Baustein 43 „Protokollieren“

Version: 2.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V3.1_Protokollieren_V2.0	01.Juni 2026	
SDM-V2.0_ Protokollieren_V1.0a	21. Juli 2020	30. Juni 2026
SDM-V2.0_Protokollieren_V1.0	30. Juni 2020	20. Juli 2020

1 Beschreibung

1.1 Einführung

Protokolldaten im Kontext des operativen Datenschutzes sind die Voraussetzung dafür, die Verarbeitung von personenbezogenen Daten nachvollziehen zu können.

Definition

„Protokollierung“ soll das Erzeugen, die Organisation des Protokollierungsprozesses, die Auswertung im Sinne des zweckbestimmten Nutzens, die Offenlegung sowie das Archivieren und Löschen von Protokoll- bzw. Logdaten auf allen Ebenen und für alle Phasen einer Verarbeitung bezeichnen. Protokolldaten werden in der Regel automatisiert erstellt („Logs“), können aber auch händisch in digitaler oder analoger Form erfolgen. Der hier verwendete Begriff „Protokolldaten“ reicht von a) Logdaten, die automatisiert von Systemen, Programmen und Diensten erzeugten werden über b) manuell erzeugte Protokollnotizen bspw. von Sitzungen bis hin zur c) fachlichen Ebene, in der Akten als Protokolle ordnungsgemäßen Agierens geführt werden.

Zusammen mit der Spezifikation, die eine Prüfbarkeit für die Zukunft, und Dokumentation, die eine Prüfbarkeit in der Gegenwart und vor Ort am Prüfgegenstand sicherstellen soll, ist Protokollierung eine wesentliche Voraussetzung dafür, eine Verarbeitung für die Vergangenheit technisch-organisatorisch bzgl. sämtlicher beteiligter IT-Komponenten, Organisation(seinheit)en und menschlicher Aktivitäten zu prüfen und datenschutzrechtlich beurteilen zu können.

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.

Besonderheiten

Im Vergleich zu anderen Maßnahmen zur Sicherstellung des Datenschutzes weist die Protokollierung einige besonders beachtenswerte Eigenschaften und Besonderheiten auf.

Eine Besonderheit besteht darin, dass durch die Protokollierung eine neue Gruppe datenschutzrechtlich betroffener Personen erzeugt wird. Zusätzlich zu den Betroffenen, deren Daten innerhalb der Verarbeitung unmittelbar verarbeitet werden, werden auch unter Umständen Daten weiterer Personen verarbeitet, z.B. von Beschäftigten der Organisationseinheit oder von Mitarbeitenden beauftragter Dienstleister. Als Beschäftigte sollen diejenigen bezeichnet werden, die in Form der fachlichen Bearbeitung (Sachbearbeitung,) oder mittelbar, in Form der technischen oder organisatorischen Administration, an einer Verarbeitung beteiligt sind. Dies hat zur Folge, dass die Protokollierung in einem

ganz besonderen Maße rechtlichen Anforderungen und deren Abwägungen unterliegt, um das richtige Maß für eine datenschutzrechtlich gebotene Verhaltenskontrolle Beschäftigter gegenüber den Betroffenen festzulegen und dabei zugleich eine unzulässige Leistungskontrolle der Beschäftigten auszuschließen.

Des Weiteren erzeugen IT-Komponenten in der Regel Logdaten automatisch, um bei Fehlfunktionen die Ursachen finden zu können. Dies hat in der Praxis zur Folge, dass viele Logdaten funktional gut begründbar vorgehalten werden, aber aufgrund fehlerfreien Funktionierens nur selten oder gar nicht kontrolliert und dann über sehr lange Zeiträume, auf Vorrat gespeichert und unbeachtet, nicht gelöscht werden. Viele auch vermeintlich rein technische Daten können, mit ein wenig zusätzlicher Kontextierung, einen Personenbezug aufweisen. Deshalb müssen auch alle technischen Logdaten, wenn sie zur Aufrechterhaltung der Prüfbarkeit der Funktionalität im Rahmen einer Verarbeitung nicht mehr erforderlich sind, grundsätzlich zusammen mit den unmittelbaren personenbezogenen Daten, ebenfalls gelöscht werden. Davon kann es Ausnahmen geben.

Diese Ausnahme entsteht aus der weiteren Besonderheit, dass viele IT-Komponenten, insbesondere die Komponenten auf der Ebene der Infrastruktur, von unterschiedlichen IT-Fachanwendungen gemeinsam verwendet werden. Das heißt, dass die Protokolldaten dieser IT-Komponenten bzw. Betriebsmitteln von unterschiedlichen Verarbeitungen zwecks Prüfbarkeit gespeichert werden müssen. Das kann dazu führen, dass die Nutzung bzw. Speicherung der gleichen Protokolldaten im Kontext der einen Verarbeitung nicht mehr erforderlich ist, im Kontext einer anderen Verarbeitung wie bspw. zur Sicherstellung der IT-Sicherheit, aber sehr wohl weiterhin. Um solche Konfliktfälle von zugleich bestehenden Lösch- und Speicheranforderungen an das gleiche Datum zu erkennen und dann das rechtlich gebotene Speichern oder Löschen oder Archivieren von Teilmengen der Protokolldaten umzusetzen, sollte für die Protokollierung neben einem datenschutzrechtlich geforderten verfahrensbezogenen, fachlichen Protokollierungskonzept ein die betroffenen Verarbeitungen übergreifendes, organisationsweites Protokollierungskonzept erstellt werden, in dem für diese Konflikte Regelungen, bis hin zu eigenen Rechtsgrundlagen, festgelegt werden. Dieser Baustein behandelt, wegen der Verarbeitungsbezogenheit der DS-GVO primär dasjenige Protokollieren, welches nur für eine spezifische Verarbeitung gefordert ist.

1.2 Anwendungsbereich

Der Baustein Protokollierung muss grundsätzlich auf alle Phasen bzw. auf jeden Verarbeitungsvorgang angewendet werden, sowohl auf der Ebene des Fachverfahrens als auch auf der Ebene der Nutzung von Systemen und Diensten; Protokollierung muss für jedes Betriebsmittel gewährleistet sein. Protokolldaten müssen, neben der Fehleranalyse, den Nachweis zu führen erlauben, dass die, gemäß den Gewährleistungszielen getroffenen, Schutzmaßnahmen tatsächlich wirkungsvoll funktioniert haben.

Die angemessene Dimensionierung der Protokollierung im Hinblick auf Erzeugung, Speicherung, Übermittlung, Nutzung, Löschung und Transparenz von Protokolldaten und deren Auswertung ist abhängig von der Höhe des Risikos, das von einer Verarbeitung für Betroffene ausgeht. Eine hochriskante Verarbeitung personenbezogener Daten stellt grundsätzlich auch hohe Anforderungen an die Protokollierung (Stichwort: „revisionsfeste Protokollierung“).

1.3 Zweck

Protokolldaten ermöglichen zu prüfen, ob die funktional zweckbestimmten sowie die von der DS-GVO geforderten Eigenschaften der Verarbeitung im Hinblick auf die Beachtung der Rechte und Freiheiten betroffener Personen durch die Daten verarbeitende Organisation, als Verantwortlicher im Sinne Art. 4 Nr. 7 i. V. m. Art. 24 DS-GVO, in der Vergangenheit erfüllt wurden. Der datenschutzrechtlich begründete

Zweck des Protokollierens besteht in der Herstellung der Auswertbarkeit von Protokolldaten im Hinblick auf die Prüfbarkeit der Erfüllung der Anforderungen der DS-GVO.

Das Protokollieren ist erforderlich, damit der Verantwortliche nachweisen kann, dass jede seiner Verarbeitungen personenbezogener Daten gemäß der DS-GVO erfolgt (Art. 24 Abs. 1 DS-GVO). Die Protokolldaten müssen es insbesondere den Aufsichtsbehörden erlauben, die Verarbeitungen zu prüfen.

Die Nutzung von Roh- oder vorverarbeiteten Protokoll- und Logdaten ist abhängig von den unterschiedlichen Zwecken, mit denen auf diese Daten zugegriffen wird. Die vier datenschutzrechtlich wesentlichen Zwecke sind die Sicherstellung

- der Überprüfbarkeit der Sachbearbeitung;
- der Überprüfbarkeit und Aufrechterhaltung des technischen Betriebs;
- der Überprüfbarkeit von Administrationstätigkeiten;
- der Überprüfbarkeit, dass die vorgenannten Aktivitäten kontrolliert wurden.

Vielfach werden durch umgesetzte Protokollierungsanforderungen Daten erzeugt, die zu unterschiedlichen Zwecken genutzt werden. So müssen auch Anforderungen der Informationssicherheit, des Qualitätsmanagements, der Korruptionskontrolle usw. beim Protokollieren berücksichtigt werden, die aber weniger auf die Bestätigung rechtskonformer Ausführungen als vielmehr, bspw. als Monitoring eingerichtet, auf das Entdecken von Ausnahmen, Störungen und Informationssicherheitsvorfällen im Rahmen eines „Security Information and Event Managements“ (SIEM) abstellen. Ein Monitoring ist als ein Spezialfall des Protokollierens zu verstehen, dessen Zweck darin besteht, zum Zeitpunkt „jetzt“ spezifische Ereignisse definierter Entitäten beobachten und über den Fortgang einer Verarbeitung unmittelbar entscheiden zu können, bspw. als eine Maßnahme für Verarbeitungen mit hohem Risiko.

Der Schwerpunkt der datenschutzrechtlich motivierten Protokollierung besteht vornehmlich darin, das korrekte Funktionieren der erforderlichen Schutzmaßnahmen des Datenschutzes nachweisbar zu machen bzw. deren Fehlen feststellbar zu machen und so die datenschutzrechtlichen Nachweispflichten des Verantwortlichen zu unterstützen. Die Aktivitäten der verwendeten IT-Systeme und weiterer technischer Betriebsmittel müssen anhand der Protokolldaten geprüft werden können, ob sie den Transparenzanforderungen bzgl. der Gewährleistungsziele genügen. Diese Anforderung der Sicherstellung der Prüfbarkeit ist bspw. bei der Beschaffung von IT-Komponenten zu beachten.

1.4 Kategorien personenbezogener Daten und betroffener Personen

Der Bezugspunkt der Gestaltung einer Verarbeitung, mit der notwendigen Protokollierung von Aktivitäten der Beschäftigten und der genutzten IT zu den oben genannten Zwecken, ist die fachliche Sachbearbeitung einer Verarbeitung. Jeder Protokollierungsvorgang muss deshalb in einer mit der Verarbeitung begründbaren Beziehung stehen.

Bei personenbeziehbaren Protokolldaten kann es sich grundsätzlich

a) um Daten betroffener Personen handeln, deren Daten in einer Verarbeitung verarbeitet wurden (Betroffenendaten) oder
b) um Beschäftigtendaten, inkl. Administrator*innen und Vorgesetzten, handeln, die an der Verarbeitung beteiligt waren (Beschäftigtendaten) oder von Mitarbeitenden beauftragter Dienstleister sowie
c) um mittelbare personenbeziehbare Daten, die in einer Kette von automatischen Weiterverarbeitungen erzeugt und als Logdaten gespeichert werden (Technikdaten) wie zum

Beispiel die Logdaten eines Internet-Routers bzgl. der IP-Pakete oder eines Mailgateways bzgl. bspw. der beteiligten Mailserver, Sender und Empfänger von Mails.

zu a) Wenn sichergestellt wird, dass zwischen einer Aktivität innerhalb einer personenbezogenen Verarbeitung und dem entsprechenden Eintrag dieser Aktivität in den Protokolldaten ein eindeutiger kausaler Zusammenhang hergestellt werden kann – dies sollte bei vollem Zugriff auf die Daten und einem hinreichend hochauflösenden Zeitstempel grundsätzlich möglich sein -, dann besteht in der Regel kein Anlass, dass verarbeitete Inhaltsdaten betroffener Personen auch in den Protokolldaten explizit gespeichert werden.

zu b) Generell gilt, dass die Arbeit von Beschäftigten für den Verantwortlichen überprüfbar sein muss und sie deshalb datenschutzrechtlich in einem gewissen Ausmaß die Prüfbarkeit ihrer Arbeit akzeptieren müssen. Dieses in einem angemessenen Maße prüfbar zu machen ist deshalb ein wesentlicher Zweck der Protokollierung. Beschäftigte sind dabei aus Gründen der Transparenz über die Verarbeitung ihrer Daten und die Zwecke zu unterrichten. Zugriffsprotokolle sind zudem auch grundsätzlich vom Herausgabe-Anspruch nach Art. 15 DS-GVO umfasst, die Identität der betroffenen Beschäftigten muss jedoch nur in Ausnahmefällen offengelegt werden (EuGH, Urteil vom 22.6.2023 – C-579/21).

zu c) Logdaten, die von Betriebsmitteln und IT-Diensten automatisiert erzeugt werden und dadurch das Verhalten oder die Leistung der Beschäftigten auf der Ebene der Sachbearbeitung ausgewertet oder/und überwacht werden können oder Rückschlüsse zu von der Verarbeitung betroffenen Personen und Beschäftigten hergestellt werden können, sind grundsätzlich ebenfalls als personenbeziehbare Daten aufzufassen und sind als solche nach den Regeln der DS-GVO zu verarbeiten.

1.5 Rechtliche Anforderungen

Verantwortliche müssen den Nachweis dafür erbringen können, dass die von ihnen verantwortete Verarbeitung die Anforderungen der DS-GVO umsetzt (SDM: „Anforderung B1.8 Rechenschafts- und Nachweisfähigkeit“). Die getroffenen Maßnahmen sind bezüglich ihrer Wirksamkeit regelmäßig zu evaluieren (SDM: „Anforderung B1.21 Evaluierbarkeit“). Verantwortliche müssen für betroffene Personen Transparenz bezüglich der sie betreffenden Verarbeitungen schaffen (SDM: „Anforderung B1.1 Transparenz für Betroffene“). Weiterhin ist die Verarbeitung hinsichtlich ihrer Sicherheit zu überwachen, um relevante Abweichungen im Betrieb feststellen und im Nachhinein überprüfen zu können (SDM: „Anforderung B1.23 Angemessene Überwachung der Verarbeitung“). Hierzu ist es erforderlich, dass jede für diese Zwecke erhebliche Aktivität einer Person oder eines Programms, einschließlich der aus den Gewährleistungszielen begründeten Maßnahmen des operativen Datenschutzes oder der IT-Sicherheit, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, angemessen protokolliert wird.

Nr.	Anforderungen der DS-GVO	Gewährleistungsziel
B1.1	Transparenz für Betroffene (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DS-GVO)	Transparenz
B1.8	Rechenschafts- und Nachweisfähigkeit (ErwGr. 74, Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)	Transparenz
B1.21	Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO).	Sie ist als ein Prozess umzusetzen, der alle Anforderungen umfasst

		(siehe Kap. D4 Datenschutzmanagement mit dem SDM).
B1.23	Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DS-GVO)	Transparenz, Integrität

Die Protokollierung auf der fachlichen Ebene, d.h. die Erzeugung und Auswertung von Protokolldaten zu fachrechtlichen Vorgaben, ist eine datenschutzrechtlich umzusetzende Schutzmaßnahme zum Zweck der Erzeugung von Transparenz für die Verarbeitung. Eine fachliche Protokollierung ist deshalb der Verarbeitung als Schutzmaßnahme zuzurechnen und ist daher von der Rechtsgrundlage der Verarbeitung grundsätzlich bereits umfasst. Typische Controlling-Zwecke sind, neben dem hier im Vordergrund stehenden Nachweis der DS-GVO-Konformität der Verarbeitung und des Datenschutzmanagements, die Aktivitäten des IT- oder Informationssicherheitsmanagement, insbesondere mit Bezug zu den Richtlinien zur Netzwerk und Informationssicherheit (NIS), der Innenrevision bzw. das Qualitätsmanagement allgemein sowie darüber hinaus haftungsrechtlich begründete Verarbeitungen. All diese Verarbeitungen mit Rückgriff auf Protokolldaten sind ihrerseits mit einer eigenen Rechtsgrundlage auszugestalten, die dann insofern berechtigt auf „ihre“ Protokolldaten zugreifen dürfen. Ebenso können bzw. müssen bspw. externe Aufsichts- oder Sicherheitsbehörden berechtigt auf diese Daten zugreifen. Hinzukommen möglicherweise berechtigte Interessen anderer Abteilungen an Protokolldaten wie bspw. Marketing, Wissenschaft und Forschung sowie Datenanalysen im Kontext von KI-Trainings. Die Erzeugung, Speicherung, Verarbeitung, Übermittlung und Löschung oder Archivierung der Protokolldaten auch für diese Zwecke müssen rechtlich erfasst und im organisationsweiten Protokollkonzept geregelt sein.

Neben dem Rahmen datenschutzrechtlicher Regelungen durch die DS-GVO regeln weitere spezialgesetzliche Vorschriften die Protokollierung wie bspw. § 76 BDSG i. V. m. Art. 25 JI-Richtlinie der Europäischen Union (RL (EU) 2016/680) sowie auch weitere, spezial- und landesgesetzliche Regelungen, wie bspw. Art. 51 des Polizeiaufgabengesetzes von Bayern (PAG).

1.6 Risiken für eine Person, die ohne und durch die Maßnahme entstehen

Ohne Protokollierung ist es nicht möglich, für die Vergangenheit zu prüfen, ob die Anforderungen der DS-GVO, insbesondere die Umsetzung der Anforderungen der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO) und der Betroffenenrechte, durch den Verantwortlichen erfüllt wurden. Zugleich kann eine zu hochauflösende, vollumfängliche Protokollierung dazu führen, dass auch nicht erforderliche Daten, insbesondere über Personen die mit Sachbearbeitung befasst sind, erhoben werden.

Generell gilt, dass Protokolldaten ihrerseits durch Schutzmaßnahmen geschützt werden müssen, insbesondere bei einer mit hohen Risiken verbundenen Verarbeitung personenbezogener Daten. Das heißt konkret, dass deren Verfügbarkeit durch Redundanz wie bspw. Backups, Integrität durch Prüfsummenmanagement, Vertraulichkeit durch Verschlüsselung, Intervenierbarkeit durch Annotationsoptionen, Nichtverkettung durch Datenminimierung, Zweckbindung sowie Trennung von Abteilungen, Datenbeständen und IT-Systemen sowie Transparenz wiederum durch eine Protokollierung auch der Auswertung von Protokolldaten sichergestellt werden muss.

1.6.1 Risiken für eine Person, die ohne Protokollieren bestehen

Unzulässige Zweckänderungen und Zweckdehnungen
Ohne eine angemessene Protokollierung des Betriebs von IT-Komponenten bzw. Betriebsmitteln sowie den Aktivitäten der Beschäftigten einer Organisation besteht das Risiko, dass eine Verarbeitung hinsichtlich ihrer zweckgemäß funktionalen Implementierung und insbesondere Zweckdehnungen oder nicht vereinbare Zweckänderungen nicht entdeckt werden können (ErwGr. 50, Art. 5 Abs. 1 lit. b, Art. 6 Abs. 3 und 4 DS-GVO).

Mangelnde Prüfbarkeit
Es besteht das Risiko, dass in Bezug auf den Zweck der Verarbeitung nicht ausreichend prüfbar ist, durch welche Entität oder Instanz, wann und in welcher Form personenbezogene Daten erzeugt, gespeichert, verändert bzw. verarbeitet, abgegriffen bzw. übermittelt oder gelöscht bzw. archiviert wurden.

Keinen Einfluss auf die Ausgestaltung
Ohne Protokollierung können Mängel in Bezug auf die zweckbestimmte Verarbeitung sowie die Funktionalität der dabei eingesetzten Informationstechniken, nicht behoben werden. Protokollierung macht die Verarbeitung insgesamt steuerbar.

Ungewissheit bzgl. der Korrektheit der Verarbeitung
Ohne Protokolldaten können Soll-Vorgaben nicht für alle in der Verarbeitung eingesetzten Komponenten anhand von Ist-Werten geprüft und in Bezug auf ihre Korrektheit funktional und rechtlich beurteilt werden.

Unzuverlässige Verfügbarkeit der Verarbeitung
Ohne Protokollierung ist nicht feststellbar, ob eine Verarbeitung stattgefunden hat oder nicht.

Mangel an Vertraulichkeit
Ohne Protokollierung kann nicht festgestellt werden, ob die Umstände der Verarbeitung so eingerichtet sind, dass nur Befugte Kenntnis von den Daten genommen werden konnten.

Regelwidrige Datenverarbeitung
Speziell in Bezug auf Beschäftigte kann eine mangelhafte Protokollierung, insbesondere im Schadensfall, zu dem Verdacht führen, dass diese nicht regelkonform entsprechend der DS-GVO oder einer Sicherheitsleitlinie gearbeitet haben. Protokolldaten sind eine Voraussetzung dafür, dass Verantwortliche und Beschäftigte nachweisen können, normenkonform gearbeitet zu haben.

Dynamische Informationstechnik
Die Verarbeitung und die dafür verwendeten informationstechnischen Mittel werden u. U. durch Software-Aktualisierungen in einer Weise verändert, die zu einer unzulässigen Verarbeitung führen kann. Bleibt diese Veränderung unbemerkt oder in seiner Tragweite unbekannt, entstehen den Betroffenen evtl. dadurch Folgerisiken, wie etwa die unrechtmäßige Weiterverarbeitung durch Auftragsverarbeiter oder nachgelagerte Hersteller und Diensteanbieter.

Mangelnde Aufklärbarkeit von Sicherheitsvorfällen
Fehlende Protokolldaten können dazu führen, dass IT-Sicherheitsvorfälle nicht erkannt oder deren Ursache und Ausmaß nicht angemessen untersucht werden können. Dadurch können die negativen Auswirkungen für die betroffenen Personen nicht angemessen behoben und abgemildert werden.

1.6.2 Risiken für eine Person, die durch Protokollieren bestehen

Unverhältnismäßige Protokollierung
Eine Protokollierung kann eine Steigerung von Risiken für Betroffene und Beschäftigte mit sich bringen,

wenn generell unangemessen viele, nicht auf zweckgemäße Erforderlichkeit und Richtigkeit überprüfte Protokolldaten zu lange und nicht ausreichend vor unbefugten Zugriffen geschützt gespeichert werden und die Auswertung von Protokolldaten nicht von Vornherein für bestimmte Zwecke definiert und der Zugriff auf diese Daten entsprechend beschränkt ist.

Offenlegung vertraulicher Daten
Abzuwägen ist bspw., ob aufgrund hoher Integritätsanforderungen an die zu löschenden oder verschlüsselt zu übermittelnden personenbezogenen Daten, diese Daten in Logs bzw. Protokollen explizit gespeichert werden sollten oder nicht. Eine Speicherung solcher Daten kann wiederum das Risiko einer unangemessenen Verringerung der Sicherung der Vertraulichkeit oder der Nichtverkettung dieser Daten vergrößern.

Verhaltens- und Leistungskontrolle
Risiken können ebenfalls entstehen, wenn die datenschutzrechtlich gebotene Überwachung nicht allein der fachlich gebotenen Verhaltenskontrolle, sondern einer darüberhinausgehenden allgemeinen, etwa auf psychische Dispositionen von Personen abstellende, Verhaltens- sowie Leistungskontrolle unterzogen wird.

Mangelnder Schutz vor Manipulation

Werden Protokolldaten nicht hinreichend vor unbefugten Manipulationen geschützt, ist ihre Aussagekraft und Verwertbarkeit fraglich. In diesem Fall können die Ziele der Protokollierung unterlaufen werden und eine Protokollierung eine falsche Sicherheit vermitteln.

2 Anforderungen

Die Anforderungen an die Protokollierung beziehen sich nachfolgend auf die Anforderungen an den Nachweis des zweckgemäßen Funktionierens der Sachbearbeitung sowie der dabei verwendeten IT-Komponenten und der Wirksamkeit von Schutzmaßnahmen für eine Verarbeitung. Die Protokollierung dokumentiert einen tatsächlich erfolgten Verarbeitungsvorgang.

Die während einer Verarbeitung erzeugten Protokolldaten können über verschiedene Systeme verteilt erzeugt und gespeichert werden; das beginnt bspw. mit den Logdaten auf Clients, kann über die Logdaten eines hauseigenen Routers bis zu den Servern von Rechenzentren bzw. Cloudinstanzen reichen. Eine Auswertung von Protokolldaten kann bspw. eine Teilmenge bei der Sachbearbeitung erfassen oder durch Vollzugriff auf alle Daten durch eine interne oder organisationsexterne Controllinginstanz erfolgen. Der Verantwortliche muss in der Lage sein und sicherstellen, dass derart räumlich über die Verarbeitungsebenen 2 („Fachapplikation“) und 3 („Infrastruktur“) sowie zeitlich über alle Phasen bzw. Vorgänge eines Verarbeitungsprozesses verteilt erzeugten und gespeicherten Protokolldaten, mit Bezug zu den Nachweisanforderungen einer Verarbeitung, entsprechend dem SDM-Würfel verfügbar sind und ausgewertet werden können. Soweit dies die weitere Verarbeitung von personenbezogenen Daten (z.B. Beschäftigtendaten) impliziert, muss sich die Auswertung nach dem ursprünglichen Erhebungszweck richten. Bspw. dürfen Protokolle zu Aktivitäten von Administrator*innen, die erhoben wurden, um prüfen zu können, ob diese ausschließlich die ihnen übertragenen Aufgaben durchgeführt haben, nicht verwendet werden, um eine Leistungskontrolle der Administrator*innen („Wie schnell wurde eine Aufgabe umgesetzt?“) durchzuführen.

2.1 Planen des „Protokollierens“

M43.21.01: Für die Protokollierung soll ein organisationsweites Protokollierungskonzept erstellt werden.

Die Erzeugung, Speicherung, Verarbeitung, Übermittlung und Löschung oder Archivierung von Protokolldaten müssen geregelt werden.

Ein datenschutzrechtlich orientiertes Protokollierungskonzept („PK“) soll zunächst seinen Geltungsbereich ausweisen. Das heißt, für welche Verarbeitung oder Verarbeitungen und für welche daran beteiligten IT-Systeme es gilt. Insbesondere muss das Konzept diejenigen Fälle bei der Erhebung, Speicherung, Nutzung und Löschung der Protokolldaten ansprechen, bei denen die gleichen Betriebsmittel von verschiedenen Verarbeitungen genutzt werden (typisch: Router, Dienste bzw. Server) und für die dann die verarbeitungsspezifischen Regelungen bzgl. Aufbewahrungs- und Löschfristen auszuweisen sind.

Das PK soll den allgemeinen Zweck der Protokollierung getrennt für Verarbeitungen ausweisen. Die Dokumentation zu einer verarbeitungsspezifischen Protokollierung muss die Rechtsgrundlagen für die Protokollierung ausweisen.

Das PK muss Zuordnungen von Hardware und IT-Komponenten zu Verarbeitungen aufweisen, um für die Verarbeitungen die Teilmenge der für sie relevanten Protokolldaten der IT-Komponenten, die als Betriebsmittel der Verarbeitung gelten, bestimmen zu können.

Für jede Verarbeitung muss festgelegt werden, welche Ereignisse protokolliert werden sollen, welche Maßnahmen zur Sicherstellung der datenschutzrechtlichen Anforderungen getroffen werden müssen, welche allgemein gültigen Zugriffs-, Übermittlungs- und Auswertungsregelungen auf diese Daten bestehen, in welcher Form die Auswertung von Protokolldaten protokolliert und dokumentiert werden und welche Maßnahmen bei Auffälligkeiten - wie bspw. Protokollierungslücken, rechtlich wahrscheinlich die Organisation oder betroffene Personen belastende Protokolldaten oder bei Hinweisen auf technische Fehlfunktionen – ergriffen werden müssen. Sie müssen ausreichend detailliert sein, um den Vorgang eindeutig zuzuordnen und eine zeitnahe Auswertung zu ermöglichen.

Es muss festgelegt werden, was als eine Entität oder ein Objekt – das können Organisationen, Verarbeitungen, IT-Systeme oder auch Betriebsmittel sein – und was als „Schnittstelle“ zwischen diesen Einheiten gilt. Aktivitäten sind zumindest an solchen Schnittstellen zu protokollieren, bei denen ein Übergang zwischen den Entitäten mit unterschiedlichen Rechtsgrundlagen, unterschiedlichen Verarbeitungen oder Zwecken und formal ein Erheben/Sammeln, eine Übermittlung oder ein Abruf vorliegen. Dies gilt in besonders augenscheinlichen Maße, wenn Daten eine Organisation über Router oder Firewalls bzw. an Services mit Kontakt zum Internet erreichen oder verlassen. Deshalb muss festgelegt werden, welche Teilmengen aus den Protokoll- bzw. Logdaten bspw. beteiligter IT-Komponenten bzw. Betriebsmittel für verarbeitungsspezifische Auswertungen relevant sind. Wenn bspw. Daten über einen USB-Port eines Arbeits-PC begründet abrufbar sein müssen, kann es erforderlich sein, zumindest die Tatsache, dass der Port für eine bestimmte Zeit benutzt wurde, zu protokollieren.

Das PK muss ausweisen, ob und wie Betroffenenrechte auf Auskünfte aus dem Protokolldatenbestand, wenn sie nach Art. 15 DS-GVO möglicherweise ebenfalls zu beauskunften sind, real erfüllt werden können und wie die Information der Beschäftigten über das Ausmaß der Kontrolle ihrer Arbeit sichergestellt und dabei Leistungskontrollen vermieden und das Maß für rechtlich gebotene Verhaltenskontrollen eingehalten werden.

Das Protokollierungskonzept muss, mit Bezug zur Verarbeitung, folgende Anforderungen verbindlich regeln:

1. welche Eigenschaften einer Aktivität, sei es die einer Sachbearbeitung oder die einer IT-Komponenten sollen in welcher Phase und auf welcher Ebene bzgl. welcher Anforderung protokolliert werden;
2. wo diese Protokolldaten gespeichert werden sollen;
3. welches Format die Protokolldaten aufweisen und welche Auswertungstools dafür bereitgehalten werden sollen;
4. zu welchen Zwecken diese Protokolldaten erhoben, gespeichert und ausgewertet werden dürfen,
5. idealerweise: zu welchen Fragestellungen die Protokolldaten mit welchen Mitteln ausgewertet werden sollen;
6. ob und in welcher Form ggfs. auf Protokolldaten aus anderen Zwecken als denen der Verarbeitung heraus zugegriffen werden darf (unter Ausweis der Rechtsgrundlage);
7. wann und wie Protokolldaten gelöscht oder archiviert werden sollen, wenn der Zugriff auf diese nicht mehr, insbesondere aus Sicht betroffener Personen, erforderlich ist und diese aus der Produktion zu nehmen sind.

Die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO gelten auch für Protokolldateien. So ist darauf zu achten, dass der Zweck der Protokollierung angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist (Datenminimierung). Im Regelfall soll daher auf eine Speicherung von Personen- und Inhaltsdaten im Protokolldatenbestand verzichtet werden. Es müssen die Fälle, in denen der Personenbezug im Protokolldatenbestand erforderlich ist, begründet bzw. gerechtfertigt sein. Vorgesetzte müssen die Aktivitäten der Sachbearbeitung prüfen können, der Verantwortliche muss die Controlling-Aktivitäten von Vorgesetzten prüfen können (lassen).

Wenn die Protokollierung einer Verarbeitung ihrerseits als eine Verarbeitung gestaltet ist, die mehrere Zwecke umfassen kann, dann muss das Konzept auch die Rechtsgrundlage der Protokollierung ausweisen.

Das PK muss die Auswertungsverfahren, mit denen die Protokolldaten verarbeitet werden, benennen bzw. dokumentieren.

Das PK soll das Testverfahren zum Nachweis des ordnungsgemäßen Funktionierens der Protokollierungen der Verarbeitungen und deren Betriebsmittel dokumentieren (siehe Kap. 2.4 zur Evaluierung).

Das PK sollte außerdem festlegen, wie das Protokollierungskonzept fortgeschrieben wird. Bei der Erstellung und Fortschreibung des PK soll es auf alle nachfolgend hier aufgeführten Anforderungen und Maßnahmen Bezug nehmen, mit dem Zweck, Expert*innen in die Lage zu versetzen, die datenschutzrechtlich begründete Protokollierung einer Verarbeitung mit ihren Prozessen und Komponenten implementieren, prüfen und gebotene Veränderungen veranlassen zu können.

M43.21.02: Die Protokoll- bzw. Logdaten der Protokollierung sollen inventarisiert werden.

Der Verantwortliche soll erfassen, welche Protokoll- und Logdaten von den eingesetzten Systemen und Diensten erzeugt werden, von welchen Instanzen diese zu welchen Zwecken gespeichert und genutzt werden, und wann diese gelöscht werden. Dies gilt sowohl für die Daten der unmittelbar verwendeten lokalen IT als ggfs. auch der verfahrensbezogenen externen IT bei Dienstleistern.

Jedes Protokolldatum muss einer Verarbeitung, mit einem entsprechenden Zweck und einer Rechtsgrundlage sowie den Anforderungen, die zu erfüllen sind, zugeordnet werden können.

Protokolleinträge sollen es ermöglichen, dass die Aktivitäten der Betriebsmittel und Personen in Beziehung zur Verarbeitung und den Organisationsplänen, Geschäftsverteilungsplänen und Berechtigungs- und Rollenkonzepten gesetzt werden können.

M43.21.03: Für die Protokollierung personenbezogener Daten muss die Rechtsgrundlage bestimmt werden.

Für die Verarbeitung ist festzulegen, welche Protokolldatenbestandteile a) von der Rechtsgrundlage für die Verarbeitung, b) von einer etwaigen spezialrechtlichen Rechtsgrundlage, die die Protokollierung erfordert, oder c) von einer Rechtsgrundlage zu anderen Zwecken als denen der Verarbeitung abgedeckt werden.

M43.21.04: Für die Protokollierung muss die Struktur der Protokolldaten festgelegt sein.

Jedes Protokoll muss Daten enthalten, mit denen folgende Fragen beantwortet werden können:

1. Zeit: Wann hat ein bestimmtes Ereignis von einer bestimmten Entität stattgefunden (Wann)?
2. Aktivität: Welches Ereignis hat zu einem bestimmten Zeitpunkt mit der Beteiligung einer bestimmten Entität stattgefunden (Was)?
3. Instanz: Welche Entität (BM, Administrator, Mitarbeiter) hat zu einem bestimmten Zeitpunkt ein bestimmtes Ereignis ausgelöst oder welche Entität war zu einem bestimmten Zeitpunkt mit einem bestimmten Ereignis befasst (Wer)?

Es muss für eine Protokollierung und deren Auswertung außerdem eindeutig festgelegt sein, welche Instanz diese Daten zentral sammelt und von welcher Instanz aus diese Daten ausgewertet werden. 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, wenn sich dies nicht bereits aus dem Kontext der Protokollierung eindeutig ableiten lässt.

Die Zeitkomponente muss es ermöglichen, Ereignisse kausal zusammenhängender Systemaktivitäten über Programmteile, Server-, Dienst- oder Abteilungs- und Organisationsgrenzen hinweg als zusammenhängende Abläufe nachvollziehen zu können. Dies erfordert bei automatisiertem Protokollieren gesichert verlässliche Zeitstempel der ausgelösten Ereignisse in Logdateien sämtlicher beteiligter Systeme. Die Zeitstempel sollen 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.

Die Aktivitätskomponente muss es ermöglichen, die Art und die Qualität der Ausführung einer Instanz prüfen zu können.

Die Instanzkomponente, die als „Quelle einer Aktion“ 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.

M43.21.05: Die Protokolldaten sollen hinsichtlich Inhalts und Formats standardisiert sein.

Die Inhalte der Protokolldaten und die Formate sollen standardisiert sein. Dies erleichtert die (Automatisierung der) Auswertung von Protokolldaten zum Zweck der Erhöhung der Verfügbarkeit, der Integrität und der zweckbestimmten Auswertung von Protokolldaten.

Der Zeitstempel, der Bezeichner für Instanzen, deren Aktivitäten protokolliert werden und die Bezeichnungen der Aktivitäten dieser Instanzen sollten die Verarbeitungen übergreifend standardisiert werden.

Die Protokolldaten sollen in einem strukturierten, gängigen, maschinenlesbaren und maschinenauswertbaren Format (z.B. JSON, CSV) vorliegen oder in ein solches exportierbar sein.

M43.21.06: Für die Protokollierung müssen Maßnahmen zur Gewährleistung der Sicherheit getroffen sein.

Für das Erheben, Speichern, Nutzen und Löschen von Protokolldaten müssen IT-Sicherheitsmaßnahmen getroffen werden, um dabei technisch ihre Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten:

Protokolldaten sollen nach ihrer Erstellung nicht mehr geändert werden können. Dies kann durch den Einsatz von WORM-Speichern (Write Once, Read Many) oder durch digitale Signaturen/Signieren erreicht werden, die eine nachträgliche Änderung erkennen lassen.

Protokolldaten sollten verschlüsselt gespeichert werden. Nur autorisierte Personen sollen Zugriff auf die Protokolldaten haben, was durch Zugriffskontrollmechanismen erreicht werden kann, die den Zugang auf Basis von Rollen und Berechtigungen regeln.

Protokolldaten sollten nicht auf Produktivsystemen, sondern auf speziell dafür vorgesehenen, zugriffsbeschränkten zentralen Protokollservern gespeichert werden, die in Echtzeit über ein sicheres Protokoll auf den oder die Protokollserver übertragen werden. Wenn Protokolle dagegen sowohl lokal, etwa auf einem Client mit der Anwendung, oder auf einem Server, der einen Dienst bereitstellt, sowie zusätzlich auf einem Protokollserver gespeichert werden, der sich außerhalb der Kontrolle der regulären Systemadministratoren befindet, ermöglicht dies Vergleiche zwischen Protokolldaten und hilft, verdächtige Aktivitäten zu erkennen.

Zugriffe auf Protokolldaten sollen ebenfalls protokolliert werden. Protokolldaten müssen regelmäßig überprüft und ausgewertet werden, um die Einhaltung der rechtlichen Anforderungen sicherzustellen. Protokolldaten müssen nach Ablauf der gesetzlichen begründeten Aufbewahrungsfristen sicher gelöscht werden.

Die Auswertungsinstanz (Hardware und Software), mit der Protokolldaten ausgewertet und Berichte erstellt werden, soll gesichert betrieben werden und vor unbefugten Zugriffen und Manipulationen – insbesondere durch die Administration der an einer Protokollierung beteiligten Betriebsmittel – geschützt werden.

M43.21.07: Die Protokollierung soll für die Tätigkeiten der Administration sachgerecht gestaltet sein.

Die administrative Protokollierung umfasst die Aktivitäten der Administrierenden, die Hardware und Software installieren und die deren Betrieb, Konfigurationen und die Kontroll- bzw. Prüfmöglichkeiten sicherstellen.

Die Aktivitäten einer Administratorin oder eines Administrators an einer IT-Komponenten bzw. einem Betriebsmittel einer Verarbeitung müssen vollständig und in hinreichender Auflösung protokolliert werden.

Es zählt grundsätzlich zu den Aufgaben von Administrierenden im Sinne der auf sie zugeschnittenen Sacharbeit, die Protokollierung von Betriebsmitteln den Anforderungen entsprechend zu konfigurieren und deren Auswertbarkeit sicherzustellen.

Die Administration 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.

Es muss festgelegt werden, welche Aktivitäten bei der Administration von IT-Systemen zu protokollieren sind:

- Systemgenerierung und Modifikation von Systemparametern,
- Verwaltung von Benutzenden (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 soll im Protokollierungskonzept erfasst sein, die eine Prüfbarkeit der folgenden Aktivitäten erlaubt:

- 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 Speicherbereichen,
- des Anlegens, Änderns, Sperrens und Löschens von Nutzenden und Nutzendengruppen, 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.

Im Falle der Möglichkeit zur Kenntnisnahme personenbezogener Daten, die zur Kenntnis zu nehmen Administrierende grundsätzlich nicht befugt sind, soll die Protokollierung von Administrationsaktivitäten bei einer Verarbeitung, von der nur ein normales Risiko für Betroffene ausgeht, trotzdem hohen Anforderungen genügen („revisionsfeste Protokollierung“), um zumindest im Nachhinein durch das Controlling bspw. des Fachverantwortlichen oder des/der DSB bzw. letztlich des Verantwortlichen zweifelfrei Verstöße der Vertraulichkeit und Zweckbindung der Nutzung technischer Mittel auf Seiten der Administration feststellen zu können.

Es muss sichergestellt sein, dass der Bezug zwischen der administrativen Protokollierung und der Sachbearbeitung ohne besonderen Aufwand hergestellt werden kann, damit nicht-fachlich begründete Aktivitäten der Administration zweifelsfrei erkennbar werden.

M43.21.08: Der Umfang der Protokolldaten soll gut begründet festgelegt sein.

Der Nachweis der Aktivitäten des regelkonformen Arbeitens von Mitarbeitern und Vorgesetzten kann in der Regel anhand von **Akten** oder **Berichten** erfolgen. Eine darüberhinausgehende automatisch erfolgende Protokollierung kann sich darauf beschränken, Daten von Aktivitäten an Schnittstellen zu anderen Systemen oder Verarbeitungen oder auch Räumlichkeiten zu speichern.

Bei den Aktivitäten sowohl der Sachbearbeitung im Fachprogramm als auch der Aktivitäten der technischen Administration muss jeweils geprüft werden, welche der folgenden Aktivitäten zu protokollieren sind:

    - 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 muss festgelegt werden, 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). Protokolldaten müssen spätestens zum Zeitpunkt der Auswertung einem konkreten Vorgang zugeordnet werden können (bspw. über ein Akten- oder Vorgangszeichen).

Eine Historie kann Teile einer Funktion der Protokollierung erfüllen, verfolgt aber einen anderen Zweck und ist, anders als eine Protokollierung für den Nutzer zugänglich. Mit ihrer Hilfe kann über einen längeren Zeitraum hinweg jede einzelne Änderung rückgängig gemacht werden.

Die fachliche Protokollierung des Controllings muss es erlauben festzustellen, welche Controlling-Aktivitäten anhand von Auswertungen von Protokolldaten insbesondere durch Vorgesetzte von Adminstrator*innen und Sachbearbeiter*innen tatsächlich stattgefunden haben. Die Aktivitäten eines reinen Controllings im Sinne des Prüfens von Soll- mit Ist-Werten besteht typischerweise nur im Lesen dieser Daten, weshalb dann auch nur dieser Vorgang zu protokollieren ist.

M43.21.09: Für die Protokolldaten müssen die Aufbewahrungsfrist und die Löschung festgelegt sein.

Es muss geregelt sein, was mit Protokolldaten, die verarbeitet wurden und nicht mehr erforderlich sind, geschehen soll. Für Protokolldatenbestände müssen Löschfristen festgelegt werden, wenn personenbezogene Daten enthalten sind. In der Regel sind mindestens 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. Wenn dasselbe Protokolldatum von einer weiteren

Verarbeitung genutzt wird, muss eine rechtliche Abwägung getroffen werden, ob das rechtliche Interesse an der Löschung aus der einen Verarbeitung oder das Interesse an der Fortsetzung der Speicherung aus der anderen Verarbeitung überwiegt. Solche Konflikte geben dann den Anlass, Protokolldatenbestände einzelverarbeitungsorientiert getrennt zu führen und ggfs. Redundanzen der Datenbestände in Kauf zu nehmen, so dass ein verarbeitungsorientiertes Löschen von Daten nach Entfallen der Erforderlichkeit ihrer weiteren Speicherung wirksam umgesetzt werden kann.

Um bspw. zu vermeiden, dass im Protokolleintrag die Namen gelöschter Personendaten zum integren Nachweis, dass genau diese Daten gelöscht wurden, gespeichert werden, kann ein Quittierungsmechanismus eingerichtet werden. Das kann konkret heißen: Im 4-Augen-Prinzip wird gesichert nachweisbar quittiert, dass bestimmte personenbezogene Daten aus den Produktionsdatenbestand der Verarbeitung gelöscht wurden; diese Quittung ersetzt dann den ansonsten notwendigen Protokolleintrag.

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. Entweder sind Protokolldaten zu löschen oder der Archivierung zuzuführen, d.h. aus der Produktion herauszunehmen und nach den Regeln und Vorgaben des Archivrechts zu behandeln. Aus den Protokolldaten zum Löschen muss hervorgehen, welches Datum mit welchem Programm in welcher Qualität gelöscht wurde (bei einer Datei bspw. mit einem einfachen Lösch-Befehl, oder mit einem zertifizierten wipe-Programm oder durch Zerstören des Mediums, auf dem die Datei gespeichert ist) und ob eine befugte und kompetente Instanz das Löschen ausgelöst hat.

M43.21.10: Für die Protokolldaten sollen die Auswertungstools und Formate der Ausgaben festgelegt sein.

Um die Nutzung der Protokolldaten zu spezifizierten Prüfzwecken zu erleichtern, soll die Aufbereitung von Protokolldaten konzipiert und mit entsprechenden Auswertetools hinterlegt sein:

- Filterung: Protokolldaten werden so gefiltert, dass unnötige Protokollmeldungen aussortiert werden.
- Normalisierung: Protokolldaten werden in ein einheitliches Datenformat standardisiert.
- Aggregation: Protokolldaten identischen Inhalts werden zusammengefasst.
- Kategorisierung: Protokollmeldungen werden nach Systemen, Aktivitäten oder nach Risikobereichen kategorisiert.
- Priorisierung: Die Ausgabe von Protokollmeldungen kann dynamisch nach Relevanz priorisiert werden.

Beispiele für weitere aufbereitete Ausgaben von Protokolldaten in Berichten und Reports 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?),
- Analysen mit Hilfe von KI-Prompts.

Das Monitoring ist ein Spezialfall, wenn aktuelle Aktivitäten und Ereignissen definierter Entitäten beobachtet werden müssen und in der Gegenwart Entscheidungen zu treffen sind. So sind insbesondere diejenigen Fälle zu betrachten, in denen auf Fehlfunktionen in einer Verarbeitung unmittelbar reagiert

und Alarm ausgelöst werden muss. Zusätzlich kann es auch geboten sein, einen Prozess zu stoppen, bis eine Fehlfunktion behoben oder ein Problem gelöst wurde.

2.2 Technisch-organisatorisches Umsetzen der Protokollierung in den Phasen

M43.22.01: Die Protokollierung muss die Aktivitäten an Schnittstellen umfassen.

Daten, die im Rahmen einer Verarbeitung erhoben werden, weil sie bspw. eingegeben, zugeschickt oder (automatisiert) abgerufen wurden, müssen protokolliert werden. Es muss der Zeitpunkt des Eintreffens/ Erhebens bzw. Verlassens, die absendende/empfangene Instanz und die Eigenschaften bzgl. der Sicherung des Transports der Nachrichten (wie Verschlüsselung) anhand von Protokolldaten prüfbar sein.

An den Schnittstellen von Routern und Sicherheitsgateways sollen die folgenden Aspekte beachtet werden:

- 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 soll 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 Risiko sollten geeignete Maßnahmen, wie bspw. die automatische Blockierung sämtlichen Verkehrs, zur Verfügung stehen und ggfs. getroffen werden können, wenn die Schnittstellenprotokollierung des Datenstroms nicht gesichert erfolgen kann.
- Ereignisse wie unzulässige Verbindungsversuche oder der Aufruf unsicherer Routinen für ungesicherte Kommunikationsverbindungen sollen im Protokolldatenbestand hervorgehoben werden. Sie sollten zu einer unverzüglichen Warnung der Administration 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). 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.

Für die Auswertung dieser Daten muss, durch Zusammenarbeit der thematisch-fachlichen („Sachbearbeitung“) und der technisch-fachlichen („Technikadministration“) Ebene einer Organisation, sichergestellt sein, dass prüfbar ist, ob für die Übermittlung/ den Abruf/ das Erheben dieser technischen Daten eine Rechtsgrundlage bestand und ob die vereinbarten Schutzmaßnahmen für den Transport – wie bspw. die Authentisierung beteiligter Systeme, und die Verschlüsselung der transportierten Inhalte auch gegenüber dem Transporteur – der Daten eingehalten wurden. Die Ebene der Sachbearbeitung befasst sich insofern mit der rechtlich-sachlichen Begründung der Übermittlung der Daten, die Ebene der Technikadminstration mit der technisch-sachlichen Beschreibung, wie die Daten technisch in das System gelangen.

M43.22.02: Die Protokollierung muss die Aktivitäten von Systemen und Diensten umfassen.

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 muss festgelegt werden, welche der folgenden IT-Komponenten bzw. welcher der von ihnen erbrachten Dienste anhand von Protokollen bzw. Logdaten überprüfbar gemacht werden müssen:

- Applikationen (Fachanwendungen),
- Datenbanken,
- Dienste (wie Webserver, Mailserver, Fileserver),
- KI-Systeme,
- 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 sollen 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).

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.

M43.22.03: Die Protokollierung muss die Aktivitäten von Schutzmaßnahmen umfassen.

Die technische Protokollierung („Logdaten“) muss die Kontrolle und Prüfung der Funktionen aller IT-Komponenten/Betriebsmitteln nach Maßgabe der Anforderungen an das Verfahren erlauben.

Wenn personenbezogene Daten zur Umsetzung der Gewährleistungsziele verarbeitet werden (bspw. bei Datensicherungen, Entschlüsselung, Integritäts- und Authentizitätsprüfungen), so müssen die relevanten Aktivitäten der eingesetzten Schutzprogramme bzw. Betriebsmittel protokolliert werden.

Die Logdateien oder Einträge in einer Logdaten-Datenbank müssen eine Prüfung ermöglichen, ob geforderte Schutzmaßnahmen implementiert und deren Funktionalitäten grundsätzlich prüfbar zugänglich sind.

Die Inhalte von Logdateien (Logdaten) müssen eine Prüfung erlauben, ob eine Schutzmaßnahme anhand von verarbeitungsrelevanten Soll-Vorgaben und Ist-Feststellungen im richtigen Maße funktioniert und für eine funktionale und rechtliche Beurteilung zugänglich ist.

M43.22.04: Die Protokollierung muss die Zugänge und Zugriffe von Mitarbeiter*innen umfassen.

Personenbeziehbarkeit über Protokollierung herzustellen ist unabdingbar, um den Nachweis der Authentisierung eines/einer Beschäftigten für den Zugang zur Organisation und der Autorisierung für den Zugriff auf eine Verarbeitung mit all ihren Daten und Betriebsmitteln erbringen zu können. Die Bandbreite an Protokolldaten kann von ausgefüllten Formularen an der Pforte der Zugänge von Grundstücken oder

Gebäude(teilen) bis zu den Logdaten nach Abfragen von Nutzernamen, Passworten sowie ggfs. Authentisierungstoken reichen.

M43.22.05: Die Protokollierung soll für die Tätigkeiten der fachlichen Sachbearbeitung sachgerecht gestaltet sein.

Die fachliche Protokollierung der Sachbearbeitung muss es erlauben, den Nachweis der gesetzlichen Ordnungsmäßigkeit bzw. der Vertragskonformität des fachlichen Handels zu erbringen. Deshalb müssen die Inhalte der Aktenführung und Regeln zu deren Bearbeitung festgelegt werden.

Die fachliche Protokollierung muss die (relevanten) Aktivitäten der Sachbearbeitung bzw. der Organisation elektronisch oder in Papierform in Akten, Berichten oder von Hand erfassten Protokollmitschriften dokumentieren.

Akten, Berichte, Protokolle auf der Ebene der Sachbearbeitung müssen vor unbefugtem Zugriff und fehlerhaften Änderungen geschützt werden, zweckändernde Nutzungen müssen erkennbar sein, Möglichkeiten zur Kommentierung bzw. Annotation bestehen und Fristen für Löschung oder zur Übergabe ans Archiv festgelegt und deren Ausführungen nachweisbar sein. Diese Umsetzung dieser Schutzmaßnahmen muss befugten Controlling-Instanzen zugänglich sein.

Die fachliche Protokollierung Sachbearbeitung soll bei einem Einsatz von IT - also Hardware sowie Betriebsmitteln wie Fachapplikationen, Textverarbeitungen, Tabellenkalkulationen oder Datenbanken, Mailprogramme und Webbrowser sowie insbesondere der elektronischen Akte – die automatisch angelegten Logdateien und Ablauf-Aufzeichnungen („Histories“) mit vollautomatisch generierten Logdaten aus den verwendeten Fachprogrammen und Betriebsmitteln umfassen.

Diese Daten können sowohl in den Nutzdateien (bspw. die Dateien einer Textverarbeitung) oder auch als eigenständige Logdaten in Dateien oder Datenbank gespeichert sein.

Um zu prüfen, ob das Protokollieren aussagekräftig ist, soll 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.

M43.22.06: Für die Protokollierung muss ein Prozess zur Klärung festgelegt sein, falls Zweifel an der Richtigkeit und Vollständigkeit der Protokolldaten bestehen.

Es muss eine Regelung getroffen werden für solche Fälle, in denen Protokolldaten in Zweifel gezogen werden. Hierfür muss das Annotierenkönnen von Protokolldaten mit integrem Bezug zu diesen Daten sichergestellt werden.

2.3 Skalieren der Protokollierung für hohes Risiko

Um den Anforderungen an Transparenz einer Verarbeitungstätigkeit auch bei hohem Risiko gerecht zu werden, müssen erhöhte Anforderungen an die Qualität insbesondere der Prüfbarkeit der Verarbeitung (Transparenz), der Revisionsfestigkeit (Integrität) und des Beweiswerts sowie der Sicherung der Vertraulichkeit und eine nur zweckbestimmte Auswertung der Protokolldaten berücksichtigt werden. Bei der Protokollierung müssen die Interessen an der Nachweisbarkeit nicht nur des Verantwortlichen, 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 sowie gelöscht werden. Eine generelle Strategie zur Umsetzung von technischen und organisatorischen

Maßnahmen bei hohem Risiko besteht darin, die Maßnahmen der verschiedenen Gewährleistungsziele auch auf die Schutzmaßnahmen selber anzuwenden.

An besonders kritischen Schnittstellen oder in besonders sensiblen Verarbeitungen soll ein Monitoring erfolgen, das in Echtzeit Schnittstellen und Verarbeitungen überwacht und bei Abweichungen oder Auffälligkeiten Alarme an festgelegte Personen auslöst und ggf. automatisiert Datenübertragungen oder andere Verarbeitungen blockiert. Es kann ein Datum zum Anzeigen der Dringlichkeitsstufe ergänzt werden, wenn ein Datum bspw. den Bereich der für den Abruf oder die Verarbeitung gültigen Rechtsgrundlage wechselt.

M43.23.01: Die Protokollierung soll in Form einer Vollprotokollierung gestaltet werden.

Ein hohes Risiko 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.

„Vollprotokollierung“ bezeichnet – im Unterschied zur anlassbezogenen- oder Stichproben-Protokollierung, bei der nur ausgewählte Vorgänge aufgezeichnet werden -, die lückenlose und vollständige Aufzeichnung sämtlicher Aktivitäten, die im Rahmen der Verarbeitung personenbezogener Daten stattfinden. Dabei wird jede einzelne Aktion – wie Zugriffe, Änderungen, Löschungen oder Weitergaben – durch an der Verarbeitung beteiligten Instanzen (z.B. Systeme, Personen oder Organisationseinheiten) erfasst.

M43.23.02: Die Protokolldaten sollen eine hohe Verfügbarkeit aufweisen.

Die Verfügbarkeit von Protokolldaten betrifft zum einen die Verfügbarkeit vorhandener Protokolldaten für eine Auswertung und zum anderen die Sicherstellung, dass für jede zu protokollierende Aktivität ein ansprechendes Protokoll erstellt wird. Das kann bedeuten, dass eine Funktion eines Programms nur dann ausgeführt wird, wenn zuvor sichergestellt wurde, dass hinreichend Speicherplatz für das Protokollieren dieser Funktion bereitsteht.

M43.23.03: Die Protokolldaten sollen durch Prüfsummen abgesichert werden.

Die Protokollierung soll im Kryptokonzept erfasst werden zum Zweck, dass jedes Protokolldatum von einer Prüfsumme erfasst ist und somit Änderungen an dem Datum sichtbar werden.

M43.23.04: Die Protokolldaten sollen zertifizierte Zeitstempel und Zeitsynchronisation aufweisen.

Protokolldaten sollen mit einem zertifizierten Zeitstempel versehen sein. Es muss automatisch eine Zeitsynronisation zwischen allen beteiligten Instanzen einer Verarbeitung stattfinden.

M43.23.05: Die Protokolldaten sollen verschlüsselt transportiert und gespeichert werden.

M43.23.06: Die Protokollierung soll auch für die Administration die Unveränderbarkeit von Protokolldaten zu eigenen Aktivitäten gewährleisten.

Bei der Protokollierung administrativer Aktivitäten soll die Protokollierung so ausgestaltet sein, dass Administratoren die eigenen Aktivitäten in den aufgezeichneten Protokolldaten nicht manipulieren können. Sofern dies nicht bereits durch technische Mittel gänzlich ausgeschlossen werden kann, sollen geeignete technische Maßnahmen zur Kontrolle, wie beispielsweise Screencasts während administrativen Tätigkeiten, eingerichtet werden. Die Auswertung der administrativen Protokolldaten ist festzulegen, beispielsweise durch regelmäßige Stichprobenkontrollen.

M43.23.07: Die Protokollierung soll auf einem zentralen Protokollserver betrieben werden.

Zur Speicherung aller Protokoll- und Logdaten soll ein dedizierter Protokollserver betrieben werden, für dessen Implementation, Konfiguration und Betrieb wiederum technische und organisatorische Maßnahmen anhand aller Gewährleistungsziele zu treffen sind. Insbesondere sind Protokolldaten beim Transfer von Produktivsystemen auf andere Computer, wie bspw. einen Protokollserver, gegen unbefugte Kenntnisnahmen und Änderungen zu schützen. Das Protokollkonzept muss eine Protokollstrategie und entsprechende Protokollierungsarchitektur ausweisen.

2.4 Evaluierung der Eigenschaften der Protokollierung

Das Testkonzept für die Protokollierung sollte die Planung/Vorbereitung, den Testumfang, die Testmethode, die Testdurchführung, die Auswertung und Dokumentation sowie die Nachbereitung regeln.

Hierbei muss beachtet werden, dass erhobene Testdaten in einem geschützten Bereich gespeichert werden. Anhand von Prüffragen und ggfs. Prüftools müssen dann Testfälle erzeugt werden, die a) die automatisierten Prozesse zum Speichern und ggfs. zum Übertragen von Protokollierungsdaten zum zentralen Protokollierungsserver sowie zu Integritätschecks und zum Verschlüsseln sowie b) die Tests auf die speziellen Nachweisanforderungen der Verarbeitung entsprechend des festgelegten Testumfangs zum Gegenstand haben.

Wenn die Auswertung von Testläufen bzgl. Protokollierung mit Hilfe besonderer Auswertungsverfahren durchgeführt werden, wie bspw. mit Hilfe einer künstlichen Intelligenz, dann muss auch hier die DS-GVO-Konformität eingehalten werden und insbesondere die Nachprüfbarkeit der Integrität der Ergebnisse mit Bezug auf die Rohprotokolldaten sichergestellt sein.

M43.24.01: Für die Protokollierung soll ein Testkonzept erstellt werden.

Es sollen Protokolldaten über verschiedene Ebenen der Verarbeitungstätigkeiten hinweg und entlang der aufeinanderfolgenden Verarbeitungsprozesse geprüft werden zwecks Sicherstellung der Zweckbindung über den gesamten Verarbeitungsprozess hinweg.

Planung und Vorbereitung

1. Formulierung von Fragestellungen aus Usecases und Testfällen („Prüffragen“), mit denen anhand von Protokolldaten a) der Nachweis des ordnungsgemäßen Funktionierens erfolgen kann sowie b) Antworten auf Ausnahmefälle gefunden werden können.
2. Prüfen, ob Auswertungstools für Protokolldatenauswertungen bereitstehen, einschließlich administrativen Sachverstands zur Nutzung von Auswertungstools.
3. Sichergestellt werden muss, dass die Testaktivitäten protokolliert werden.

Testumfang

1. Festlegung, ob eine Protokollierung auf einem einzelnen IT-System, auf den IT-Systemen einer Ebene oder über die IT-Systeme aller beteiligten Ebenen und der dabei genutzten Dienste und Betriebsmittel hinweg für die festgelegten Usecases getestet werden soll, mit Erstellung entsprechender Prüffragen.
2. Festlegung, ob die Protokollierung für alle Phasen der Erhebung, Speicherung, Nutzung und Übermittlung sowie der Löschung von personenbezogenen Daten getestet werden soll, mit Erstellung entsprechender Prüffragen.
3. Festlegung, ob alle Anforderungen gemäß den sieben Gewährleistungszielen getestet werden sollen, mit Erstellung entsprechender Prüffragen.
4. Ermittlung der Konfigurationen der Protokollierung der am Test beteiligten IT-Systeme.

Testmethode

1. Dokumentenprüfung: Erheben von Testdaten anhand der Dokumentation zur Protokollierung gemäß vorbereiteter Prüffragen.
2. Vor-Ort-Prüfung: Erheben von Testdaten mit Hilfe von Auswertungstools für Protokolldaten anhand vorbereiteter Prüffragen.

M43.24.02: Für die Protokollierung soll die Auswertung, Dokumentation und Nachbereitung von Tests festgelegt sein.

1. Erstellung eines Prüfberichts mit den Ergebnissen der Dokumentenprüfung und Vor-Ort-Prüfung.
2. Bewertung der Testergebnisse, ob die Protokolldaten den Nachweis der Ordnungsmäßigkeit der Durchführung der Verarbeitung letztlich mit Bezug zur DS-GVO erfüllen.
3. Dokumentation von Abweichungen und Empfehlungen zur Verbesserung der Protokollierung.

Die Überprüfung muss verstetigt werden. Das bedeutet:

1. Regelmäßige Überprüfung und Aktualisierung des Testkonzepts basierend auf Änderungen der Verarbeitungen sowie der IT-Infrastruktur mit neuen Anforderungen.
2. Planung und Durchführung von Folgetests zur Überprüfung der Umsetzung von Verbesserungsmaßnahmen bzgl. der Protokollierung.

3 Referenzen

BSI 2023: Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen, V2.0: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_2_0.pdf?__blob=publicationFile&v=3

BSI 2023: OPS.1.1.5 Protokollierung https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_5_Protokollierung_Edition_2023.pdf?__blob=publicationFile&v=3

BSI 2022: Prüfschema für die Erteilung eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz, V2.0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Testat/Pruefschema.pdf?__blob=publicationFile&v=2

4 Zusammenfassung der Maßnahmen

4.1 Planen des Protokollierens

Nr.	Maßnahme	ersetzt Maßnahme in V1.0	Gültigkeit
M43.21.01	Für die Protokollierung soll ein Protokollierungskonzept erstellt werden.	M43.P01, M43.P05, M43.P09	V1.0/ V2.0
M43.21.02	Die Protokoll- bzw. Logdaten der Protokollierung sollen inventarisiert werden.	M43.D08, M43.D11	V1.0/ V2.0
M43.21.03	Für die Protokollierung personenbezogener Daten muss die Rechtsgrundlage bestimmt werden.		V2.0

M43.21.04	Für die Protokollierung muss die Struktur der Protokolldaten festgelegt sein.	M43.D01, M43.D02, M43.D03, M43.D04	V1.0/ V2.0
M43.21.05	Die Protokolldaten sollen hinsichtlich Inhalts und Formats standardisiert sein.	M43.D17	V1.0/ V2.0
M43.21.06	Für die Verarbeitung durch die Protokollierung müssen Maßnahmen zur Gewährleistung der Sicherheit getroffen sein.	M43.D07	V1.0/ V2.0
M43.21.07	Die Protokollierung soll für die Tätigkeiten der Administration sachgerecht gestaltet sein.	M43.D09	V1.0/ V2.0
M43.21.08	Der Umfang der Protokolldaten soll gut begründet festgelegt sein.	M43.S01	V1.0/ V2.0
M43.21.09	Für die Protokolldaten müssen die Aufbewahrungsfrist und die Löschung festgelegt sein.	M43.D05	V1.0/ V2.0
M43.21.10	Für die Protokolldaten sollen die Auswertungstools und Formate der Ausgaben festgelegt sein.	M43.D12, M43.D13, M43.D14, M43.D15, M43.D16, M43.D18, M43.P04, M43.S02	V1.0/ V2.0

4.2 Technisch-organisatorisches Umsetzen des Protokollierens in allen Phasen

Nr.	Maßnahme	ersetzt Maßnahme in V1.0	Gültig-keit
M43.22.01	Die Protokollierung muss die Aktivitäten an Schnittstellen umfassen.	M43.D10	V1.0/ V2.0
M43.22.02	Die Protokollierung muss die Aktivitäten von Systemen und Diensten umfassen.	M43.D08	V1.0 V2.0
M43.22.03	Die Protokollierung muss die Aktivitäten von Schutzmaßnahmen umfassen.	M43.D08	V1.0/ V2.0
M43.22.04	Die Protokollierung muss die Zugänge und Zugriffe von Mitarbeiter*innen umfassen.	M43.D06, M43.D09, M43.P03	V1.0/ V2.0
M43.22.05	Die Protokollierung soll für die Tätigkeiten der fachlichen Sachbearbeitung sachgerecht gestaltet sein.	M43.D06, M43.D18	V1.0/ V2.0
M43.22.06	Für die Protokollierung muss ein Prozess zur Klärung festgelegt sein, falls Zweifel an der Richtigkeit und Vollständigkeit der Protokolldaten bestehen.		V2.0
M43.S03	Ausführen von Befehlen, wenn bestimmte Protokolleinträge erscheinen		V1.0

4.3 Skalieren des Protokollierens für hohes Risiko

Nr.	Maßnahme	ersetzt Maßnahme in V1.0	Gültig-keit
M43.23.01	Die Protokollierung soll in Form einer Vollprotokollierung gestaltet werden.		V2.0
M43.23.02	Die Protokolldaten sollen eine hohe Verfügbarkeit aufweisen.		V2.0
M43.23.03	Die Protokolldaten sollen durch Prüfsummen abgesichert werden.	M43.D17	V1.0/ V2.0
M43.23.04	Die Protokolldaten sollen zertifizierte Zeitstempel und Zeitsynchronisation aufweisen.	M43.D19	V1.0/ V2.0
M43.23.05	Die Protokolldaten sollen verschlüsselt transportiert und gespeichert werden.	M43.P07	V1.0/ V2.0
M43.23.06	Die Protokollierung soll auch für die Administration die Unveränderbarkeit von Protokolldaten zu eigenen Aktivitäten gewährleisten.	M43.P03	V1.0/ V2.0
M43.23.07	Die Protokollierung soll auf einem zentralen Protokollserver betrieben werden.	M43.P06	V1.0/ V2.0

4.4 Evaluierung der Eigenschaften des Protokollierens

Nr.	Maßnahme	ersetzt Maßnahme in V1.0	Gültig-keit
M43.24.01	Für die Protokollierung soll ein Testkonzept erstellt werden.	M43.P02	V1.0/ V2.0
M43.24.02	Für die Protokollierung soll die Auswertung, Dokumentation und Nachbereitung von Tests festgelegt sein.	M43.P02	V1.0/ V2.0

Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden durchgestrichen weiterhin aufgeführt. Damit bleibt die Nummer einer Maßnahme aus der vorigen Version in der 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.

5 Nutzung dieses Bausteins

„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).“