Baustein 43 „Protokollieren“

Version: 1.0a
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Protokollieren_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_ Protokollieren_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DSGVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO:

Anforderungen der DS-GVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit. a DS-GVO)	Transparenz
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2; Art. 24 Abs. 1 DS-GVO)	Transparenz
Angemessene Überwachung und Evaluierbarkeit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO)	Transparenz

2. Beschreibung

Das Protokollieren hat zum Zweck, eine Verarbeitungstätigkeit, die in der Vergangenheit stattfand, prüfbar zu machen. Es ist erforderlich, um der Rechenschaftspflicht nach Art. 5 Abs. 2 zu genügen. Zusammen mit der Spezifikation und Dokumentation ist es eine wesentliche Voraussetzung, um eine Verarbeitungstätigkeit datenschutzrechtlich beurteilen zu können. Prüfbarkeit bedeutet, dass Ist- und Soll-Werte aller relevanten Verarbeitungseigenschaften ermittelt und verglichen werden und somit Prüfergebnisse erzeugt werden können, mit denen fachliche, organisatorische, technische und administrative Aktivitäten und Entscheidungen, die in der Vergangenheit im Rahmen einer Verarbeitung stattfanden, überprüfbar sind (siehe SDM V2.0b Abschnitt D 4.4.3). Die Prüfbarkeit ist somit eine Voraussetzung für den Nachweis einer wirksamen Umsetzung der gesetzlichen Datenschutzanforderungen und deren Beurteilung („Rechenschaftspflicht“).

Das Protokollieren muss die Frage beantworten können, welche Instanz (Organisationseinheiten, Systeme oder für den Verantwortlichen handelnde Personen) welche Aktivität zu bestimmten Zeitpunkten an der Verarbeitungstätigkeit ausgeführt und welche Instanz das Protokoll darüber geführt hat. Protokolle werden in der Regel automatisiert erstellt („Logs“), können aber auch händisch in digitaler oder analoger Form erfolgen. Der hier verwendete Begriff „Protokolldaten“ reicht von automatisiert von Systemen, Diensten, Programmen und Diensten erzeugten Logdaten, Videoaufzeichnungen

bspw. von Aktivitäten in Serverräumen über manuell erzeugte Protokollnotizen etwa von Sitzungen bis hin zu Akteneinträgen auf der fachlichen Ebene. Für den Fall, dass ein lückenloser Nachweis geführt werden muss, ist ein Vollprotokollieren zumindest bei technischen Systemen und Diensten notwendig.

Außerdem müssen Protokolldaten valide, verlässlich, aktuell und vollständig sein (Integritätsschutz). Zumindest bei hohem Schutzbedarf ist eine gesicherte Revisionsfestigkeit von Protokollen begründet. Weisen Protokolldaten einen Personenbezug auf, dürfen sie nur zu ausgewiesenen Zwecken von speziell dazu Befugten ausgewertet werden.

Für die Protokollierung der Tätigkeiten von Beschäftigten, Administrationstätigkeiten sowie der Aktivitäten von IT-Systemen und Diensten sowie an Schnittstellen gelten ebenfalls die datenschutzrechtlichen Grundsätze der Zweckbindung und der Datenminimierung sowie die Regelungen des Beschäftigtendatenschutzes. In der Regel dürfen Protokolldaten nur zu den Zwecken, die Anlass für ihre Speicherung waren, ausgewertet werden. Über diese Zwecke müssen Beschäftige aufgeklärt werden, auch um von einem unbefugten Zugriff auf Daten zu entmutigen. Um durchgehend feststellen zu können, ob die Zweckbindung eingehalten wird, müssen Protokolldaten unterschiedlicher Ebenen (Sachbearbeitung, Fachprogramme, IT-Infrastruktur, Administration) miteinander in eine Beziehung gesetzt werden können, um die Rechtskonformität aller Aktivitäten auf den verschiedenen Ebenen, die sich letztlich zumeist aus den gesetzlichen Regelungen auf der Ebene der Fachlichkeit herleiten, nachweisen zu können (M43.S01).

Es wird empfohlen, ein Protokollierungskonzept zu erstellen, in dem alle Details sowohl zur Protokollierung selbst als auch zur Auswertung und Prüfung der Protokolle dokumentiert werden (M43.P01).

„Protokollierung“ sollte als ein Verarbeitungen-übergreifender Prozess mit Ausweis des Zwecks, der Verantwortung, der verwendeten Mittel sowie der getroffenen Schutzmaßnahmen verstanden und das Protokollierungskonzept folgerichtig organisationsweit konzipiert und umgesetzt werden. Es ist zu prüfen, ob im Zusammenhang mit einer Verarbeitungstätigkeit die Protokollierung ihrerseits als eine Verarbeitungstätigkeit aufzufassen ist (M43.P09). Dies hätte zur Folge, dass eine Rechtsgrundlage geschaffen und entsprechend geeignete Schutzmaßnahmen zur Umsetzung der DS-GVO zu treffen sind. Die Protokollierung muss dann in das Verzeichnis der Verarbeitungstätigkeit aufgenommen werden.

Was ist zu protokollieren? Zeit, Instanz, Aktivität, Speicherinstanz

Damit eine Verarbeitung vollständig geprüft werden kann, sind zumindest die folgenden Protokolldaten erforderlich:

a) **Zeitkomponente** („Wann?“),
b) **Instanz**, die eine Aktivität auslöst („Wer?“),
c) **Aktivität** bzw. **Ereignis**, das durch die Instanz ausgelöst wurde („Was?“) sowie

d) **Speicherinstanz (Quelle und Ziel)**, die diese Protokolldaten speichert („Protokollierung durch wen?“).

a) **Zeitkomponente**: Die Erfassung der Zeitpunkte von Ereignissen, die protokolliert werden, soll es ermöglichen, kausal zusammenhängende Systemaktivitäten über Programmteile, Server-, Dienst- oder Abteilungs- und Organisationsgrenzen hinweg als zusammenhängende Abläufe nachzuvollziehen. Dies erfordert bei automatisiertem Protokollieren gesichert verlässliche Zeitstempel der ausgelösten Ereignisse in Logdateien in sämtlichen Systemen. Die Zeitstempel sollten in einer menschenlesbaren und standardisierten Form, idealerweise über sämtliche zu einer Verarbeitung gehörenden Systeme, Programme und Dienste hinweg, gespeichert werden. Der Zeitpunkt des Ereignisses und der Zeitpunkt des Eintrags in die Log- bzw. Protokolldatei sollten so wenig wie möglich voneinander abweichen (M43.D01).

b) **Instanz**: Diejenige funktionale Instanz, die einen Protokolleintrag erzeugt, muss mit einem eindeutigen Bezeichner im Protokolldatensatz oder aus dem Aufzeichnungskontext heraus erkennbar und innerhalb eines Systems oder einer Netzinfrastruktur von anderen Instanzen und deren Bezeichnungen unterscheidbar sein (M43.D02).

Diese Protokolleinträge sollten es ermöglichen, Bezüge zu den Instanzenbezeichnungen aus Inventarverzeichnissen für Systemkomponenten und Organisationsplänen, Geschäftsverteilungsplänen und Berechtigungs- und Rollenkonzepten sowie dem Verzeichnis der Verarbeitungstätigkeiten herzustellen.

c) **Aktivität**: Die Aktivitäten dieser Instanzen müssen aus dem Protokoll ableitbar sein. Dies ist gegeben, wenn sie anhand zweifelsfreier Bezeichner eindeutig identifizierbar sind. Das Herausschreiben der bezeichneten Aktivität geschieht typischerweise aus dem Programmcode und nach der Abarbeitung eines Funktionsaufrufes heraus (M43.D03).

d) **Protokollierende Instanz**: Wenn es sich um die Logdatei eines unter mehreren Diensten eines Servers handelt, so muss für diese Logdatei ein eindeutiger Name festgesetzt sein, aus dem die Protokolle-speichernde Instanz und der Zeitraum der Log-Datenerfassungen hervorgehen (M43.D04), wenn sich dies nicht bereits aus dem Kontext der Protokollierung ableiten lässt.

Um zu prüfen, ob das Protokollieren aussagekräftig ist, sollte für verschiedene Szenarien (Usecases) geprüft werden, ob die vorhandenen Protokolldaten ausreichen. Dabei ist auch zu prüfen, ob die Protokolldaten-Einträge für Zeitstempel, Aktivitäten und Instanzen verständlich sind (M43.P02).

Für Protokolldatenbestände müssen Löschfristen festgelegt werden, wenn diese personenbezogene Daten enthalten. In der Regel sind zwei Löschfristen zueinander ins Verhältnis zu setzen: Zum einen die Löschfrist, die aus der Fachlichkeit abzuleiten ist, zum zweiten die Löschfrist, die aus funktionalen Gründen auf der jeweiligen Protokollierungsebene bestehen kann. Die fachlich begründete Löschfrist ist maßgebend (M43.D05).

Protokollierung der Nutzeraktivitäten einer Fachapplikation

Die Protokollierung eines Anwendungsprogramms („Fachapplikation“) ist entweder auf dem Client oder zentral auf einem Server einzurichten) (M43.D04). Eine wirkungsvolle Protokollierung der Fachapplikation muss sicherstellen, dass folgendes geprüft werden kann:

- die Aktivitäten des Sachbearbeiters,
- die Funktionen des Programms, insbesondere die Aktivitäten an Schnittstellen (typisch: Fachprogramm/Datenbank),
- die Aktivitäten der Administration an dem Fachprogramm und
- die Authentisierungs- und Autorisierungsmechanismen auf der Ebene der Sachbearbeitung.

Bei den Aktivitäten der Sachbearbeitung im Fachprogramm ist zu prüfen, welche der folgenden Aktivitäten zu protokollieren sind (M43.D06):

- das Lesen von Daten,
- die Eingabe von Daten,
- die Änderung von Daten,
- das Sperren von Daten,
- die manuelle Löschung von Daten,
- die Übermittlung von Daten,
- die Nutzung eines automatisierten Abrufverfahrens,
- der Aufruf von Programmen.

Wenn diese Aktivitäten zu protokollieren sind, müssen die folgenden Eigenschaften festgehalten werden:

- der Zeitpunkt des Zugriffs,
- der Name oder die Kennung des Zugreifenden,
- die Bezeichnung der Aktivität (Lesen, Erfassen, Ändern, Sperren, Löschen, Übermitteln, Nutzung Abrufverfahren, Programmaufruf).

Es ist festzulegen, ob nur die Tatsache des Zugriffs auf einen Datensatz oder eine Datei protokolliert wird oder ob zusätzlich auch (Auszüge aus den) Inhaltsdaten, die bei einem schreibenden Zugriff verändert wurden, im Protokoll notiert werden sollen (etwa nach dem Schema Vorher / Nachher). Die Protokolldaten müssen spätestens zum Zeitpunkt der Auswertung einem konkreten Vorgang zugeordnet werden können (bspw. über ein Akten- oder Vorgangszeichen). Im Regelfall sollte jedoch auf eine Speicherung von Inhaltsdaten auch im Protokolldatenbestand verzichtet werden (Grundsatz der Datenminimierung).

Viele Programme bieten eine Historie an, mit deren Hilfe über einen längeren Zeitraum hinweg jede einzelne Änderung rückgängig gemacht werden kann. Wenn Zeitpunkt und Autor in der Historie erfasst werden, entspricht dies einer Vollprotokollierung der

Änderungsvorgänge. Der Umfang einer Historie ist bei der Konfiguration eines Programms festzulegen. Die Historie ist entsprechend den Anforderungen zu konfigurieren und in der Regel wie eine Vollprotokollierung zu behandeln.

Wenn rechtlich begründete Sperr- und/oder Löschvorschriften für Daten bestehen, dann muss sichergestellt sein, dass anhand von Protokollauszügen fachlich nachvollzogen und belegt werden kann, dass diese Daten gelöscht bzw. deren Verarbeitung eingeschränkt wurden.

Die Protokolldaten sind so zu sichern, dass entsprechend dem Berechtigungs- und Rollenkonzept Berechtigte (insbesondere die bearbeitenden Beschäftigten) diese einsehen, aber nicht ändern können (M43.D07).

Protokollierung der Systemaktivitäten und Dienste

Ziel der Protokollierung der Systemaktivitäten ist es, Implementationen von Funktionalitäten und wesentliche Veränderungen an den IT-Systemen, den Diensten und Teilprozessen, den Betriebssystemen, den Netzen und den Speicherfunktionen und deren Anwendungen im laufenden Betrieb nachträglich nachvollziehen zu können, um deren Rechtmäßigkeit und Sicherheit, die bis auf die Sachbearbeitungsebene ausstrahlen können, nachweisen zu können.

Es ist festzulegen, welche der folgenden IT-Komponenten anhand von Protokollen bzw. Logdaten überprüfbar gemacht werden müssen (M43.D08):

- Applikationen (Fachanwendungen),
- Datenbanken,
- Dienste (wie Webserver, Mailserver, Fileserver),
- Betriebssysteme, inkl. virtualisierte Systeme,
- aktive Netzkomponenten (wie z. B. Router, Switche),
- Sicherheitskomponenten im Netz (wie Firewall, Proxy, Intrusion-Detection-System),
- Speichersysteme (SAS, NAS),
- Sicherheitskomponenten auf Servern (wie Sicherheitsgateways, Virus-Scanner),
- physikalische Zutrittssysteme.

Diese Protokolle bzw. Logdaten sollten insbesondere im Rahmen des organisationsweit betriebenen Datenschutzmanagements geprüft werden, wobei die besondere Aufmerksamkeit den Prozessen mit speziellen Datenschutz-Schutzfunktionen (etwa Hashwertbildungen für Integritätsprüfungen, Verschlüsselungen, Pseudonymisierungen, Anonymisierungen, Löschen) gelten muss. Hier können die Prüfanlässe enger als zur Prüfung anderer Eigenschaften geregelt werden (bzgl. der Regelmäßigkeit, der Häufigkeit, jedenfalls nicht nur anlassgetrieben).

Protokollierung der Administrationstätigkeiten

Ziel der Protokollierung von Administrationstätigkeiten bei personenbezogenen Verarbeitungen ist es, die Aktivitäten der Administrierenden prüfen zu können (M43.P03). Dieser Personenkreis verfügt in der Regel über umfangreiche Rechte, die es erlauben, die Strukturen einer Verarbeitung und die Berechtigungen und Rollen der Nutzenden zu ändern sowie mitunter auch unbefugt auf Inhaltsdaten zuzugreifen. Wenn die Aktivitäten der Administrierenden kaum wirkungsvoll eingeschränkt werden können, müssen diese wenigstens nachträglich überprüfbar sein. Eine Protokollierung der Aktivitäten schützt Administrierende zudem vor pauschalen Verdächtigungen und dient dem Nachweis ordnungsgemäßer Tätigkeit. Diese Protokolle müssen regelmäßig oder anlassbezogen kontrolliert, geprüft und beurteilt werden. Außerdem muss der Zugriff auf die Protokolldaten im Kontext des Datenschutz-Managements bzw. des oder der Datenschutzbeauftragten jederzeit vollumfänglich möglich sein.

Es ist festzulegen, welche Aktivitäten bei der Administration von IT-Systemen zu protokollieren sind (M43.D09):

- Systemgenerierung und Modifikation von Systemparametern,
- Verwaltung von Benutzern (Einrichtung, Änderungen, Austragungen),
- Erstellung von Rechteprofilen (Aktivitäten und Berechtigungen),
- Einspielung und Änderung von Anwendungssoftware,
- Durchführung von Datensicherungsmaßnahmen (inkl. Rücksicherungen),
- sonstiger Aufruf von Administrationsprogrammen und Verfolgen der Aktivitäten,
- Versuche unbefugten Einloggens und Überschreitung von Befugnissen.

Eine umfangreiche Protokollierung von Administrationsaktivitäten ermöglicht die Prüfbarkeit (M43.P26)

- des Zugriffs auf Inhaltsdaten, in Bezug auf Lesen, Eingabe, Änderung, Sperren oder Löschen,
- des Zugriffs auf Protokolldaten, in Bezug auf Lesen, Eingabe, Änderung, Sperren oder Löschung,
- des Zugriffs auf Daten zur Nutzerverwaltung, in Bezug auf Lesen, Eingabe, Änderung oder Löschung,
- der Änderungen von Rechteprofilen an Programmen, Datenbeständen und Verzeichnissen, insbesondere Änderungen von Datensicherungsmaßnahmen,
- des Anlegens, Änderns und Löschens von Verzeichnissen,
- des Anlegens, Änderns, Sperrens und Löschens von Nutzern und Nutzergruppen, um klären zu können, wer von wem für welchen Zeitraum das Recht eingeräumt bekommen hat, bestimmte IT-Komponenten zu nutzen oder bestimmte Übermittlungen auszulösen oder bestimmten anderen Personen bestimmte Rechte eingeräumt zu haben,

- des Aufsetzens (Installation, Konfiguration) von Systemen, Hardware und Software,
- des Aufrufs von Administrationstools,
- der Übermittlung von Daten,
- des Härtens von Systemen, Integrationssicherungsmaßnahmen der Systeme (durch Hashwertbildungen und Verwaltung) unmittelbar vor der Produktivstellung,
- der Installation, des Patchens, der Konfiguration von Betriebssystemen, Middleware und Applikationen,
- des Zugangs zu IT-Systemen und zu Räumen.

Protokollierung von Schnittstellenaktivitäten

Ziel der Protokollierung an Schnittstellen ist es, die Übermittlung von Daten prüfen zu können. Dies ist von besonderer Bedeutung, weil Übermittlungen mit einer Änderung des Zwecks einhergehen oder zu einer Verarbeitung unter einer anderen Rechtsgrundlage und mit anderen Verantwortlichen führen können.

Für den Einsatz der Protokollierung an Schnittstellen (Routern, Sicherheitsgateways) sollten die folgenden Aspekte beachtet werden (M43.P10):

- Die organisationsinternen Protokolldaten müssen den einzelnen IT-Systemen (oder Rollen), den Diensten und Fachprogrammen der Organisation eindeutig zugeordnet werden können.
- Die Größe des freien Protokollspeicherplatzes auf dem verwendeten Speichermedium sollte regelmäßig kontrolliert werden, da insbesondere bei unbefugten Datentransporten mit zahlreichenden Übermittlungsvorgängen zu rechnen ist. Es muss daher sichergestellt werden, dass diese unbefugten Aktivitäten auch in Gänze in den Protokolldaten der Systeme nachzuvollziehen sind. Bei hohem Schutzbedarf sollten geeignete Maßnahmen, wie bspw. automatische Blockierung sämtlichen Verkehrs, getroffen werden, wenn keine Schnittstellenprotokollierung des Datenstroms erfolgt.
- Ereignisse wie unzulässige Verbindungsversuche oder der Aufruf unsicherer Routinen für ungesicherte Kommunikationsverbindungen sollten im Protokolldatenbestand hervorgehoben werden. Sie sollten zu einer unverzüglichen Warnung des Administrationspersonals und/oder des fachlich Verantwortlichen über einen gesicherten Kommunikationskanal führen.

Art und Umfang bei der Protokollierung an Paketfiltern und Proxys müssen besonders beachtet werden. Hierbei gibt es wesentliche Überschneidungen aber auch Konflikte mit den Interessen an der IT-Sicherheit (z.B. Speicherung von IP-Adressen). Um die gemeinsamen und unterschiedlichen Anforderungen abzuklären, sollte der operative Datenschutz das Gespräch mit der IT-Sicherheit suchen.

Die Aktivitäten dieser IT-Systeme und Dienste müssen durch hinreichend genaue Zeitstempel sowie konsistente Bezeichnungen in eine kausal-prüfbare Beziehung sowohl zu

den Aktivitäten auf der Ebene der Sachbearbeitung als auch zu den Aktivitäten der Systemadministration gesetzt werden können.

Verarbeitung von Protokolldaten

Um Protokolldaten datenschutzrechtlich prüfen zu können, ist zu kontrollieren, welche Protokolldaten die Fachapplikationen, die verschiedenen IT-Systeme und Dienste sowie Teilprozesse insbesondere auf der Infrastrukturebene sowie die Administrationstätigkeiten an diesen Systemen erzeugen.

Bei bestehenden Systemen sollten sämtliche Protokolldaten inventarisiert werden inklusive des Nachweises, dass diese Protokollinhalte gesichtet und deren Relevanz für den Datenschutz beurteilt wurde (M43.D11).

Bereits in der Spezifikationsphase sollte definiert werden, für welche Fragen und Prüfungen welche Protokolldaten erforderlich sind. Insbesondere wenn marktgängige Standard-Programme eingesetzt werden sollen, wird es notwendig sein, noch vor der Inbetriebnahme zu prüfen, welche Protokolldaten standardmäßig erzeugt werden und ob ggfs. datenschutzrechtlich erforderliche Änderungen beim Hersteller zu verlangen sind.

Protokolldaten werden von verschiedenen Systemen und Diensten erzeugt und liegen daher in der Regel in verschiedenen Formaten vor. Um die Prüfung der Protokolle zu erleichtern ist es vielfach hilfreich, die „rohen“ Protokolldaten wie folgt aufzubereiten:

- **Filterung:** Protokolldaten sollten so gefiltert werden, dass unnötige Protokollmeldungen aussortiert werden (M43.D12).
- **Normalisierung:** Protokolldaten sollten bspw. durch Konvertieren in ein einheitliches Datenformat standardisiert werden (M43.D13).
- **Aggregation**: Protokolldaten identischen Inhalts sollen zusammengefasst werden (M43.14).
- **Kategorisierung:** Protokollmeldungen sollten nach Systemen, Aktivitäten oder nach Risikobereichen kategorisiert werden, um den Informationsgehalt zu erhöhen (M43.D15).
- **Priorisierung:** Die Ausgabe von Protokollmeldungen sollten dynamisch priorisiert werden können, um deren Beurteilung zu vereinfachen (M43.D16).

Generell ist für diese Verarbeitungsschritte von Protokolldaten sicherzustellen, dass die Skripte zur Verarbeitung von Protokolldaten integritätsgesichert zum Einsatz kommen und ausschließlich die oben genannten Schritte umsetzen, ohne den Inhalt der Protokolldaten zu ändern (M43.D17).

Beispiele für weitere aufbereitete Ausgaben von Protokolldaten, mit denen der laufende Betrieb insbesondere durch die Administration sichergestellt wird, sind:

- **Gruppierung** und Markierung zusammengehörender Protokolldaten,

- Anzeige **relevanter Protokolldaten** aufgrund charakteristischer Zeichenketten bzw. Ausblenden irrelevanter Daten mittels regulärer Ausdrücke,
- **statistische Analyse** der Protokolldaten (z. B. auf die Frage: Wie oft traten welche Meldungen auf?).

Um die Aussagekraft relevanter Protokolldaten zu erhöhen sollten Tools eingesetzt werden, die abhängig von einer erkannten Auffälligkeit Aktionen (z. B. Ausführen eines Befehls) ermöglichen (M43.S0312). Auffällige Protokolleinträge sind beispielsweise:

- gehäuft auftretende Anfragen an Ports, auf denen keine Dienste laufen,
- nicht erfolgreiche Zugriffsversuche auf Komponenten eines Servers, insbesondere auf Sicherheitsgateways,
- aus einem nicht-vertrauenswürdigen Netz eintreffende Pakete mit IP-Adressen des vertrauenswürdigen Netzes (Hinweis auf IP-Spoofing),
- verdächtige, ausgehende Verbindungen von Servern aus dem vertrauenswürdigen Netz (diese können ein Anzeichen dafür sein, dass nach einem erfolgreichen Einbruch der Angreifer Daten aus dem vertrauenswürdigen Netz nach außen kopiert oder von außen Dateien nachlädt, die er für seine weiteren Aktivitäten braucht.),
- nicht-spezifizierte Protokolleinträge,
- unberechtigter Zugang und Zugriff,
- Autorisierungsverstöße.

Zur Analyse von Protokolldaten sollten „Logfile-Analyzer“ eingesetzt werden (M43.S02). Zeichenketten, nach denen Protokolldatenbestände durchsucht werden, sollten dokumentiert werden (M43.D18). Dadurch können für die Prüfung verantwortliche Beschäftigte nachvollziehen, welche Analysen durch die Systemadministration durchgeführt werden.

Vorverarbeitete Protokolldaten sind, zumeist geleitet von bestimmten inhaltlichen Fragestellungen, zu Reports zusammenzustellen, die den verantwortlichen Beschäftigten zur Prüfung und letztlich dem Verantwortlichen zur Entscheidung über die datenschutzrechtliche Konformität der Datenverarbeitung vorgelegt werden. Dabei sind Protokolldaten in der Regel mit inhaltlichen Daten zu korrelieren (M43.P04).

Behandlung von Prüfergebnissen

Um relevante Prüfergebnisse für die Wirksamkeit der Schutzmaßnahmen im laufenden Betrieb erzeugen zu können, müssen die Protokolldaten, Protokollsysteme und die daran anknüpfenden Prüfprozesse hinreichend spezifiziert sein. Für die Spezifikation bzw. Planung der Protokollierung über die zuvor genannten Ebenen sind folgende Fragen relevant (M43.P05):

- Welche Prüfdaten sind zu erzeugen, um die Wirksamkeit der Maßnahmen zur Umsetzung der Gewährleistungsziele nachweisen zu können oder um die fehlende Wirksamkeit der Maßnahmen im laufenden Betrieb entdecken zu können?
- Welche darauf bezogenen Prüfergebnisse sind einer gesonderten, über verschiedene Systeme hinweg, zu vertiefenden Beurteilung zu unterziehen?
- Wer ist für die Herstellung und die nachfolgende Beurteilung von Prüfergebnissen zuständig (Rollen oder Personen)?
- Auf welche Weise müssen Prüf- und Beurteilungsergebnis übermittelt werden?
- Bei welchen Warnungen und Vorfällen, die im Rahmen der Überwachung des Datenschutzes und der IT-Sicherheit anfallen, ist auch der/die IT-Sicherheitsbeauftragte bzw. Datenschutzbeauftragte zu beteiligen?

Die Ursachenforschung bei der Feststellung von fehlerhaften bzw. nicht-rechtskonformen Abweichungen ist wichtig. Es muss das Ziel sein, den laufenden Betrieb rechtskonform zu gestalten bzw. zu halten und Fehler in Zukunft zu verhindern oder zumindest möglichst schnell zu beheben. Die Analyse von Fehlern, die Entscheidungen und die eingeleiteten Maßnahmen nach erfolgter Ursachenforschung sind zu dokumentieren (M43.P08).

Zwei spezielle Aspekte des Protokollierens sollen noch kurz angesprochen werden: Das „Monitoring“ und das „Quittieren“. Im Unterschied zur Protokollierung ist ein Monitoring die laufende Beobachtung, welche Aktivitäten von welcher Instanz aktuell ausgeführt werden, um unmittelbare Entscheidungen über den Fortgang treffen zu können (z.B. Pförtner-Aktivitäten). In der Regel werden die Entscheidung, der Zeitpunkt und die betroffene Instanz in einem Protokoll notiert. „Quittungen“ werden vielfach eingesetzt, um Betroffenen die korrekte Ausführung in Bezug auf ein bestimmtes Ereignis, dass eine bestimmte Instanz zu einem Zeitpunkt ausgelöst hat, zu bestätigen. Auch Quittungsdaten werden zumeist gesammelt und sind als Protokolldaten geeignet, um Systemzustände in der Vergangenheit bei den Beteiligten zu dokumentieren.

3. Differenzierung bei hohem Schutzbedarf

Um den Anforderungen an Transparenz einer Verarbeitungstätigkeit auch bei hohem Schutzbedarf gerecht zu werden, sind erhöhte Anforderungen an die Qualität insbesondere der Revisionsfestigkeit (Integrität) und des Beweiswerts der Protokolldaten zu berücksichtigen. Bei der Protokollierung müssen die Interessen nicht nur der Stelle, sondern auch der Betroffenen sowie der Aufsichtsbehörden beachtet werden.

Resultiert aus der Verarbeitung ein hohes Risiko für die betroffenen Personen, wirkt sich dies grundsätzlich auch auf die Inhalte sowie die Auswahl und Ausgestaltung von Maßnahmen aus, mit denen die Inhalte eines Protokolls bzw. Logs generiert, gespeichert, transformiert, übermittelt und geschützt werden. Eine generelle Strategie zur Umsetzung von technischen und organisatorischen Maßnahmen bei hohem Schutzbedarf besteht darin, die Maßnahmen der verschiedenen Gewährleistungsziele auch auf die Schutzmaßnahmen selber anzuwenden. So sollte bspw. die Integrität von Protokolldaten durch regelmäßiges Hashen,

die Vertraulichkeit dieser Daten durch Verschlüsselung und der Zugang zu Protokolldaten im Berechtigungs- und Rollenkonzept sichergestellt werden.

Ein hoher Schutzbedarf stellt höhere Anforderungen an die Transparenz einer Verarbeitungstätigkeit und kann daher eine Vollprotokollierung erfordern. Zudem gibt es in einigen Fällen rechtliche Regelungen zum Umfang der Protokollierung bei hohem Schutzbedarf.

Für Verarbeitungstätigkeiten, aus denen ein hohes Risiko resultiert, sollte ein zertifizierter Zeitstempel genutzt werden (M43.D19).

Sofern administrative Tätigkeiten protokolliert werden, muss der Verantwortliche dafür Sorge tragen, dass auch diese Aktivitäten der o.g. Strategie folgen. Die Protokollierung muss so ausgestaltet sein, dass Administratoren die eigenen Aktivitäten in den aufgezeichneten Protokolldaten nicht manipulieren können. Geeignete technische Maßnahmen, beispielsweise, Screencasts während der tatsächlichen administrativen Tätigkeit, sollten betrachtet werden. Die Auswertung der administrativen Protokolldaten ist festzulegen, beispielsweise durch regelmäßige Stichprobenkontrollen.

Zur Speicherung aller Protokoll- und Logdaten sollte ein dedizierter Protokollserver betrieben werden, für dessen Implementation, Konfiguration und Betrieb wiederum technische und organisatorische Maßnahmen anhand des vollständigen Sets an Gewährleistungszielen zu treffen sind (M43.P06). Insbesondere sind Protokolldaten beim Transfer von Produktivsystemen auf andere Computer, wie bspw. einen Protokollserver, gegen unbefugte Kenntnisnahmen und Änderungen zu schützen (M43.P07).

4. Referenzen

BSI: *OPS.1.1.5 Protokollierung*
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html;jsessionid=8B275BA38F10A2449C5258B4839E9CE4.1_cid369

5. Zusammenfassung der Maßnahmen

Die einzelnen Maßnahmen können hinsichtlich des Anwendungsbereichs unterschieden werden nach Maßnahmen, welche primär auf einzelne Verarbeitungen angewandt werden sollten (*kursive Darstellung*) und solche, welche primär die gesamte Organisation betreffen und damit im Rahmen des Datenschutzmanagements gebündelt und verwaltet werden sollten (nicht-kursive Darstellung). Weiterhin sind alle Maßnahmen grob den Phasen des Datenschutzmanagement-Prozesses (siehe SDM-Methode) zugordnet. Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden weiterhin aufgeführt (~~durchgestrichene Darstellung~~). Damit bleibt die Nummer einer Maßnahme bei einer neuen Version erhalten. Die Spalte „Gültigkeit“ gibt an, seit welcher Version die Maßnahme in der enthaltenen Form gültig ist. Bei ungültigen

Maßnahmen enthält diese Spalte die Versionsnummer des Bausteins, in der die Maßnahme letztmalig gefordert bzw. empfohlen wurde.

Ebene Daten

Nr.	Maßnahme	PDCA	Gültigkeit
M43.D01	*Zeitstempel standardisieren*	P	V1.0
M43.D02	*Bezeichner der Instanz festlegen*	P	V1.0
M43.D03	*Bezeichner für Aktivität festlegen*	P	V1.0
M43.D04	*Protokollierungsinstanz festlegen*	P	V1.0
M43.D05	*Löschfristen für Protokolldaten festlegen*	P	V1.0
M43.D06	*Inhalte der Protokollierung der Sachbearbeitung festlegen*	P	V1.0
M43.D07	*Integritätssicherung der Protokollierung auf Ebene Sachbearbeitung*	P	V1.0
M43.D08	Inhalte der Protokollierung der Systemaktivitäten festlegen	P	V1.0
M43.D09	Inhalte der Protokollierung von Administrationstätigkeiten festlegen	P	V1.0
M43.D10	Inhalte der Protokollierung der Schnittstellen festlegen	P	V1.0
M43.D11	*Protokolldaten inventarisieren (kontrollieren, prüfen, beurteilen)*	P, D	V1.0
M43.D12	*Protokolldaten filtern*	P, D	V1.0
M43.D13	*Protokolldaten normalisieren / standardisieren*	P, D	V1.0
M43.D13	*Protokolldaten normalisieren / standardisieren*	P, D	V1.0
M43.D14	*Protokolldaten aggregieren / zusammenfassen*	P, D	V1.0
M43.D15	*Protokolldaten kategorisieren*	P, D	V1.0
M43.D16	*Protokolldaten priorisieren*	P, D	V1.0
M43.D17	Protokollbearbeitungsskripte integritätssichern	P, D	V1.0
M43.D18	*Liste mit kritischen Zeichenketten für Protokolldatenanalyse erstellen*	P, D	V1.0
M43.D19	*Einsatz von zertifizierten Zeitstempeln in Protokolleinträgen*	P, D	V1.0

Ebene Systeme

M43.S01	*Korrelationen von Protokollen über verschiedene Ebenen der Verarbeitungstätigkeiten prüfen zwecks Sicherstellung der Zweckbindung und „Abschreckung“ vor unbefugtem Mißbrauch*	P, D, C	V1.0
M43.S02	*Protokolldaten mit „Log-Analyzern“ analysieren*	P, D, C	V1.0
M43.S03	*Ausführen von Befehlen, wenn bestimmte Protokolleinträge erscheinen*	P, D	V1.0

Ebene Prozesse

M43.P01	Protokollierungskonzept erstellen	P	V1.0

M43.P02	*Usecases bilden und Vollständigkeit und Verständlichkeit von Protokolldaten prüfen*	P, C	V1.0
M43.P03	*Aktivitäten der Systemadministration protokollieren*	P, D	V1.0
M43.P04	*Reports aus Protokolldaten erstellen*	D, C	V1.0
M43.P05	*Fragen zur Spezifikation von Protokolldaten*	P, D, C	V1.0
M43.P06	Einsetzen eines Protokollservers	P, D	V1.0
M43.P07	*Sichern des Transfers von Protokolldaten*	P, D	V1.0
M43.P08	*Dokumentation von Prüfergebnissen, insbesondere wenn Fehler behoben wurden*	D, C	V1.0
M43.P09	*Prüfen, ob Protokollierung ihrerseits als Verarbeitungstätigkeit zu gestalten ist*	P	V1.0

6. Bezug zum Datenschutzmanagement

Dieser Baustein bezieht sich in weiten Teilen auf Anforderungen an eine Gesamtprotokollierung einer Organisation und bildet Nachweispflichten des Verantwortlichen ab, welche auf ein einzelnes Verfahren aber auch die gesamte Organisation angewendet werden können. Wird der Baustein auf die die gesamte Organisation angewendet, sind die getroffenen Maßnahmen im Datenschutzmanagement der Organisation zu betrachten.

7. Anmerkung zur Nutzung dieses Bausteins

Dieser Baustein darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird:

„Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Daten sind mit einem Veränderungshinweis im Quellenvermerk zu versehen. Datenlizenz Deutschland – Namensnennung – Baustein Protokollieren (www.govdata.de/dl-de/by-2-0).“