur Umsetzung / FAQ	10

1. Einleitung und Ziel des Dokuments

Mit dem Inkrafttreten von Art.4 DSV¹ per 01.09.2023 muss der private Verantwortliche und sein privater Auftragsbearbeiter bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren.

Die vorliegenden Empfehlungen sollen eine Übersicht geben, was zu dieser Protokollierung gehört und was zur technischen Erfüllung des Art.4 DSV gemacht werden muss. Wie die konkrete Umsetzung erfolgt, muss von den verschiedenen Systemeignern danach definiert werden und ist nicht Teil dieser Empfehlungen. Neben dem DSG können auch weitere Vorgaben, wie z.B. zur Informationssicherheit, relevant sein. Ziel ist eine möglichst effiziente und effektive Protokollierung zu erreichen, indem Doppelspurigkeit vermieden wird.

1.1. Art. 4 DSV

Der Wortlaut des besagten Art. 4 DSV Protokollierung ist der folgende:

¹ Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.

² Das verantwortliche Bundesorgan und sein Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.

³ Bei Personendaten, welche allgemein öffentlich zugänglich sind, sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

⁴ Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

⁵ Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

1.2. Art. 3 Abs. 3 DSV

Die Protokollierung dient der Nachvollziehbarkeit der Bearbeitung und insb. des Zugriffs von Personendaten. Dies ist in Art.3 Abs. 3 DSV verankert und dieser Absatz beschreibt, was die Protokollierung leisten muss:

³ Um die Nachvollziehbarkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);
- b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur

¹ [Verordnung vom 31. August 2022 über den Datenschutz \(Datenschutzverordnung, DSV, SR 235.11\) \(admin.ch\)](#)

- Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);
- c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

Die Nachvollziehbarkeit beinhaltet auch das Lesen der Daten, was mit dem Aufzeichnen der Zugriffe für die Erkennung einer Verletzung der Zugriffskontrolle gemäss Abs. 3 Lit. c erfolgt.

1.3. Zweck der Protokollierung

Der Zweck der Protokollierung besteht darin, dass Bearbeitungen von Personendaten nachträglich überprüfbar sind, so dass im Nachhinein festgestellt werden kann, ob ein Datenzugriff erfolgt ist oder die Daten gelöscht, vernichtet oder verändert wurden. Ausserdem geht es auch um die Gewährleistung der Zweckkonformität und einer angemessenen Datensicherheit. So können sich aus der Protokollierung auch Hinweise ergeben, ob Personendaten nicht zweckkonform bearbeitet wurden. Weiter können die Protokollierungen auch dazu dienen, Verletzungen der Datensicherheit aufzudecken und aufzuklären. Die Protokollierung darf hingegen nicht zum Ziel der Verhaltensüberwachung von Nutzerinnen und Nutzern, die Personendaten bearbeiten, ausgewertet werden.

2. Protokollierung

Die Protokollierung im Datenschutzrecht bezieht sich auf die systematische Aufzeichnung von Informationen über die Bearbeitung von Personendaten. Die Protokollierung dient dazu, Transparenz und Rechenschaftspflicht zu gewährleisten und im Falle von Datenschutzverletzungen oder -vorfällen nachvollziehen zu können, wer wann auf welche Personendaten zugegriffen hat und was geändert wurde.

2.1. Die drei Grundpfeiler der Protokollierung

Die drei Aspekte der Protokollierung umfassen die Erfassung, die Speicherung, sowie die Analyse von Protokolldaten.

Der private Verantwortliche und sein privater Auftragsbearbeiter müssen zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.

Der Vorgang des «Lesens» ist als Zugriff ohne «Verändern» zu verstehen; es reicht demnach aus, wenn die Zugriffe auf Personendaten und das Verändern dieser Daten protokolliert werden. Der Protokollierung des «Lesens» wird damit Genüge getan. Hinzuweisen ist hier auf die Einschränkung gemäss Art. 4 Abs. 3 DSV bei Personendaten, welche allgemein öffentlich zugänglich sind. Hier sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

2.1.1. Erfassung

Es müssen Protokolldaten erfasst werden, um sicherzustellen, dass alle Vorgänge, die Personendaten betreffen, aufgezeichnet werden. Das bedeutet, dass alle Zugriffe (Personen oder Maschinen) auf Personendaten protokolliert werden müssen, einschliesslich die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

2.1.2. Speicherung

Protokolldaten müssen sicher und geschützt gespeichert werden. Die Speicherung von Protokolldaten muss getrennt von Datenbearbeitungssystemen erfolgen, um sicherzustellen, dass sie auch dann verfügbar bleiben, wenn das primäre System beeinträchtigt wird (z.B. durch Ransomware). Der Zugriff darf nur berechtigten Personen, welchen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung bzw. Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, möglich sein.

2.1.3. Analyse

Die Protokolldaten müssen bei Bedarf analysiert werden können, um mögliche Datenschutzverletzungen aufzudecken und um sicherzustellen, dass alle Zugriffe auf Personendaten rechtmässig erfolgen. Dies erfordert leistungsfähige Analysetools, die in der Lage sind, grosse Mengen an Protokolldaten zu verarbeiten und Muster oder Anomalien zu identifizieren, die auf mögliche Verstösse hinweisen. Sie dürfen ausschliesslich denjenigen Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden (Art.4 Abs.5 DSV).

2.2. Konzept

Ein Konzept für die Protokollierung ist zu erstellen und sollte eine umfassende und systematische Beschreibung der Protokollierungspolitik und -verfahren enthalten. Im Wesentlichen sollten folgende Punkte berücksichtigt werden:

- a) Ziele der Protokollierung: Das Konzept sollte klare Ziele definieren, die durch die Protokollierung erreicht werden sollen, z.B. Überwachung der Bearbeitung von Personendaten, Sicherheitsüberwachung, Fehlerbehebung.
- b) Protokollierungsrichtlinien: Das Konzept sollte klare Richtlinien für die Protokollierung festlegen, unter anderem welche Ereignisse protokolliert werden, welche Daten erfasst werden, welche Speicherzeit vorgesehen ist und wer auf die Protokolldaten zugreifen darf.
- c) Protokollierungswerkzeuge: Das Konzept sollte beschreiben, welche Werkzeuge für die Protokollierung verwendet werden, z.B. Protokollgenerierungs-Agenten, Log-Management-Tools, Event-Logging-Frameworks oder Security-Information-and-Event-Management-Systeme (SIEM).
- d) Alarmierungskonzept: Das Konzept sollte beschreiben, welche Ereignisse Alarme generieren können, wie auf Alarme reagiert wird, wer benachrichtigt werden muss und welche Massnahmen bei der Entdeckung von Problemen ergriffen werden müssen.
- e) Verantwortlichkeiten und Rollen: Das Konzept sollte klare Verantwortlichkeiten und Rollen für die Verwaltung der Protokollierung definieren, z.B. wer für die Überwachung der Protokollierung verantwortlich ist, wer die Rechte dazu vergibt und wer die Protokollierungsrichtlinien aktualisiert. Ausserdem muss beschrieben werden wer für die Analyse und Berichterstellung verantwortlich ist.
- f) Schulung: Das Konzept sollte beschreiben, wie sich Mitarbeitende, die mit der Protokollierung befasst sind, das notwendige Wissen und die Fähigkeiten aneignen können, um effektiv und sicher zu arbeiten.
- g) Überprüfung: Das Konzept sollte regelmässige Überprüfungen der Protokollierungspolitik und -verfahren vorsehen, um sicherzustellen, dass sie effektiv und den aktuellen Anforderungen entsprechend sind.

Ein umfassendes Konzept als Grundlage für die Prüfung der Angemessenheit und Verhältnismässigkeit der Protokollierungspolitik sowie der Einhaltung des befugten gesetzlichen Zugangs zu den Daten der Protokollierung ist entscheidend.

3. Technische Empfehlungen

3.1. Allgemeine technische Empfehlungen zur Protokollierung

Es gibt eine Reihe von technischen Empfehlungen im Zusammenhang mit der Protokollierung in der Informationssicherheit oder dem Datenschutz. Nachfolgend sind die wichtigsten Aspekte aufgelistet:

- a) Verwendung von standardisierten Protokollierungsformaten: Die Verwendung von standardisierten Protokollierungsformaten wie Syslog oder Common Event Format (CEF) helfen eine einheitliche Protokollierung von Ereignissen zu gewährleisten.
- b) Einlesen und Interpretation von Protokollen: Protokolle sollen nicht nur abgelegt, sondern auch eingelesen und interpretiert werden (Parsing und Indexing). Dies ist die Grundlage für die Überwachung, Alarmierung und Erkennung von Anomalien. Dabei sollten alle Informationselemente beim Einlesen (Ingestion) mithilfe von Muster-Extraktion extrahiert werden und wo sinnvoll mit Informationen aus bestehenden Protokollen ergänzt werden (Korrelation). Nicht verwendete Informationsfelder sollten in diesem Prozess ausgelassen werden, um u.A. Speicherplatz zu sparen.
- c) Regelmässige Überprüfung der Protokolldaten: Die Protokolldaten sollten regelmässig überprüft werden, um sicherzustellen, dass sie vollständig sind, die Sicherheitsrichtlinien eingehalten werden und um sicherzustellen, dass sie nicht manipuliert wurden.
- d) Mechanismen zur Erkennung von Anomalien: Es sollten Mechanismen zur Erkennung von Anomalien in den Protokolldaten implementiert werden (z.B. Zugriff von ungewöhnlichen Geolokationen aus), um verdächtige Aktivitäten zu erkennen. Dafür ist es auch notwendig erst normales Verhalten zu definieren, um danach Änderungen feststellen zu können.
- e) Einsatz von Sicherheitsvorkehrungen für Protokolldaten: Es ist wichtig, geeignete Zugriffskontrollen für die Protokolldaten zu implementieren, um sicherzustellen, dass sie vor unbefugtem Zugriff geschützt sind.
- f) Zeitstempel: Die Protokolldaten müssen mit Zeitstempel versehen sein, um den genauen Zeitpunkt eines Ereignisses im System zu erfassen. Ein genauer Zeitstempel ist wichtig, um den zeitlichen Zusammenhang zwischen verschiedenen Ereignissen im System zu verstehen.
- g) Zeitsynchronisation: Um genaue Zeitstempel zu gewährleisten, ist es wichtig, dass alle Systeme im Netzwerk über eine zuverlässige und genaue Zeitsynchronisation verfügen. Durch die Synchronisation der Uhren aller Systeme über einen gemeinsamen NTP-Server wird sichergestellt, dass die Protokolldaten genau und konsistent sind.
- h) Data Enrichment: Durch Data Enrichment werden die Protokolldaten mit zusätzlichen Informationen angereichert, um ein besseres Verständnis der Ereignisse zu ermöglichen. Hierbei können z.B. Geo-Informationen, Benutzerkontext oder Systemkonfigurationsdaten ergänzt werden. So können Protokolldaten besser analysiert und potenzielle Sicherheitsbedrohungen schneller erkannt werden. Wichtig

beim Data Enrichment ist, dass nur jene Informationen hinzugefügt werden, die für die konkrete Zielerreichung (der Protokollierung) geeignet und erforderlich sind. Bei einer Verknüpfung mit weiteren Daten oder der Bildung von Profilen mithilfe der Anreicherung, muss der eventuell vorhandene Datenschutzberater einbezogen werden. Wenn ein Auftragsverarbeiter zur Durchführung von Data Enrichment beauftragt wird, muss ausserdem sichergestellt werden, dass zwischen dem Auftraggeber und dem Auftragsverarbeiter ein rechtsgültiger Vertrag besteht, der die Anforderungen gemäss DSGVO erfüllt.

- i) Alarmierung: Die verwendeten Protokoll-Analyseapplikationen sollten die Verantwortlichen bei Auftreten von Anomalien oder bekannter sicherheitsrelevanter Ereignisse sofort informieren können.

Durch die Umsetzung dieser technischen Empfehlungen können die privaten Verantwortlichen eine umfassende Protokollierung erreichen, welche eine effektive Überwachung, Analyse und Reaktion auf sicherheitsrelevante Ereignisse ermöglicht.

3.2. Speicherung und Speichervolumen

Eine Herausforderung bei der Verarbeitung von Protokolldaten ist das benötigte Speichervolumen. Für die Analyse-Werkzeuge sollten die Protokolldaten so lange im direkten Zugriff bleiben, wie sie für das Erkennen und Reagieren auf Datenschutzverletzungen bzw. Sicherheitsvorfälle benötigt werden. Dies kann je nach Art und Grösse der Organisation variieren, aber typischerweise umfasst dies einen Zeitraum von einigen Tagen bis mehrere Wochen. In diesem Zeitraum können die Daten aktiv genutzt werden, um verdächtige Aktivitäten zu erkennen und auf diese zu reagieren.

Nachdem die Protokolldaten nicht mehr direkt für die Analyse, sondern z.B. für die Überprüfung der Anwendung der Datenschutzvorschriften benötigt werden, können sie in ein längerfristiges Speichersystem verschoben werden. Dies erlaubt die Daten auf günstigeren Speicherplatz zu kopieren und zu komprimieren. Dies erlaubt selbstverständlich keine längere Aufbewahrungsdauer, als in der einschlägigen Rechtsgrundlage vorgesehen. Dazu gibt es die folgenden Empfehlungen:

- a) Verwendung von geeigneten Speichermedien: Für die Langzeitspeicherung von Protokolldaten sollten geeignete Speichermedien verwendet werden, die eine lange Lebensdauer und Zuverlässigkeit bieten.
- b) Speicherdauer: Es ist wichtig, eine klare Speicherdauer für Protokolldaten zu definieren, um sicherzustellen, dass diese nicht unnötig lange aufbewahrt werden. Dabei müssen selbstredend die gesetzlichen Vorgaben zur Aufbewahrungsdauer eingehalten werden. Die Speicherdauer für Protokolldaten im Zusammenhang mit der Bearbeitung von Personendaten ist auf mindestens ein Jahr festgelegt.
- c) Speichervolumen berechnen: Um das erforderliche Speichervolumen für Protokolldaten zu berechnen, müssen verschiedene Faktoren berücksichtigt werden, wie z.B. die Menge der erzeugten Protokolldaten, die Anzahl der Systeme im Netzwerk und die Dauer der Speicherung. Es ist wichtig, genügend Speicherkapazität bereitzustellen, um eine Unterbrechung des Protokollierungsprozesses zu vermeiden. Für die Planung der Speichervolumen und die entsprechende Kostenschätzung dazu, kann von der Empfehlung ausgegangen werden, dass die Daten normalerweise 1-2 Wochen im Index verbleiben und danach mindestens ein Jahr im längerfristigen Speichersystem gespeichert werden müssen.

Zusammenfassend lässt sich festhalten, dass die Langzeitspeicherung der Protokolldaten Teil der Datensicherungsstrategie ist, und dass es wichtig ist, dass die Speicherung der Protokolldaten getrennt von Datenbearbeitungssystemen (gem. Art. 4 DSV) erfolgt, um

deren Integrität und Verfügbarkeit zu gewährleisten. Eine zusätzliche Sicherungskopie der Protokolldaten auf einem anderen System ist normalerweise nicht notwendig, solange eine robuste Speicherlösung vorhanden ist und die Daten regelmässig auf Integrität und Vollständigkeit überprüft werden. Es muss aber fallabhängig entschieden werden, ob ein Backup der Protokolldaten notwendig ist.

3.3. Protokollierung bei bestehenden Anwendungen

Bei neuen Anwendungen ist es relativ einfach von Beginn an alle Aktivitäten mit Personendaten zu protokollieren. Bei bestehenden, älteren Applikationen ist es aber nicht immer möglich die Applikation selbst anzupassen. Für diese Fälle gibt es aber verschiedene Lösungsansätze.

Die Umsetzung der Protokollierung hängt von vielen Aspekten wie der Programmiersprache, der Laufzeitumgebung und der benutzten Entwicklungsmethoden der Anwendung ab. Unsere Empfehlungen sind deshalb generischer Natur, können aber bei konkreten Anwendungen die Planung unterstützen.

Schritt 1: Kennen der Protokollierungsanforderungen für die Anwendung

Es muss eruiert werden, wie lange die Protokolle indexiert und im Langzeitspeicher verbleiben sollen. Die (gesetzlich vorgeschriebene) Aufbewahrungsdauer wirkt sich auf die Berechnung der Speicher und Datenvolumen (letzter Schritt 5) aus.

Schritt 2: Kennen der Bearbeitungsvorgänge, die protokolliert werden sollen

Nicht alle Aktivitäten in einer Anwendung stellen eine Bearbeitung von Personendaten dar, die protokolliert werden muss. Eine Auflistung der entsprechenden Aktivitäten hilft, die Anpassungen auf diese zu fokussieren. Beim Protokollieren geht es letztlich darum, die wichtigen Aktivitäten gemäss DSV zu erfassen und nicht möglichst viele.

Bei Anwendungen, in denen Personendaten bearbeitet werden, es im Voraus aber nicht offensichtlich ist, welche Aktivitäten genau stattfinden (z.B. ein Dokumentationssystem), müssen alle Aktivitäten protokolliert werden.

Zur Stärkung der Informationssicherheit der Anwendung kann es wünschenswert sein, zusätzlich auch sicherheitskritische Ereignisse zu protokollieren.

Schritt 3: Kennen der Informationsflüsse, die Bearbeitungsaktivitäten auslösen

Es gibt verschiedene Arten von Anwendungen:

- Bei den meisten findet bei der Bearbeitung von Personendaten eine Kommunikation (d.h. ein Informationsfluss) zwischen der Präsentationsebene (dem Frontend) und der Administrativen Logik (Backend) statt. Diese Informationsflüsse gehen oft durch mehrere Netzwerke und Sicherheitssysteme (als Beispiel in Abbildung 1 dargestellt), die zumindest einen Teil der Aktivitäten sehen und deshalb bei der Protokollierung im Hinblick auf die Informationssicherheit nützlich sein können.

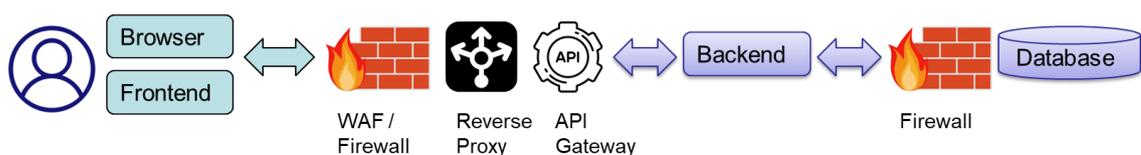


Abbildung 1 - Möglicher Informationsfluss in der Applikation

- Bei Anwendungen, bei der die Bearbeitung nur beim Anwender selbst stattfindet und es zu keiner Kommunikation mit serverseitigen Backends oder Datenbanken kommt, sollte das erstmalige Herunterladen auf das Anwendersystem als «Zugriff»

protokolliert werden. Veränderungen könnten in diesem Fall meist nur durch eine Erweiterung der Applikation selbst erfasst werden, was nur in Ausnahmefällen sinnvoll wäre.

- Ein anderer Anwendungsfall sind Anwendungen, bei denen die Bearbeitung autonom durch einen Prozess im Backend durchgeführt wird (z.B. das automatisierte Verknüpfen von verschiedenen Personendaten zu Profilen, das automatisierte Erweitern von Personendaten wie User-IDs mit den entsprechenden Namen etc). Auch hier wird oft eine Erweiterung der Applikation selbst notwendig sein.

Schritt 4: Entscheiden wo die Protokollierung eingebaut werden kann und soll

Mit dem Wissen, bei welchen Aktivitäten Protokolle generiert werden müssen und wie die Informationsflüsse aussehen, kann evaluiert werden, wie die Protokollierung am einfachsten nachgerüstet werden soll. Das NCSC empfiehlt folgendes Vorgehen:

1. Anwendungen unterstützen oft bereits eine Protokollierung von Aktivitäten, die aber deaktiviert ist und eingeschaltet werden muss. Ob dies der Fall ist sollte also als erstes überprüft werden. Wenn eine bestehende Protokollierungsfunktion alle Aktivitäten abdeckt und genügend Informationen beinhaltet (d.h. die Identität der Person, die die Personendaten erhält oder bearbeitet, sowie die Aktivität der Bearbeitung), ist dies der einfachste Lösungsansatz.
2. Es ist möglich, dass bei den Netzwerksystemen bereits genügend Informationen über die Aktivität sichtbar wird (z.B. die User-ID anhand der IP-Adresse und die Aktivität in Bezug auf das Backend). Wenn dies der Fall ist, können die Protokolle der Firewall oder der *Web Application Firewall* (WAF) für die Erfüllung der Anforderungen bereits genügen.
3. Webserver oder HTTP Reverse Proxys sehen oft die entschlüsselten Anfragen. Auch diese Systeme unterstützen Protokollierung von Aktivitäten und können Kommunikationsanfragen selektiv erfassen und an ein Protokoll-Analysesystem weiterleiten.
4. Bei moderneren Applikationen werden auch API Gateways eingesetzt, die alle Anfragen vom Anwender zum Backend oder zwischen Backends (bei automatisierter Bearbeitung) entgegennehmen, um sie zum richtigen Ziel-Backend weiterzuleiten. Diese sehen den Inhalt der Anfragen und eine Protokollierung kann dort nachgerüstet werden, ohne die Applikationen selbst zu verändern.
5. Das Lesen oder Verändern von Personendaten geschieht meist über Datenbanksysteme. Diese unterstützen fast immer auch eine Protokollierung der entsprechenden Anfragen.
6. Sofern keine der vorhergehenden Empfehlungen umgesetzt werden kann, muss die Applikation erweitert werden. Um die Anwendung selbst nicht zu verändern ist es manchmal möglich einen «Wrapper» zu schreiben, dies ist eine neue Anwendung, die alle Anfragen entgegennimmt, protokolliert und dann an die eigentliche Anwendung weiterreicht, sonst aber keine Veränderungen vornimmt.

Schritt 5: Berechnen der Speichervolumen und der Analysesysteme.

Mithilfe der Entscheidungen aus den vorhergehenden Schritten, kann nun die Berechnung der Speichervolumen vorgenommen (siehe dazu Kapitel 3.3) und mit dem Leistungserbringer des Zielsystems das Einlesen und Überwachen der Protokolle festgelegt werden.

4. Konkrete Fragen zur Umsetzung / FAQ

Die aufgeführten Fragen aus der Praxis wurden an das NCSC herangetragen. Die Liste wird in Zukunft bei Bedarf ergänzt:

1) *Müssen alle im Dokument aufgeführten Empfehlungen umgesetzt werden?*

Die aufgeführten Empfehlungen zur Protokollierung sind allgemeiner Art. Um die Cybersicherheit der Systeme - und eine gewisse Nachvollziehbarkeit nach Vorfällen - gewährleisten zu können, ist es eine Notwendigkeit zu protokollieren.

Art. 4 DSV schreibt nicht vor ob und welches Analyse-Tool zu verwenden wäre und wir gehen davon aus, dass viele Datenbearbeitungssysteme «out of the box» in der Lage sind, die zusätzlich geforderte Protokollierung zu leisten.

Die Verordnung verpflichtet nur zum «Wegkopieren» der Protokolldaten. Wegen dem Datenschutz alleine müssen diese, im Gegensatz zur Cybersicherheit, nicht im Online-Speicher gehalten oder «analysiert» werden.

2) *Was heisst «allgemein öffentlich zugänglich»? Wie kann das zuverlässig bestimmt werden?*

Der Zugriff ist ohne Authentisierung möglich, z.B. auf einem Webserver.

Unter «allgemein öffentlich zugänglich» werden Informationen verstanden, die breit zugänglich sind, wie z.B. eine Adresssuche über eine Webseite. Gemäss Ausnahmebestimmung von Art. 4 Abs. 3 DSV müssen bei solchen Personendaten nur das Speichern, Verändern, Löschen und Vernichten der Daten protokolliert werden. Ziel dieser Bestimmung ist es, dass das Lesen und Bekanntgeben solcher Personendaten nicht protokolliert werden muss.

3) *Welcher Level-of-Assurance ist für die Bestimmung der Identität (gemäss Art. 4, Abs. 4 DSV) zur Protokollierung zulässig (Google-ID, Facebook oder 2-FA)?*

Die Protokollierung bezieht sich auf die Identität(en) der an der Datenbearbeitung beteiligten Person(en) und ist in diesem Sinne unabhängig vom LoA

4) *Was passiert, wenn aktuelle Systeme diese Anforderungen nicht erfüllen können und auch nicht erfüllen werden?*

Praktisch jedes bekannte System kann in irgendeiner Form protokollieren. Sonst gibt es Drittanwendungen, welche das tun können. Sollte es im Einzelfall auch keine Drittanwendung geben, dann müsste eine geeignete Lösung entwickelt, oder die Empfehlungen unter Ziffer 3.3 berücksichtigt werden, um den Vorgaben zu genügen.

5) *Ist ein Backup der Protokolldaten auch eine separate Speicherung nach Artikel 4 Absatz 5 DSV?*

Ein Backup der Protokolldaten würde der Anforderung einer separaten Speicherung nach Artikel 2 Absatz 5 DSV bereits genügen. Der Sinn der separaten Speicherung ist neben der zusätzlichen Sicherheit vor einem möglichen Angreifer v.a. auch ein verhindern, dass bei einem Ransomware Vorfall diese Daten mitverschlüsselt werden.

6) *Muss die Ausführung von automatischen Scripts auch protokolliert werden?*

Wenn diese Scripts die Personendaten Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten können - dann Ja. Ziel der Protokollierung ist die Nachvollziehbarkeit der Datenbearbeitungsvorgänge gewährleisten zu können. Dies kann beispielsweise durch das Aufzeichnen von Startzeitpunkt, Endzeitpunkt, Scriptversion, Identität des Bearbeiters, umgesetzt werden.

7) *Was ist mit NAS, SAN und anderen unstrukturierten Datenablagen? Beispiel: Öffnen eines Worddokumentes aus den Verzeichnis O:\Abteilung_A\Daten\Register\xy.docx. Müssen solche Zugriffe protokolliert werden?*

Die Bestimmung von Art. 4 Abs. 1 DSV ist im Zusammenhang mit Art. 3 Abs. 3 Bst. a DSV so zu verstehen, dass sich die Pflicht zur Protokollierung einzig auf Personendaten in automatisierten Datenbearbeitungssystemen bezieht. Beim in der Frage beschriebenen Szenario müssen Zugriffe also nicht protokolliert werden.

8) Müssen alle Logs am gleichen Ort gespeichert werden?

Nicht unbedingt und auch nicht realistisch - für die Protokollierung ist es wichtig, dass Logs vorhanden sind und in einer sinnvollen Art und Weise zusammengeführt werden können. Firewall Logs können zum Beispiel an einem anderen Ort als die Active Directory Logs gespeichert werden, solange Veränderungen und Zugriffe auf die Personendaten rekonstruierbar bleiben. Für die Informationssicherheit ist zudem wichtig, dass die Logs soweit zusammengeführt wurden, dass Anomalien erkannt werden können.

9) Dürfen externe Log-Management-as-a-Service Lösungen eingesetzt werden?

Wenn möglich sollten dazu im Anwendungsfall der Rechtsdienst und die Datenschutzberaterin oder der Datenschutzberater des Unternehmens konsultiert werden, da die Risiken im Bereich der Personendaten eher zu- als abnehmen. Wir raten davon ab. Eine Ausnahme wäre, wenn die Bearbeitung an sich schon als SaaS betrieben würde - in der Annahme, dass die oben genannten Personen schon konsultiert worden sind.

10) Bei jedem Dokument fallen in den Metadaten auch Personendaten (der beteiligten Mitarbeiter) an, nämlich bezüglich Erstellung, Änderungen und Kommentaren. Wir gehen davon aus, dass solche Personendaten mit der Protokollierung gemäss Art. 4 DSV nicht gemeint sind.

Ja, das ist richtig. Zweck der Protokollierung ist es, die bearbeiteten (d.h. in einem Dokument enthaltenen) Personendaten zu schützen. Der Umstand, dass aufgrund der Bearbeitung dieser Personendaten wieder neue Personendaten generiert werden (weil Person X das Dokument erstellt, verändert usw. hat), gibt jedoch keinen neuen Anlass zur Protokollierung. Die Personendaten, die aufgrund der Nachvollziehbarkeit der Datenbearbeitung generiert werden, sind selbst nicht Gegenstand der Protokollierung.