Protokollierung und Protokollierungskonzept – Eine Einführung in die Thematik

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe „Datenschutz & IT-Sicherheit“

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

IHE Deutschland e.V.

Autoren

Ammon, Danny	Universitätsklinikum Jena
Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Isele, Christoph	Cerner Deutschland GmbH
Kadi, Hasan	VISUS Health IT GmbH
Letter, Michael	5medical management GmbH
Rüdlin, Mark	Rechtsanwalt + Datenschutzbeauftragter
Schlütter, Johannes	net.ter GmbH
Schütze, Bernd	Deutsche Telekom Healthcare and Security GmbH
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

Stand: 23. September 2020

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
>
> Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
>
> Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Inhaltsverzeichnis

Teil 1: Protokollierung und Protokollierungskonzept: Was ist das und wozu braucht man eines?

Es gibt verschiedene Gründe, im Zusammenhang mit informationstechnischen Vorgängen eine Protokollierung vorzunehmen, u. a. um die Einhaltung von Datenschutzmaßnahmen zu kontrollieren oder nachzuweisen oder um den Ablauf der Vorgänge nachvollziehen zu können. Weiterhin müssen ggf. Änderungen nachweisbar sein. So verlangen verschiedene Gesetze eine Nachverfolgbarkeit, so z. B.:

- § 630f Abs. 2 BGB verlangt, dass bei stattfindenden Berichtigungen und Änderungen von Eintragungen in einer Patientenakte sowohl der ursprüngliche Inhalt als auch der Änderungszeitpunkt erkennbar bleibt, daher muss Letzteres protokolliert werden.
- Nach § 146 Abs. 4 AO ist die Veränderung einer Buchung oder Aufzeichnung in einer Weise, durch welche der ursprüngliche Inhalt nicht mehr feststellbar ist, unzulässig. Aus dieser Regelung ableitend fordert das Bundesministerium für Finanzen in ihren „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) in Kapitel 8 eine entsprechende Protokollierung[1].
- § 113e TKG verlangt, dass für Zwecke der Datenschutzkontrolle jeder Zugriff protokolliert wird.
- § 22 Abs. 2 Ziff. 2 BDSG verlangt, dass von dem oder den Verantwortlichen bei der Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten Kategorien von personenbezogenen Daten Maßnahmen ergriffen werden, welche gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind[2].
- § 291a Abs. 5 SGB V verlangt, dass bei Verarbeitung von Daten mittels der elektronischen Gesundheitskarte nachprüfbar protokolliert wird, wer auf die Daten zugegriffen hat und von welcher Person die zugreifende Person autorisiert wurde bzw. dass Zugriffe mit Einwilligung der Versicherten erfolgten.
- Nach § 303 Abs. 4 SGB V schränkt die Korrektur von Diagnosedaten durch Krankenkassen gegenüber dem BVA ein, sodass diese Krankenkassen bei Prüfungen dies ggf. auch nachweisen müssen, wozu regelhaft eine entsprechende Protokollierung erforderlich ist.
- In Umsetzung von Art. 25 EU der Richtlinie 2016/680 beinhalten die Datenschutzgesetze des Bundes und der Länder Regelungen, dass in automatisierten Verarbeitungssystemen eine entsprechend den Vorgaben von Art. 25 Abs. 2 RL 2016/680 zweckgebundene Protokollierung stattfinden muss.

[1] Bundesministerium für Finanzen (BMF): Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD). [Online] 2019 [Zitiert 2020-08-09] Verfügbar unter https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html

[2] Ähnliche Vorgaben finden sich auch in verschiedenen landesgesetzlichen Regelungen: § 26 Abs. 1 Ziff. 2 BlnDSG, § 24 Ziff. 2 BbgDSG, § 11 Abs. 2 Ziff. 2 BremDSGVOAG, § 20 Abs. 2 Ziff. 2 HDSIG, 8 Ziff. 2 DSG M-V, § 17 Abs. 2 Ziff. 1 NDSG, § 15 Ziff. 2 DSG NRW, § 19 Abs. 2 Ziff. 1 LDSG RP, § 8 Abs. 2 Ziff. 2 SDSG, § 9 Abs. 2 Ziff. 5 SächsDSG, § 14 Abs. 1 Ziff. 1 DSAG LSA, § 12 Abs. 3 Ziff. 3 LDSG SH

Ergänzend sollte bzgl. der Gestaltung der Protokollierung beachtet werden, dass es gemäß § 130 Abs. 1 OWiG eine Ordnungswidrigkeit darstellt, wenn ein oder mehrere Inhaber[3] eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig Aufsichtsmaßnahmen unterlässt, welche erforderlich sind, um Zuwiderhandlung gegen betriebsbezogene Pflichten zu verhindern, wozu insbesondere auch die die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen als auch die Durchführung von Stichproben gehören[4].

Eine Protokollierung bei der Verarbeitung elektronischer Daten ist daher die Norm; nur in begründeten Ausnahmefällen kann auf eine Protokollierung und damit auf die durch diese ermöglichte Nachweisbarkeit der ordnungsgemäßen Verarbeitung verzichtet werden. Nicht ohne Grund forderte die Artikel-29-Datenschutzgruppe schon 2007 in ihrem Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ eine „ausführliche Protokollierung und Dokumentierung sämtlicher Verarbeitungsschritte, die im System stattgefunden haben, [...] in Verbindung mit regelmäßigen internen Überprüfungen der Berechtigungen und den entsprechenden Folgemaßnahmen“[5].

In der Regel enthalten diese Protokolle personenbeziehbare Daten, weshalb datenschutzrechtliche Vorgaben zu beachten sind, insbesondere ist für jede Verarbeitung personenbezogener Daten ein Erlaubnistatbestand erforderlich. Dementsprechend ist beim Software-Customizing der zur Verarbeitung verwendeten informationstechnischen Systeme auf eine datenschutzkonforme Umsetzung auch der Protokollierung zu achten[6].

Sind an dem Vorgang verschiedene Interessensgruppen beteiligt oder werden Aufgaben delegiert, ist es sinnvoll, die Voraussetzung und die beschlossenen Maßnahmen in einem Konzept schriftlich festzuhalten.

1 Einführung ins Thema „Protokollierung“

Grundsätzlich ist in einem Protokoll festgehalten, zu welchem Zeitpunkt welche Verarbeitung durch wen bzw. durch was veranlasst oder durchgeführt wurde. Die Begriffe „Protokolldateien“, „Logdaten“, „Logfiles“ oder auch „Audit Trails“ werden häufig in Zusammenhang mit einer Protokollierung genannt, teilweise auch synonym zur Protokollierung verwendet. Protokollierung und Audit Trail sind hierbei tatsächlich synonyme Begriffe und bezeichnen das Speichern von Aktivitäten von Nutzern – seien diese Menschen oder Systeme – bei der Nutzung von IT-Systemen. Protokolldateien, Logdaten, Logfiles stellen dabei die bei der Protokollierung angefallenen Daten dar.

[3] Normadressaten der Regelung sind natürliche Personen. Ist der Inhaber eines Betriebs eine juristische Person, so ist entsprechend § 130 i.V.m. § 9 OWiG als „Inhaber“ derjenige aufzufassen, dem die Erfüllung der den Betrieb oder das Unternehmen treffenden Pflichten obliegt. Siehe z.B.

- Bohnert J, Krenberger B, Krumm C.: § 130 Rn. 8. In: Krenberger/Krumm (Hrsg.) Ordnungswidrigkeitengesetz: OWiG. C. H. Beck Verlag 5. Auflage, 2018. ISBN 978-3-406-71566-2
- Rogall K.: § 130, Rn. 25. In: Mitsch (Hrsg.) Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten: OWiG. C. H. Beck verlag 5. Auflage, 2018. ISBN 978-3-406-69510-0

[4] Bohnert J, Krenberger B, Krumm C.: § 130 Rn. 20. In: Krenberger/Krumm (Hrsg.) Ordnungswidrigkeitengesetz: OWiG. C. H. Beck Verlag 5. Auflage, 2018. ISBN 978-3-406-71566-2

[5] Artikel-29-Datenschutzgruppe: Arbeitspapier 131 „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“. [Online] 2007 [Zitiert 2020-08-09] Verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

[6] Czernik A. (2016) Software-Customizing datenschutzkonform umsetzen. ZD-Aktuell: 05029

Bei einer Protokollierung wird insbesondere erfasst, wer, wann, welche Aktivitäten, zu welchem Zeitpunkt an einem System durchführte. Bei den Aktivitäten kann es sich beispielsweise um das Lesen, Ändern, Kopieren oder Löschen von Dateien handeln, aber ebenso stellt das Einspielen von Software-Updates oder Patches eine Aktivität dar.

Vertreter von Aufsichtsbehörden stellen die Notwendigkeit einer Protokollierung zur Gewährleistung verschiedener Schutzziele dar[7]:

Schutzziel	Protokollierung
Vertraulichkeit	Protokollierung lesender Zugriffe Protokollierung der Ausgaben (Drucken, Speichern, Senden)
Integrität	Protokollierung von schreibenden/ändernden Zugriffen bzw. Protokollierung geänderter Daten
Transparenz	Protokollierung von Datenverarbeitungen mit je nach Schutzbedarf zunehmendem Detaillierungsgrad und zunehmender Speicherdauer
	Protokollierung von Konfigurationsänderungen
	Integritätsschutz der Protokolle (separater Protokollierungsserver)

2 Protokollarten: Wozu Protokolle heute verwendet werden

Ein Protokoll wird von einem Schriftführer oder Protokollführer bzw. in seiner digitalen Form automatisiert durch einen informationstechnischen Vorgang angefertigt. In dieser Praxishilfe zur Protokollierung bzw. zur Gestaltung eines Protokollierungskonzeptes geht es ausschließlich um die letztere Variante.

Protokolle können zum einen aufgrund ihrer inhaltlichen Gestaltung unterschieden werden:

- Im Verlaufsprotokoll werden wesentliche Ereignisse in ihrem zeitlichen Kontext dargestellt: was geschah wann in welcher Reihenfolge.
- Im Ergebnisprotokoll werden wesentliche Aktionen und insbesondere die Ergebnisse der Aktionen festgehalten, wobei ein Ergebnisprotokoll die Aktionen mindestens so präzise darstellen sollte, dass die Ergebnisse nachvollzogen werden können.
- Bei einem Wortprotokoll wird jede Aktion in ihrem zeitlichen Verlauf festgehalten.

Bei den informationstechnischen Protokollen gibt es Schreib-/Leselogs, die jedes Lesen und jede Änderung aufzeichnen, gleiches kann mit mehr Aufwand natürlich auch durch handschriftliche Protokollierung gewährleistet werden.

Zum anderen können Protokolle aufgrund ihrer Verwendung unterschieden werden; dies entspricht einer Typdarstellung der Protokolle. Zu den häufigsten verwendeten Protokollarten gehören:

- Behandlungs- bzw. Therapieprotokolle,
- Betriebssystemprotokolle,
- Diagnoseprotokolle,
- Ereignisprotokoll,
- Gesprächsprotokolle,
- Unterrichtungsprotokolle,
- Untersuchungsprotokolle (speziell auch bei digitalen forensischen Untersuchungen angefertigte Protokolle),

[7] So z. B. Probst T. (2012) Generische Schutzmaßnahmen für Datenschutz-Schutzziele. DuD: 439-444

- Versuchsprotokolle,
- Webprotokoll.

Protokolle können dabei zu verschiedenen Zwecken eingesetzt werden, z. B.

- Auditing wird insbesondere zur Verfolgung von An- und Abmeldungen von Benutzern, Änderungen von Benutzerrechten, Zugriff auf und Änderungen an Daten verwendet.
- Monitoring wird zur Analyse des Anwendungsverhaltens, insbesondere der Performance, in Echtzeit genutzt.
- Tracing wird zur Nachvollziehbarkeit des Programmablaufs angewendet.

3 Protokollierung: Hinweise zur technischen Gestaltung

Eine Protokollierung aller Ereignisse kann die vom Rechnersystem bereitgestellten Ressourcen vollständig aufbrauchen, sodass Anwendern das System nicht mehr in der gewohnten Form zur Verfügung steht; das Arbeiten mit dem System ist dann nur noch extrem langsam oder z. T. auch gar nicht mehr möglich. Daher existieren verschiedene Stufen der Protokollierung („Log-Level"), welche die Intensität der Protokollierung beschreiben. Üblicherweise[8] werden Log-Level unterschieden in:

- Fatal: Es werden nur Fehler protokolliert, welche als „fatal" anzusehen sind, z. B. Fehler, die zu einer Beendigung der Anwendung führen
- Error: Es werden Fehler protokolliert, welche zur Laufzeit auftreten und welche die Funktion der Anwendung behindern. Auch unerwartete Programmfehler werden protokolliert.
- Warning: Hierbei werden „Warnungen" protokolliert. Dies umfasst beispielsweise den Aufruf einer veralteten Schnittstelle, einen fehlerhaften Aufruf einer (veralteten oder aktuellen) Schnittstelle oder auch Benutzerfehler.
- Info: Dieser Level protokolliert Informationen wie „start" und „stop" einer Anwendung, An- und Abmeldung von Anwendern usw.
- Debug: Hier werden umfassende Informationen zum Programmablauf protokolliert. Dieser Level wird im Normalfall nur in der Entwicklung oder zur Nachvollziehung eines Fehlers verwendet, da Systemressourcen stark beansprucht werden.
- Trace: Dieses Level dient der detaillierten Verfolgung des Programmablaufs, insbesondere zur Nachvollziehung eines Programmierfehlers und ist damit noch umfangreicher als „Debug".

In Softwareprogrammen wie Betriebssystemen oder Anwendungen werden oftmals fertige Komponenten zur Protokollierung genutzt, sogenannte „Logger". Logger sind fertige Softwarekomponenten, die i. d. R. für eine bestimmte Programmiersprache wie z. B. Java geschrieben wurden und welche in eigene Programme eingebunden werden, um so eine Protokollierung umzusetzen. Gängige Logger sind beispielsweise:

- Apache Log4j
  https://logging.apache.org/log4j/2.x/index.html
- Apache log4net
  https://logging.apache.org/log4net/
- easylogging++
  https://github.com/amrayn/easyloggingpp

[8] Angelehnt an den Vorgaben von log4j: Class Level. [Online] 2012 [Zitiert 2020-07-03] Verfügbar unter http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/Level.html

- ELMAH
  https://elmah.github.io/
- Log4Delphi
  http://log4delphi.sourceforge.net/
- Monolog
  https://github.com/Seldaek/monolog
- NLog
  https://github.com/NLog/NLog
- PSR-3
  https://www.php-fig.org/psr/psr-3/
- spdlog
  https://github.com/gabime/spdlog

Daneben gibt es Standardisierungen zur Protokollierung. „syslog“ beispielsweise ist ein Standard, der sowohl spezifiziert, wie eine syslog-Meldung aussieht, aussieht, als auch die Übermittlung von Log-Meldungen innerhalb eines IP-Rechnernetzes beschreibt[9].

Abhängig von dem zu protokollierenden IT-System können nur Anwendungen Protokolleinträge schreiben. Dabei kann ein IT System ein oder mehrere Protokolle schreiben. Weiterhin können die Protokolle eines Informationsverbundes gemeinsam analysiert werden, um die Schutzziele zu erreichen.

Bei verteilten Anwendungen sind zusätzliche technische Maßnahmen wie beispielsweise Zeitsynchronisation oder zentrale Identity Provider zu ergreifen.

4 Datenschutzkonforme Protokollierung

Für die Protokollierung ist es zunächst egal, worauf Zugriffe erfolgen. Zugriffe können auf Rechner bzw. Server erfolgen (z. B. bei der Anmeldung des Anwenders), desgleichen können Zugriffe auf Dateien in einem Dateisystem protokolliert werden (z. B. Öffnen oder Speichern einer Textdatei), und ebenso können Internet Aktivitäten (z. B. der Aufruf einer Webseite) in einer Protokolldatei festgehalten werden. Da jedoch immer festgehalten wird, wer auf was zugegriffen hat, handelt es sich bei Protokolldaten nahezu immer um personenbezogene Daten; es ist die absolute Ausnahme, dass in einer Protokolldatei nur Zugriffe anderer Maschinen festgehalten werden und diese Maschinen nicht wiederum einem zugreifenden Menschen zurechenbar sind.

Daher müssen auch Protokolldaten den datenschutzrechtlichen Anforderungen genügen, insbesondere den in Art. 5 DS-GVO genannten Grundsätzen entsprechen:

Grundsätze gem. Art. 5 DS-GVO	Erläuterung
Rechtmäßigkeit der Verarbeitung	Die Protokollierung jedes Datums in einer Protokolldatei bedarf einer rechtlichen Grundlage.
Transparente Verarbeitung	Die Protokollierung muss in einer für die betroffenen Personen nachvollziehbaren Weise erfolgen.

[9] Näheres zu syslog siehe die entsprechenden RFCs, insbesondere RFC 3195 (Reliable Delivery for syslog, https://www.rfc-editor.org/info/rfc3195), RFC 5424 (The Syslog Protocol, https://www.rfc-editor.org/info/rfc5424), RFC 6587 (Transmission of Syslog Messages over TCP, https://www.rfc-editor.org/info/rfc6587), RFC 5425 (Transport Layer Security (TLS) Transport Mapping for Syslog, https://www.rfc-editor.org/info/rfc5425), RFC 5675 (Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, https://www.rfc-editor.org/info/rfc5675)

Zweckbindung	Vor Beginn der Aufzeichnung von Protokolldaten muss der eindeutige und legitime Verwendungszweck der Protokollierung festgelegt werden und die Daten dürfen ausschließlich hierzu verwendet werden.
Datenminimierung/ Datensparsamkeit	Es dürfen nur zur Erreichung des Protokollierungszweckes erforderliche Daten verarbeitet werden; das Merkmal der Erforderlichkeit ist immer nur dann erfüllt, wenn sich bei gleicher Eignung kein milderes Mittel finden lässt, welches die Persönlichkeitsrechte betroffener Personen wie Patienten oder Beschäftigte weniger beeinträchtigt.
Richtigkeit	Die Protokolldaten müssen richtig sein, d. h. die (i. d. R.) automatische Generierung der Protokolldaten muss regelmäßig stichprobenartig bzgl. der Richtigkeit der Daten geprüft werden, da Softwareupdates ggf. die Protokollierung ändern.
Speicherbegrenzung/ Löschfristen	Protokolldaten müssen regelmäßig gelöscht werden[10]. Insbesondere Protokolldaten, die ausschließlich für Zwecke der Fehlersuche genutzt werden und es unerheblich ist, welche natürliche Person einen Zugriff durchführte, sind schnellstmöglich zu anonymisieren oder, wenn dies nicht möglich ist, zu pseudonymisieren.
Integrität und Vertraulichkeit	Auch bei der Protokollierung muss die Sicherheit der Verarbeitung gewährleistet werden. Insbesondere müssen Protokolldaten manipulationssicher gespeichert werden, damit die Unveränderthеit und damit die Richtigkeit auch über den gesamten Lebenszyklus der Daten gewährleistet wird.

Natürlich müssen auch alle datenschutzrechtlichen Anforderungen erfüllt werden. Insbesondere gehört dazu:

Privacy by Design (Art. 25 DS-GVO)	Die Protokollierung muss so datensparsam und datenschutzfreundlich wie möglich konzipiert werden.
Privacy by Default (Art. 25 DS-GVO)	Die datenschutzfreundliche Protokollierung muss die Voreinstellung sein. Nur in begründeten Ausnahmefällen kann eine umfangreiche Protokollierung eingestellt werden, z. B. wenn anders eine Fehlerbehebung nicht möglich ist („Debug“-Protokollierung)
Sicherheit der Verarbeitung (Art. 32 DS-GVO)	Muss gewährleistet sein. Insbesondere gehört dazu eine Festlegung, welche Personen aus welchen Gründen unter welchen Umständen Protokolldaten einsehen und auswerten dürfen.

Neben datenschutzrechtlichen Aspekten sind natürlich auch alle anderen relevanten rechtlichen Gegebenheiten zu berücksichtigen, wie z. B. eine Verletzung des Fernmeldegeheimnisses durch eine entsprechende Protokollierung: „Strafbare Verletzungen des Fernmeldegeheimnisses kommen in Betracht, wenn in einem Unternehmen die private Nutzung dienstlicher Kommunikationsmittel nicht ausdrücklich geregelt ist oder eine Regelung nicht ausreichend kontrolliert wird. Protokollierungen

[10] Darauf wies schon der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der am 2.11.2009 veröffentlichten „Orientierungshilfe Protokollierung“ hin. [Online] 2009 [Zitiert 2020-08-09] Verfügbar unter http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Protokollierung.pdf?__blob=publicationFile&v=3

der Internetnutzung und sogar die Archivierung von E-Mails können den Straftatbestand von § 206 StGB erfüllen."[11]

5 Kontrolle der Protokollierung durch den Datenschutzbeauftragten

Die in Art. 39 DS-GVO erfolgten Zuweisungen von Aufgaben an den Datenschutzbeauftragten spiegeln zunächst die entsprechenden Verpflichtungen des Verantwortlichen bzw. des Auftragsverarbeiters wieder, d. h. die in Art. 39 DS-GVO festgelegten Aufgaben des Datenschutzbeauftragten spezifizieren indirekt die Verpflichtungen des Verantwortlichen, welche in dieser Detailliertheit in Art. 24 DS-GVO nicht enthalten sind[12]. Dabei wird dem Datenschutzbeauftragten lediglich die Überwachungsfunktion zugewiesen; auf Grund fehlender Regelungskompetenz ist der Datenschutzbeauftragte nicht für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich, dies ist die ausschließliche Pflicht des Verantwortlichen[13]. Bei festgestellten Defiziten besteht aber gemäß Art. 39 Abs. 1 lit. a DS-GVO für Datenschutzbeauftragte die Pflicht zur datenschutzrechtlichen Beratung, um aufzuzeigen, wie eine datenschutzkonforme Verarbeitung möglich ist[14].

Entsprechend Art. 39 Abs. 1 lit. b DS-GVO gehört die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben zu den Kernaufgaben des Datenschutzbeauftragten. Art. 39 Abs. 2 DS-GVO zufolge muss hierbei ein risikobasierter Ansatz verfolgt werden, d. h. Umfang und Intensität der vom Datenschutzbeauftragten durchgeführten Überprüfungshandlungen muss sich dabei an Umfang und Kritikalität der Datenverarbeitung orientieren[15]. Da Gesundheitsdaten wie auch genetische Daten entsprechend den Vorgaben der DS-GVO zu den besonders schützenswerten Daten gehören, verlangt die Kritikalität der mit diesen Daten verbundenen Verarbeitungen regelhaft auch entsprechende regelmäßige Kontrollen.

Dementsprechend sind neben anlassbezogenen Kontrollen immer auch stichprobenartige Regelkontrollen bzgl. der Einhaltung der Ordnungsmäßigkeit der Verarbeitung der Daten erforderlich. Die Kontrollen dürfen sich nicht auf Bewertungen der Prozessbeschreibungen beschränken, vielmehr umfasst diese Aufgabe stets auch die Überprüfung, ob vorgesehene Sicherheitsmaßnahmen tatsächlich umgesetzt und wirksam sind[16], was immer auch eine Überprüfung und Einsichtnahme in die Unterlagen vor Ort erfordert[17] und damit eine Prüfung der Protokolldaten beinhaltet. Somit stellt Art. 39 Abs. 1 lit. b DS-GVO mit der Anforderung zur Kontrolle immer auch zugleich eine Rechtsgrundlage zur Nutzung von Protokolldaten zu diesem Überwachungszweck dar.

---

[11] So Scheja G, Haag C.: Teil 5 Datenschutzrecht, Rn. 384. In: Leopold/Glossner (Hrsg.) Münchener Anwaltshandbuch IT-Recht. C. H. Beck verlag, 3. Auflage 2013. ISBN 978-3-406-64845-8

[12] Moos F.: Art. 39, Rn. 10. In: Wolff/Brink (Hrsg.) Beck'scher Online-Kommentar Datenschutzrecht. C. H. Beck Verlag 2020, 32. Ed.

[13] Reif Y, Jaspers A.: Art. 39, Rn. 14. In: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.) DS-GVO/BDSG Datenschutz-Grundverordnung Bundesdatenschutzgesetz. Verlag C. F. Müller, 1. Auflage 2018. ISBN 978-3-8114-4712-7

[14] Bergt M.: Art. 39, Rn. 13. In: Kühling / Buchner (hrsg.) Datenschutz-Grundverordnung / Bundesdatenschutzgesetz: DS-GVO / BDSG. C.H.BECK, 2 Auflage 2018. ISBN 978-3-406-71932-5

[15] Drewes S.: Art. 39, Rn. 18, 38-40. In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[16] Bergt M.: Art. 39, Rn. 15. In: Kühling / Buchner (hrsg.) Datenschutz-Grundverordnung / Bundesdatenschutzgesetz: DS-GVO / BDSG. C.H.BECK, 2 Auflage 2018. ISBN 978-3-406-71932-5

[17] Drewes S.: Art. 39, Rn. 19. In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

Auch die Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten ergibt sich unmittelbar aus dem Unionsrecht. Art. 33 Abs. 5 DS-GVO verlangt die Dokumentation aller Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten. Aus einer Verletzung des Schutzes personenbezogener Daten resultiert immer auch eine anlassbezogene Überprüfung der Verarbeitung durch den Datenschutzbeauftragten[15], natürlich auch hier verbunden mit der Nutzung der Protokolldaten zur Feststellung und Klärung des Sachverhalts für den entsprechenden Vorfall[18].

Wesentlich ist, dass eine Rückmeldung des Prüfergebnisses erfolgt. Nur wenn die zuständigen Beschäftigten resp. Abteilungen über das Prüfergebnis und dem darin ggf. festgestellten Nachbesserungsbedarf informiert werden, können diese evtl. notwendige Anpassungen am Verarbeitungsprozess vornehmen. Insbesondere bei Verletzungen des Schutzes personenbezogener Daten kann eine Information des Compliance-Verantwortlichen, der Rechtsabteilung und/oder der Revisionsabteilung erforderlich sein[19].

Die Überprüfung selbst kann dabei entsprechend den Empfehlungen des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein im Rahmen eines Stufenmodells erfolgen[20].

6 Mitbestimmung durch Personalvertretung

Eine Mitarbeitervertretung wie ein Betriebsrat oder eine Personalvertretung kann einerseits ein Recht auf Information gemäß § 80 II 1 BetrVG haben, denn zu ihren Aufgaben gehört gemäß § 80 Abs. 1 Nr. 1 BetrVG die Überprüfung der Einhaltung der geltenden Gesetze, also auch des Datenschutzrechts. Das Informationsrecht einer Mitarbeitervertretung erstreckt sich damit unter anderem auf die Frage, in welcher Weise bei IT-Systemen personenbezogene Dateien auch in Protokolldateien verarbeitet werden. Dabei handelt es sich um ein grundsätzliches Recht, welches der Arbeitgeber auch nicht mit einem Hinweis auf eine „Geringfügigkeitsschwelle“ oder eine „Erheblichkeits- oder Üblichkeitsschwelle“ umgehen kann[21].

Das in § 87 Abs. 1 Nr. 6 BetrVG enthaltene Mitbestimmungsrecht bei der Arbeitnehmerüberwachung durch technische Einrichtungen reicht sehr weit[22,23]. So genügt es, dass eine technische Einrichtung i. S. v. § 87 Abs. 1 Nr. 6 BetrVG bloß dazu geeignet ist, das Verhalten und/oder die Leistung der Arbeitnehmer zu kontrollieren[24].

---

[18] Lindner M. (2020) Datenschutz und Interne Untersuchungen – mal anders. CCZ: 160-162

[19] Drewes S.: Art. 39, Rn. 20. In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[20] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Private sowie dienstliche Internet- und E-Mail-Nutzung, Kapitel 5 „Eskalierendes Stufenmodell“. [Online] 2014 [Zitiert 2020-08-09] Verfügbar unter https://www.datenschutzzentrum.de/artikel/594-Private-sowie-dienstliche-Internet-und-E-Mail-Nutzung.html bzw. pdf-Datei unter https://www.datenschutzzentrum.de/uploads/privatwirtschaft/private-und-dienstliche-internetnutzung.pdf

[21] BAG, Urt. v. 2018-10-23, AZ 1 ABN 36/18. [Online] 2018 [Zitiert 2020-06-27] Verfügbar unter https://dejure.org/2018,36184

[22] Kaiser D, Annuß G.: § 75 BPersVG, Rn. 537-545. In: Richardi/Dörner/Weber (Hrsg.) Personalvertretungsrecht. C.H. Beck Verlag, 5. Auflage 2020. ISBN 978-3-406-74073-2

[23] Eine kritische Auseinandersetzung mit dem Thema findet sich z. B. in: Haußmann K, Thieme LM (2019) Reformbedarf und Handlungsoptionen in der IT-Mitbestimmung. NZA: 1612-1620

[24] Schulze MO, Ratzesberger E (2016) Einführung von Software – Grundlagen und Grenzen der betrieblichen Mitbestimmung. ArbRAktuell: 301-303

Das BAG stellte bereits in der „Techniker-Berichtssystem“-Entscheidung vom 14.9.1984 fest, dass es nicht von Belang ist, ob eine Datenerhebung, Datenverarbeitung oder sonstige Datennutzung zur Überwachung von Beschäftigten vorliegt[25]. Vielmehr reicht es aus, wenn die Möglichkeit einer „Überwachung“ i. S. von § 87 Abs. 1 Nr. 6 BetrVG gegeben ist. Es ist daher nicht erforderlich, dass eine technische Einrichtung dem Zweck der Mitarbeiterüberwachung dient, sie muss nur die Möglichkeit bieten, damit das Mitbestimmungsrecht der Arbeitnehmervertretung zu beachten ist.

Zwar weisen nicht sämtliche Beschäftigtendaten, die einer Überwachung zugänglich sind, einen Verhaltens- oder Leistungsbezug auf, so etwa nicht Statusdaten des Arbeitnehmers als solche, wie etwa Anschrift, Geschlecht oder Kontoverbindung[26]. Jedoch ist es nach der Rechtsprechung des BAG ausreichend, wenn bei der technischen Datenverarbeitung eine Datenverknüpfung in der Weise erfolgt, dass Aussagen über das Verhalten oder die Leistung von Arbeitnehmern möglich sind[27]. Insofern kann selbst die Verarbeitung von Statusdaten mitbestimmungspflichtig sein.

Eine Protokollierung erlaubt eher regelhaft zumindest eine Erfassung der zeitlichen Nutzung der Systeme durch die bedienenden Personen[28]. Protokollierungen beinhalten daher i. d. R. die Möglichkeit einer Form der Leistungsüberwachung von Beschäftigten und daher wird regelhaft ein Mitbestimmungsrecht der Beschäftigtenvertretung bei der Protokolldatenverarbeitung anzunehmen sein[29]. Ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG scheidet nur dann aus, wenn es um nicht-personenbezogene Protokolldaten geht.

Vor dem Hintergrund eines möglicherweise bestehenden Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG ist es sinnvoll, eine Protokollierung über eine Betriebsvereinbarung zu regeln. Der Abschluss einer Betriebsvereinbarung ist nicht nur naheliegend, soweit ein Mitbestimmungsrecht der Arbeitnehmervertretung besteht, sondern sie ist auch ein datenschutzrechtlich sinnvolles Regelungsinstrument.

Betriebsvereinbarungen i.S.v. Kollektivvereinbarungen kommen gemäß § 26 Abs. 4 BDSG als datenschutzrechtlicher Erlaubnistatbestand in Betracht. Betriebsvereinbarungen können dabei natürlich nicht den durch das Datenschutzrecht gewährleisteten Persönlichkeitsschutz der Beschäftigten reduzieren, können aber die teilweise unbestimmten Begriffe des Datenschutzrechts konkretisieren. Betriebsvereinbarungen müssen sich daher am Schutzstandard des Datenschutzrechts, insbesondere an der DS-GVO, orientieren und dürfen datenschutzrechtliche Betroffenenrechte nicht einschränken[30,31,32]. Insbesondere dürfen Betriebsvereinbarungen nicht

[25] BAG, Urt. v. 1984-09-14, AZ 1 ABR 23/82. [Online] 1984 [Zitiert 2020-06-27] Verfügbar unter https://dejure.org/1984,261

[26] BAG, Urt. v. 1986-10-22, Az. 5 AZR 660/85. [Online] 1984 [Zitiert 2020-06-27] Verfügbar unter https://dejure.org/1986,615

[27] BAG, Urt. v. 1986-03-11.03, Az 1 ABR 12/84. [Online] 1984 [Zitiert 2020-06-27] Verfügbar unter https://dejure.org/1986,220

[28] Leopold N. (2006) Protokollierung und Mitarbeiterdatenschutz: Zielkonflikte im Bundesdatenschutzgesetz. DuD, 274-276

[29] Hilber MD, Frik R. (2002) Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat. RdA: 89

[30] Reif Y. (2018) Betriebsvereinbarungen zur Datenverarbeitung nach DS-GVO und BDSG 2018. RDV: 89-91

[31] Wünschelbaum M. (2019)Zur Einschränkung des DSGVO-Auskunftsanspruchs durch Betriebsvereinbarungen. BB: 2102-2106

[32] Krieger S, Arnold C, Zeh (2020) Betriebsvereinbarungsoffene Arbeitsverträge – Gestaltungsmöglichkeiten und Grenzen in der Praxis. NZA: 81-87

hinter grundgesetzlichen Wertungen und den in § 75 Abs. 2 BetrVG genannten Standards zurückbleiben[28,33].

In einer Betriebsvereinbarung zum Umgang mit der Protokollierung in IT-Systemen können die grundsätzlichen Punkte vereinbart werden, sodass diese nicht für jedes eingesetzte IT-System einzeln verhandelt werden müssen. Zu diesen Punkten können beispielsweise gehören:

- Zweckfestlegung der Verarbeitung von Protokolldateien
- Umfang der Auswertung von Protokolldateien (lückenlos oder anlassbezogen, also bei begründetem Verdacht von Missbrauchsfällen, oder Stichprobenverfahren)
- Festlegung der Auswertungsmodalitäten und Auswertungsberechtigungen, Klärung des Umfangs einer Beteiligung der Arbeitnehmervertretung
- Festlegung, inwiefern Betroffene (Arbeitnehmer) über die Auswertung von Protokolldateien zu informieren sind.

In Anhang 4: findet sich ein Beispiel für eine derartige Betriebsvereinbarung.

7 Protokollierungskonzept

Der in Art. 5 Abs. 2 DS-GVO und an diversen anderen Stellen der DS-GVO geforderten Nachweispflicht kann ein Verantwortlicher nur nachkommen, wenn eine entsprechende Dokumentation vorliegt. Diese Dokumentation, in welcher Verwendungszweck, Rechtsgrundlage, Berechtigungen, Löschverfahren usw. dargestellt sind, nennt man „Protokollierungskonzept“.

Da in verschiedenen IT-Systemen die Art und Weise der Protokollierung unterschiedlich erfolgt, andere Daten erfasst werden, Berechtigungen unterschiedliche Ausprägungen und Möglichkeiten aufweisen und auch hinsichtlich der Möglichkeiten zur Löschung der Protokolldaten unterschiedlich agieren, muss i. d. R. pro IT-System ein Protokollierungskonzept erstellt werden. Idealerweise wird bei einer Ausschreibung von IT-Systemen darauf hingewiesen, dass es zu den Pflichten des Lieferanten resp. des Dienstleisters gehört, an der Erstellung des Protokollierungskonzeptes mitzuwirken.

Zu den Inhalten eines Protokollierungskonzeptes gehören insbesondere:

- Der Geltungsbereich des Protokollierungskonzeptes
- Zweck der Protokollierung
- Art und Umfang der bei der Protokollierung verarbeiteten Daten inkl. der Rechtsgrundlage für die Verarbeitung der Daten
- Speicherort der Daten
- Rollen und Berechtigungskonzept sowie die Beschreibung, wie die Protokolldaten von wem aufgrund welcher Ereignisse in welcher Form verarbeitet werden dürfen; dies schließt insbesondere evtl. geplante Auswertungen ein
- Löschung der Daten unter Angabe von Löschzeitpunkten
- Sicherheit der Verarbeitung, insbesondere
    - TOM gegen unbefugten Zugriff
    - Manipulationssichere Erzeugung und Speicherung
    - Beschreibung der Pseudonymisierung/Anonymisierung, wenn diese vorgesehen sind
- Ggf. Exportmöglichkeiten inkl. Beschreibung des Exportformates sowie Schutz bei Übermittlung der exportierten Daten
- Auditierung des ordnungsgemäßen Umgangs mit Löschprotokollen.

[33] Sassenberg Th, Bamberg N. (2006) Betriebsvereinbarung contra BDSG? DuD: 226-229

Teil 2: Protokollierungskonzept: Was gehört hinein?

1 Geltungs- und Anwendungsbereich des Protokollierungskonzeptes

In der Regel ist es erforderlich, dass für jedes IT-System wie beispielsweise ein Betriebs- oder Anwendungssystem, ein eigenes Protokollierungskonzept angefertigt wird. Art und Umfang der Protokollierung, Möglichkeiten der Rechtevergabe, Auswerteverfahren usw. unterscheiden sich nahezu immer, sodass hier ein gemeinsames Protokollierungskonzept für mehrere IT-Systeme häufig nicht möglich ist.

Daher muss im jeweiligen Protokollierungskonzept der jeweilige Geltungs- und Anwendungsbereich festgelegt sein, damit für Anwender und betroffene Personen eine transparente Verarbeitung erfolgt.

2 Definitionen/Begrifflichkeiten

Unbekannte bzw. nicht normierte Begrifflichkeiten sollten im Protokollierungskonzept kurz dargestellt und erläutert werden, damit ein einheitliches Verständnis der im Protokollierungskonzept getroffenen Regelungen erreicht wird.

Dabei sollten keine Begriffe in für den Verantwortlichen geltenden Gesetzen und Verordnungen als Wiederholung im Protokollierungskonzept aufgeführt werden; die gesetzlich normierten Begriffe gelten einerseits unmittelbar, andererseits kann es bei Änderungen der gesetzlichen Regelungen zu Widersprüchen mit den Vorgaben im Protokollierungskonzept kommen. Beispiele für gesetzlich normierte Begriffe, die nicht in ein Protokollierungskonzept gehören, sind:

- Personenbezogene Daten (Art. 4 Ziff. 1 DS-GVO)
- Beschäftigtendaten (§ 26 Abs. 8 BDSG, § 4 Ziff. 20 DSG-EKD, § 4 Ziff. 24 KDG)

Zu den Begriffen, die hingegen erklärt werden könnten, gehören insbesondere:

Begriff	Formulierungsvorschlag
Audit	systematische und unabhängige Prüfung von Zugriffen auf, Ergänzungen zu oder Änderungen in informationstechnischen Systemen, um zu ermitteln, ob die Aktivitäten und Daten in Übereinstimmung mit den organisationsinternen Standardarbeitsanweisungen und Leitlinien und den geltenden behördlichen Anforderungen ausgeführt bzw. erfasst, verwendet, aufbewahrt oder offenbart wurden. (Quelle: Nach DIN EN ISO 27789)
Notfallzugriff	Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen. (Quelle: DIN CEN ISO/TS 14265)
Protokolldaten	Jedes Datum, welches im Rahmen einer Protokollierung erhoben wird.
Protokollierung	Manuelle oder automatische Aufzeichnung (Speicherung) ausgewählter betriebs- und sicherheitsrelevante Ereignisse zum Zweck einer späteren Auswertung, welche zumindest mindestens den Zeitpunkt, die ausgeführte Handlung und den Handelnden beinhaltet. (Quelle: Nach BSI IT-Grundschutz-Kompendium, OPS.1.1.5 Protokollierung)

3 Zweck der Protokollierung

Der Zweck der Protokollierung besteht darin,

- eine Verarbeitung personenbezogener Daten transparent zu gestalten,
- betroffenen Personen über die Verarbeitung ihrer Daten auf Nachfrage eine Auskunft erteilen zu können und/oder
- die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisen zu können.

Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche Daten, insbesondere personenbezogene Daten, in welcher Weise verarbeitet hat.

Weiterhin dient eine Protokollierung der Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten als auch der Gewährleistung der Verfügbarkeit einer IT-Anwendung resp. der Nutzung dieser Anwendung zur Verarbeitung der personenbezogenen Daten. Insbesondere kann die Analyse technischer Fehler unter Nutzung von Protokolldaten erforderlich sein, um die Sicherheit der Verarbeitung zu gewährleisten. Desgleichen kann sowohl die Optimierung des Netzes als auch die statistische Feststellung der Nutzung der Anwendung durch die Anwender erforderlich sein, um die Verfügbarkeit der Anwendung zu gewährleisten. Die Erforderlichkeit zur Nutzung der Protokolldaten muss, sofern nicht direkt offensichtlich, im Einzelfall dargestellt und festgehalten werden.

Zusammenfassend sind die Zwecke der Protokollierung:

1) Erteilung einer Auskunft auf Antrag einer betroffenen Person,
2) Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung,
3) Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten,
4) Gewährleistung der Sicherheit der Verarbeitung,
5) Gewährleistung der Verfügbarkeit der Anwendung,
6) Gewährleistung der Integrität der Daten,
7) Missbrauchskontrolle bei Vorliegen von Hinweisen auf eine arbeitsvertragliche Pflichtverletzung oder Anhaltspunkten auf eine im Beschäftigungsverhältnis begangene Straftat.

4 Zweckbindung

Protokolldaten unterliegen einer strikten Zweckbindung. Sie dürfen ausschließlich zu den Zwecken genutzt werden, die Anlass für die Speicherung waren. Insbesondere eine Leistungskontrolle von Beschäftigten ist unzulässig.

Nur in schriftlich zu begründenden Ausnahmefällen ist eine Nutzung der Daten aufgrund bestehender gesetzlicher Regelungen für andere Zwecke, z. B. zur Strafverfolgung, zulässig.

5 Rechtsgrundlage

Der Verantwortliche muss entsprechend Art. 24 DS-GVO geeignete technische und organisatorische Maßnahmen umsetzen, welche eine Verarbeitung gemäß den Vorgaben der DS-GVO sicherzustellen und auch den Nachweis dafür erbringen. Dazu gehört auch die Protokollierung. Entsprechend seiner

Delegationsbefugnis wird mit der Kontrolle der ordnungsgemäßen Protokollierung entsprechend der jeweiligen Zwecke wie folgt beauftragt:

- Erfüllung Datenschutzrechtlicher Anforderungen: Datenschutzbeauftragter
  D.h. zu den Aufgaben des Datenschutzbeauftragten gehören insbesondere:
  - Erteilung einer Auskunft auf Antrag einer betroffenen Person[34]
    Rechtsgrundlage: Art. 15 DS-GVO i. V. m. dem jeweiligen geltenden nationalem Recht
  - Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung
    Rechtsgrundlage: Art. 39 Abs. 1 lit. b DS-GVO
  - Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten
    Rechtsgrundlage: Art. 33 Abs. 5 DS-GVO
- Sicherheit der Verarbeitung: IT-Sicherheitsbeauftragter
  D.h. zu den Aufgaben des IT-Sicherheitsbeauftragten gehören insbesondere
  - Gewährleistung der Sicherheit der Verarbeitung
    Rechtsgrundlage: Art. 32 DS-GVO
  - Gewährleistung der Verfügbarkeit der Anwendung sowie der Integrität der Daten
    Rechtsgrundlage: Art. 32 Abs. 1 lit. b DS-GVO

Gerade bei den in Art. 9 Abs. 1 DS-GVO genannten Kategorien personenbezogener Daten ist neben der Datenschutz-Grundverordnung immer auch das jeweilige nationale Recht zu betrachten; viele Erlaubnistatbestände in Art. 9 Abs. 2 DS-GVO verweisen auf nationales Recht, Art. 9 Abs. 4 DS-GVO erlaubt den Mitgliedsstaaten für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten eigene Rechtsgrundlagen zu schaffen. Im deutschen Recht müssen daher neben der DS-GVO die jeweils geltenden bundes-bzw. landesrechtlichen Bestimmungen beachtet werden.

Im Regelfall basiert die Verarbeitung der Protokolldaten, sowohl des Betroffenenkreises der Beschäftigten, deren Daten durch Anwendung der Systeme generiert werden, als auch der Betroffenenkreise, deren Daten verarbeitet werden, wie Patienten, somit auf der Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche aus dem Datenschutzrecht unterliegt, jeweils in Verbindung mit den oben genannten Bestimmungen. Insbesondere müssen natürlich Beschäftigtendaten verarbeitet werden, um die für den Verantwortlichen geltenden datenschutzrechtlichen Verpflichtungen wie z. B. die Erteilung einer Auskunft gegenüber der betroffenen Person gemäß Art. 15 DS-GVO erfüllen zu können. Selbstverständlich gilt das Auskunftsrecht auch entsprechend für betroffene Beschäftigte, sodass diese Anspruch darauf haben, eine Auskunft zu erhalten, wer ihre Daten – Protokolldaten eingeschlossen – wann zu welchen Zwecken verarbeitete[35].

[34] Grundsätzlich ist die Gewährleistung der Betroffenenrechte Aufgabe des Verantwortlichen, jedoch können diese Pflichten vom Verantwortlichen an den Datenschutzbeauftragten übertragen werden (siehe Reif Y, Jaspers A: Art. 38 Rn. 23. In: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.) DS-GVO/BDSG. C. F. Müller Verlag, 1. Auflage 2018. ISBN 978-3-8114-4712-7). Wenden sich betroffene Personen direkt an den Datenschutzbeauftragten, kann daraus auch die Pflicht entstehen, den Sachverhalt aufzuklären und der betroffenen Person entsprechende Informationen zukommen zu lassen (siehe Drewes S.: Art. 38 Rn. 45,46. In: Simitis/Hornung/Spiecker gen. Döhmann /Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2018. ISBN 978-3-8487-3590-7). Aber auch in diesen Fällen bleibt der grundsätzliche Adressat für die Anliegen der betroffenen Person der Verantwortliche (siehe Paal B.P.: Art. 38 Rn. 12, In: Paal/Pauly (Hrsg.) DS-GVO BDSG. C. H. Beck Verlag 2. Auflage, 2018. ISBN 978-3-406-71838-0).

[35] Lembke M. (2020) Der datenschutzrechtliche Auskunftsanspruch im Anstellungsverhältnis. NJW: 1841-1846

Eine grobe Unterteilung lässt sich zwischen niedergelassenem und stationärem Bereich als auch der Verarbeitung von Sozialdaten einerseits darstellen, andererseits müssen auch die nationalen Regelungen für die Verarbeitung von Beschäftigtendaten betrachtet werden. Auf diese Punkte wird im Folgenden kurz eingegangen.

5.1 Patientendaten, niedergelassener Bereich

Die Protokollierung dient einerseits den Zwecken zur Erfüllung datenschutzrechtlicher Anforderungen wie der Erteilung einer datenschutzrechtlichen Auskunft an die betroffene Person (Art. 15 DS-GVO i. V. m. § 34 BDSG) und dem Nachweis der Rechtmäßigkeit der Verarbeitung der verantwortlichen Stelle, andererseits der Gewährleistung der Sicherheit und der Verfügbarkeit des Systems (Art. 32 DS-GVO i. V. m. § 22 Abs. 2 BDSG), insbesondere auch der Nachvollziehbarkeit der Verarbeitung bei einer Verletzung des Schutzes von Gesundheitsdaten (Artt. 33, 34 DS-GVO).

5.2 Patientendaten, stationärer Bereich

Die Protokollierung dient einerseits den Zwecken zur Erfüllung datenschutzrechtlicher Anforderungen wie der Erteilung einer datenschutzrechtlichen Auskunft an die betroffene Person (Art. 15 DS-GVO i. V. m. mit der Regelung des jeweils geltenden Landeskrankenhausrechts), andererseits der Gewährleistung der Sicherheit und der Verfügbarkeit des Systems (Art. 32 DS-GVO i. V. m. mit der Regelung des jeweils geltenden Landeskrankenhausrechts) und dem Nachweis der Rechtmäßigkeit der Verarbeitung der verantwortlichen Stelle, insbesondere auch der Nachvollziehbarkeit der Verarbeitung bei einer Verletzung des Schutzes von Gesundheitsdaten (Artt. 33, 34 DS-GVO i. V. m. mit der Regelung des jeweils geltenden Landeskrankenhausrechts, sofern vorhanden).

5.3 Sozialdaten

Die Protokollierung dient einerseits den Zwecken zur Erfüllung datenschutzrechtlicher Anforderungen wie der Erteilung einer datenschutzrechtlichen Auskunft an die betroffene Person (Art. 15 DS-GVO i. V. m. § 83 SGB X)) und dem Nachweis der Rechtmäßigkeit der Verarbeitung der verantwortlichen Stelle, andererseits der Gewährleistung der Sicherheit und der Verfügbarkeit des Systems (Art. 32 DS-GVO), insbesondere auch der Nachvollziehbarkeit der Verarbeitung bei einer Verletzung des Schutzes von Sozialdaten (Artt. 33, 34 DS-GVO i. V. m. § 83a SGB X).

5.4 Beschäftigtendaten

Die Verarbeitung von Beschäftigtendaten bei der Protokollierung dient ausschließlich den Zwecken

a) von der Verarbeitung ihrer Daten betroffenen Personen Auskunft zu erteilen.
b) die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 2 DS-GVO nachweisen zu können sowie
c) der Gewährleistung der Sicherheit der Verarbeitung.

Die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten stellt hierbei § 26 BDSG[36] i.V.m. Art. 88 DS-GVO dar.

Abzugrenzen von den dargestellten Zwecken sind Verarbeitungen zu weitergehenden Compliance-Kontrollen oder internen Ermittlungen von dieser Rechtsgrundlage nicht erfasst. Hier können

[36] Hier müssen ggf. die entsprechenden Regelungen aus den Landesdatenschutzgesetzen bzw. Kirchengesetzen angegeben werden, wenn das Bundesdatenschutzgesetz für den Verantwortlichen nicht anwendbar ist.

Kollektivvereinbarungen eine Rechtsgrundlage abbilden[37,38], diese sind aber nicht Bestandteil des vorliegenden Protokollierungskonzeptes.

6 Art der verarbeiteten Daten

Es werden nur die zur Erreichung des Verarbeitungszweckes erforderlichen Daten verarbeitet. Eine Beschreibung der Daten findet sich in Kapitel 8.1.

Der Umgang mit dem Löschprotokoll wird in der Praxishilfe zum Löschkonzept[39] beschrieben.

6.1 Protokollierung mit ATNA

Die Protokollierung erfolgt entsprechend den Vorgaben von IHE ATNA. Elemente der Protokollierung sind:

- Art der Aktivität,
- Zeitpunkt der Aktivität bzw. des Ereignisses,
- ausführende Person,
- betroffene Person (Patient/Versicherter)
- ggf. Eingabedaten.

Eine genaue Beschreibung der Protokolldaten sowie eine Darlegung der Notwendigkeit der Verarbeitung findet sich in Anhang 1:.

7 Umfang der Protokollierung

Auch für die Gestaltung von Protokollierungsverfahren gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.

Die Erforderlichkeit der verarbeiteten Daten wird in den Anhängen dargestellt:

- IHE ATNA: Anhang 1:
- DIN EN ISO 27789: Anhang 2:

8 Lebenszyklus der personenbezogenen Daten

8.1 Erzeugung

Protokolldaten werden bei der Nutzung einer IT-Anwendung automatisch generiert. Bestimmte Ereignisse („trigger events“) lösen eine Protokollierung aus. Z. B. kann die Suche nach einem bestimmten Patienten oder die Suche nach Patienten mit bestimmten Erkrankungen ein entsprechendes Ereignis darstellen. Auch die Nutzung administrativer Rechte ist ein eine Protokollierung auslösendes Ereignis.

Die Inhalte der Protokollierung hängen vom Ereignis ab und sind in den Anhängen dargestellt:

- IHE ATNA: Anhang 1:

[37] Ströbel L, Böhm WT, Breunig C, Wybitul T (2018) Beschäftigtendatenschutz und Compliance: Compliance-Kontrollen und interne Ermittlungen nach der EU-Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz. CCZ: 14-21

[38] Maschmann F. (2018) Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht. NZA-Beilage: 115-124

[39] GMDS, bvitg, GDD: Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen. [Online] 2020 [Zitiert 2020-08-31] Verfügbar unter https://gesundheitsdatenschutz.org/html/loeschkonzept.php

- DIN EN ISO 27789: Anhang 2:

8.1.1 Protokollierung administrativer Tätigkeiten

Es werden alle Ereignisse und Tätigkeiten protokolliert, welche die Funktionsweise der IT-Systeme – sei es Hard-, Software oder auch Archivsysteme – beeinflussen bzw. verändern. Dazu ist es erforderlich, dass Administratortätigkeiten unter Nutzung einer personalisierten Kennung durchgeführt werden; Sammel- oder Gruppenkennungen dürfen nicht genutzt werden. Weiterhin muss verhindert werden, dass ein ändernder Zugriff auf die Protokolldaten durch diejenigen Personen stattfinden kann, deren Tätigkeiten durch die Protokolldaten dokumentiert werden.

Wenn aus wichtigen, nachvollziehbar zu dokumentierenden Gründen keine persönlichen Kennungen verwandt werden können, muss auf anderem Wege sichergestellt werden, dass nachvollziehbar ist, wer zu einem bestimmten Zeitpunkt mit der Kennung gearbeitet hat und für die entsprechenden Aktionen verantwortlich ist. Das Verfahren der Identifikation ist im Protokollierungskonzept festzuhalten und die Umsetzbarkeit regelmäßig zu überprüfen; das Prüfergebnis muss festgehalten und bei Bedarf vorgelegt werden.

Die Protokollierung dient insbesondere auch zum Schutz der Administratoren vor unberechtigten Vorwürfen hinsichtlich eines möglichen Missbrauchs.

8.1.2 Protokollierung der Nutzung von IT-Systemen – Empfehlungen der deutschen Aufsichtsbehörden

Entsprechend den Empfehlungen der deutschen Aufsichtsbehörden[40] muss eine Protokollierung mindestens folgende Angaben umfassen:

- Anmeldung am Verfahren (Login/Logout),
- Zeitpunkt des Zugriffs,
- Kennung des jeweiligen Benutzers,
- Kennung der jeweiligen Arbeitsstation,
- aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung),
- betroffene Patienten/Behandlungsfälle.

Wird eine Suche in einem Datenbestand durchgeführt, so soll ein Protokoll entsprechend den Empfehlungen der deutschen Aufsichtsbehörde weiterhin mindestens die nachfolgenden Informationen beinhalten:

- Verwendete Such- bzw. Abfragekriterien (z. B. Patientennummer, Fallnummer, Name, Geburtsdatum, Wohnort, Diagnose etc.),
- Angaben zum Ergebnis der Abfrage (z. B. Zahl der Trefferfälle,
- Fallnummern, Kennung der angezeigten Bildschirmmaske),
- etwaige Folgeaktionen bzw. Navigationsschritte (z. B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).

In wieweit die Empfehlungen des sogenannten „Düsseldorfer Kreises“ auf das Protokollierungskonzept des jeweiligen IT-Systems anwenden lassen oder für den im Protokollierungskonzept beschriebenen Vorgang sinnvoll sind, kann letztlich nur in diesen

[40] Arbeitskreise „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe Krankenhausinformationssysteme, 2. Fassung März 2014. Teil 2, Abschnitt 7.10. [Online] 2020 [Zitiert 2020-06-04] Verfügbar unter https://www.datenschutzzentrum.de/uploads/medizin/OH_KIS.pdf

Einzelfällen beurteilt werden. Die Verantwortlichen, insbesondere in Krankenhäusern, sollten sich jedoch bzgl. den Empfehlungen der deutschen Aufsichtsbehörden Gedanken machen, um bei Nachfragen der für sie zuständigen Aufsichtsbehörde ggf. erklären zu können, warum die eine oder andere Anforderung nicht umgesetzt wurde.

Beispielsweise kann eine sehr umfangreiche Protokollierung, wie sie die Vorgaben zur Protokollierung bei einer Suche im Datenbestand darstellen, auch einen Verstoß gegen die in Art. 5 Abs. 1 lit. c DS-GVO enthaltene gesetzliche Pflicht zur Datenminimierung darstellen und daher ggf. nicht in der vom Düsseldorfer Kreis empfohlenen Art und Weise durchgeführt werden.

8.2 Speicherung

Protokolldaten müssen in einer Form gespeichert werden, welche gewährleistet, dass

a) Protokolldaten nicht nachträglich verändert werden können und
b) Nur berechtigte Personen Zugriff auf die Protokolldaten haben.

8.3 Übertragung

Ggf. findet die Übertragung von Protokolldaten auf einen speziell vor Zugriffen geschützten Protokollserver statt. In diesem Fall ist der Vorgang der Übertragung wie auch die weitere Verarbeitung hier zu beschreiben.

8.4 Nutzung von Protokolldaten, Auswertung

Da Protokolldaten geeignet sind, das Verhalten oder die Leistung von Beschäftigten zu überwachen, sind die Mitbestimmungsrechte der Personalvertretungen zu berücksichtigen. Die Art und Weise der Auswertung von Protokolldaten und die an der Auswertung Beteiligten sollten daher in einer Dienst- oder Betriebsvereinbarung geregelt werden.

Auswertungen dürfen entsprechend der in Kapitel 4 dargestellten genannten Zweckbindung grundsätzlich nur zu den beschriebenen Zwecken erfolgen:

1) Erteilung einer Auskunft auf Antrag einer betroffenen Person
2) Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung
3) Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten
4) Gewährleistung der Sicherheit der Verarbeitung
5) Gewährleistung der Verfügbarkeit der Anwendung.

Die Auswertung personenbezogener Protokolldaten soll dabei immer im Vier-Augen-Prinzip, unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung der bzw. des Datenschutzbeauftragten erfolgen. Dient die Auswertung der Gewährleistung der Sicherheit der Verarbeitung oder der Gewährleistung der Verfügbarkeit der Anwendung sollte, sofern vorhanden, der IT-Sicherheitsbeauftragte und/oder der Informationssicherheitsbeauftragte einbezogen werden.

8.5 Löschung

Die Datenschutz-Aufsichtsbehörden empfahlen 2009 in ihrer OH Protokollierung[41] hinsichtlich der Speicherdauer von Protokolldaten u. a.:

- Festlegung der Aufbewahrungsdauer für jedes Protokolldatum vor der Erzeugung; Länge der Aufbewahrungsdauer wird bestimmt durch den Auswertungszyklus:
- Maßstab für Speicherdauer der Protokolldaten ist die „Erforderlichkeit der Aufgabenerfüllung".

Entsprechend der in der Orientierungshilfe Protokollierung dargestellten Ansicht der Datenschutz-Aufsichtsbehörden kann basierend auf diesen Kriterien als Speicherdauer von Protokolldaten wenige Tagen bis hin zu mehreren Monaten als zweckmäßig und akzeptabel angesehen werden.

Eine gesetzliche Vorgabe für die Speicherdauer von Protokollen existiert nicht, aber im 3. Teil des BDSG, welcher der Umsetzung der Richtlinie (EU) 2016/680 dient, findet sich in § 76 Abs. 4 BDSG die Verpflichtung „Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen". Da diese Regelung für Protokolle, welche für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung angelegt wurden, gilt, kann diese Regelung - auch wenn sie nicht der Umsetzung der DS-GVO dient - im Sinne einer Analoginterpretation genutzt werden und diese Speicherdauer für Löschprotokolle angesetzt werden.

Ein anderer Ansatzpunkt zur Bestimmung der Speicherdauer besteht in der Ableitung aus dem Recht der Ordnungswidrigkeiten: Nach § 41 BDSG gelten für Bußgelder, die nach Art. 83 DS-GVO verhängt werden (sollen), die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Entsprechend § 31 Abs. 2 OWiG verjährt die Verfolgung von Ordnungswidrigkeiten in drei Jahren bei Ordnungswidrigkeiten, die mit Geldbuße im Höchstmaß von mehr als fünfzehntausend Euro bedroht sind, wobei die Verjährung beginnt, sobald die Handlung beendet ist. Diese Regelung kann man dahingehend interpretieren, dass eine Aufsichtsbehörde eine Löschung nicht länger als drei Jahre verfolgen und dementsprechend auch keinen Nachweis bzgl. Löschung fordern kann. Somit wäre auch eine Speicherdauer von Löschprotokollen von drei Jahren als angemessen anzusehen.

Wird in dem Konzept unter Zweckbestimmung aufgeführt, dass die Protokollierung dazu dient, einer betroffenen Person Auskunft zu geben, wer auf ihre Daten zugegriffen hat, müssen die Protokolldaten solange aufbewahrt werden, wie eine Auskunftserteilung auf Anfragen von betroffenen Personen, d. h. in diesem Fall der Patienten, als angemessen anzusehen ist; im Sinne von ErwGr. 63 DS-GVO muss immer auch die Angemessenheit berücksichtigt werden. Weiterhin sollen entsprechend ErwGr. 63 DS-GVO bei einer Beauskunftung die Rechte und Freiheiten anderer Personen nicht beeinträchtigen werden, d. h. Beschäftigtendaten dürfen hier nur im erforderlichen Maß verarbeitet werden. Bei einer Protokollierung werden immer die Grundrechte anderer Personen, insbesondere die der Beschäftigten, verletzt und dies darf somit nur auf Basis einer gesetzlichen Grundlage erfolgen, was dementsprechend natürlich auch für die Speicherung der Protokolldaten zum Zwecke der Auskunftserteilung gilt. Ergänzend muss, wie bei jeder Verarbeitung, insbesondere auch Art. 5 DS-GVO bzgl. der Verarbeitung von Beschäftigtendaten beachtet werden, woraus u. a. folgt, dass die Daten der Beschäftigten nur für eine zwingend notwendige Zeitspannen gespeichert dürfen werden.

[41] AK „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: „OH Protokollierung", Kap. 6.5. [Online] 2009 [Zitiert 2020-08-09] Verfügbar unter http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Protokollierung.pdf?__blob=publicationFile&v=3

Der Nachweis, dass personenbezogene Daten vom Verantwortlichen ordnungsgemäß verarbeitet wurden, erfolgt regelhaft durch die dokumentierten Prozesse, deren Einhaltung durch Prüfungen nachgewiesen wurden, nicht jedoch durch die Protokolldaten. Insbesondere unter Berücksichtigung des Urteils des Europäischen Gerichtshofs für Menschenrechte (ECHR Application No. 20511/03[42]), der ein entsprechendes Berechtigungskonzept für eine Beauskunftung hinsichtlich des berechtigten Zugriffs auf Patientendaten als ausreichend ansah, muss daher die Angemessenheit bewertet werden, wenn für einen über mehrere Jahre zurückreichende Auskunft bzgl. der die Daten verarbeitenden Beschäftigten verlangt wird. Auch bei einer Speicherung von Protokolldaten zum Zwecke der Auskunftserteilung gilt: schnellstmögliches Löschen ist gesetzliche Pflicht, und der Verantwortliche muss nachweisen, dass eine Speicherung aus rechtlichen Gründen erforderlich ist/war.

[42] Right to Privacy Requires Strict Controls, Safeguards and Protection of Health Information. I v Finland. ECHR 20511/03 [Online] 2008 [Zitiert 2020-06-20] Verfügbar unter http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf

9 Verarbeitung von Protokolldaten

Für jeden Verarbeitungszweck muss festgelegt sein, wer welche Protokolldaten zu diesen Zwecken verarbeiten darf. Die Zwecke wurden in Abschnitt 3 dargestellt, in den folgenden Abschnitten wird die Verarbeitung dargestellt.

Grundsätzlich ist zu beachten, dass die in Art. Abs. 2 DS-GVO geforderte Rechenschaftspflicht auch für die Verarbeitung von Protokolldaten erfüllt werden muss. D. h. für jede Verarbeitung von Protokolldaten muss auch sowohl die Verarbeitung selbst wie auch evtl. aus der Verarbeitung resultierende Ergebnisse festgehalten werden.

9.1 Erteilung einer Auskunft auf Antrag einer betroffenen Person

In einem Urteil des Europäischen Gerichtshofs für Menschenrechte aus dem Jahr 2008 (ECHR Application No. 20511/03[43]) im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems wird in Absatz 44 der Urteilsbegründung[43] dargestellt, dass medizinische Daten zu schützen sind, sei es durch ein entsprechendes Berechtigungskonzept oder durch entsprechende Protokollierung („... control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file ...").

D. h. wenn eine betroffene Person von ihrem Recht auf Auskunft wahrnimmt, gehört zur Auskunft ggf. der Nachweis, dass kein unberechtigter Zugriff erfolgte. Dies kann regelhaft unter Zuhilfenahme der Protokolldaten nachgewiesen werden.

9.2 Stichprobenartige Datenschutzkontrolle

Bei einer stichprobenartigen Kontrolle geht es um die Überprüfung, dass die Verarbeitung, bei welcher die Protokolldaten anfielen, entsprechend den Vorgaben erfolgt. Grundlage bilden daher stets alle Protokolle, die bei der Verarbeitung anfielen. Die Protokolle werden dabei auf auffällige Ereignisse untersucht, Beispiele hierfür finden sich in Anhang 3:.

Im Protokollierungskonzept muss dabei das zeitliche Intervall festgelegt werden, in welchen diese Routineprüfungen stattfinden. Da es sich bei Gesundheits- oder genetischen Daten stets um sensible Daten mit einem hohen bzw. sehr hohen Schutzbedarf handelt, sollte das Intervall dies auch widerspiegeln. Eine halbjährliche Prüfung dürfte i. d. R. angemessen sein, bei der Einführung neuer Verfahren sind natürlich deutlich kürzere Prüfungen erforderlich.

Bei der stichprobenartigen Kontrolle ist, wann immer aufgrund der technischen Umstände möglich, eine pseudonymisierte Auswertung durchzuführen. Erst wenn konkrete Anhaltspunkte vorliegen, deren Überprüfung die Identifizierung von Personen erfordern, ist ein Personenbezug herzustellen.

9.2.1 Stichprobenartige Datenschutzkontrollen des Datenschutzbeauftragten

Eine stichprobenartige Prüfung ist entsprechend Art. 39 Abs. 1 lit. b DS-GVO Aufgabe der oder des Datenschutzbeauftragten. Allerdings muss auch beim Datenschutzbeauftragten das 4-Augen-Prinzip bei der Nutzung von Protokolldaten gelten, d. h. es muss eine zweite Person, die als unabhängige Kontrollstelle fungiert, die Auswertung der Protokolldaten durch den Datenschutzbeauftragten beobachten und eine ggf. erfolgende zweckfremde Nutzung der Protokolldaten verhindern.

[43] Right to Privacy Requires Strict Controls, Safeguards and Protection of Health Information. I v Finland. ECHR 20511/03 [Online] 2008 [Zitiert 2020-06-20] Verfügbar unter http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf

9.2.2 Stichprobenartige Datenschutzkontrollen des Verantwortlichen

In einem Patientendaten führenden System, insbesondere einem Krankenhausinformationssystem, hat die Protokollierung aufgrund des hohen Schutzbedarfs der Patientendaten eine besondere Bedeutung. Die Orientierungshilfe Krankenhausinformationssysteme (OH KIS) verlangt daher im Rahmen des datenschutzkonformen Einsatzes eines Krankenhausinformationssystems die aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe inklusive der Implementierung geeigneter Auswertungsmöglichkeiten[44]. Die Protokollierung dient dem Verantwortlichen sowohl als vorbeugende Maßnahme durch Kontrolle der Zugriffe, gleichermaßen auch als Maßnahme zur Nachweisbarkeit der datenschutzkonformen Verarbeitung[45]. Die in diesem Zusammenhang geforderte „stichprobenweise anlassunabhängige (Plausibiltitäts-)Kontrolle“ fällt in den Aufgabenbereich des Verantwortlichen.

Analog zur OH KIS kann eine Protokollierung der lesenden Zugriffe nur dann reduziert werden, wenn ein hinreichend differenziertes Rollen- und Berechtigungskonzept vorhanden ist, das dem Schutzbedarf der Daten Rechnung trägt[46]. Daher ist ein völliger Verzicht der Protokollierung und Kontrolle lesender Zugriffe in einem Krankenhausinformationssystem im Hinblick auf implementierte Sonderzugriffsberechtigungen und sonstige Zugriffsrechte außerhalb des Behandlungskontextes nicht realistisch datenschutzkonform umsetzbar.

Sofern stichprobenweise anlassunabhängige Kontrollen durch den Verantwortlichen umgesetzt werden, sind die damit erfolgenden geeigneten Auswertungen zu beschreiben. Die Untersuchung einer Stichprobenauswahl dient dem Verantwortlichen dazu, Rückschlüsse von deren Ergebnissen auf die Grundgesamtheit der Protokolldaten ziehen zu können, ohne sie insgesamt untersuchen zu müssen. Wird die Stichprobenauswahl in geeigneter Weise festgelegt, so gilt eine solche Stichprobe als repräsentativ und lässt den induktiven Schluss auf die Grundgesamtheit zu. Unterschieden werden eine zufällige Stichprobenauswahl von nichtzufälligen Auswahlverfahren. Ein bewusstes Auswahlverfahren könnte zum Beispiel in einem KIS in der Analyse aller Sonderzugriffe/Notfallzugriffe einer Station oder eines bestimmten Zeitintervalls bestehen. Bei einer Zufallsstichprobe wird hingegen eine hinreichend große Auswahl Datensätze mittels eines Zufallsgenerators bestimmt und analysiert.

Zu bestimmen sind weiterhin der minimal erforderliche Stichprobenumfang sowie die Häufigkeit, mit der eine Stichprobe genommen und untersucht werden sollte. Diesbezüglich sind weder aus der OH KIS noch aus sonstigen Veröffentlichungen der deutschen Aufsichtsbehörden Anforderungen bekannt. Die niederländische Aufsichtsbehörde hat sich in einem Untersuchungsbericht dahingehend geäußert, dass eine Kontrolle regelmäßig, systematisch und konsequent erfolgt[47]. Eine stichprobenartige Kontrolle von sechs Patientenakten jährlich wurde als nicht ausreichend bewertet.

---

[44] Orientierungshilfe Krankenhausinformationssysteme, 2. Fassung, Stand März 2014, Teil I Tz. 43, Teil II Tz. 7.1. [Online] 2004 [Zitiert 2020-08-01] Verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/201403_oh_krankenhausinformationssysteme.pdf

[45] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: 28. TB Datenschutz 2019 – HmbBfDI S. 34. [Online] 2020 [Zitiert 2020-08-01] Verfügbar unter https://datenschutz-hamburg.de/taetigkeitsberichte/TB-D-2019/

[46] Orientierungshilfe Krankenhausinformationssysteme, 2. Fassung, Stand März 2014,Teil II, Tz. 7.3. [Online] 2004 [Zitiert 2020-08-01] Verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/201403_oh_krankenhausinformationssysteme.pdf

[47] Autoriteit Persoonsgegevens, Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis; Definitief rapport 2019, S. 20 [Online] 2019 [Zitiert 2020-08-01] Verfügbar unter https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga_rapport_def.pdf

Die Österreichische Datenschutzbehörde hat in einer Empfehlung zur angemessenen Stichprobe bei der Zugriffskontrolle in einem Klinikum festgestellt, dass „angesichts der Größe des Klinikums ** eine Stichprobengröße von vier bis sechs Patienten je Monat zu gering, um eine verlässliche Kontrolle zu gewährleisten, die besonders schützenswerte Personengruppen (wie insbesondere eigene Bedienstete oder deren Angehörige bzw. öffentlich bekannte Personen), die sich einer Behandlung unterziehen (müssen), vor unberechtigten Zugriffen zu schützen.“[48] Bedauerlicherweise liegen keine Informationen über die Größe des Klinikums vor.

Analog zu § 1 Abs. 2 DlStatG kann zumindest eine Höchstgrenze bei höchstens 15 Prozent aller Erhebungseinheiten angesehen werden[49].

Die Konzeption der stichprobenweisen anlasslosen Kontrollen sollte sich daher am Risiko für die betroffenen Personen orientieren und anhand der Parameter

- Stichprobenart
- Stichprobenauswahlverfahren
- Stichprobenumfang
- Taktung/Häufigkeit der Kontrollen p. a.

beschrieben werden. Die Statistik kennt Verfahren, um den Umfang der erforderlichen Stichprobenanzahl in Abhängigkeit von der gewünschten Aussagekraft der stichprobenartigen Kontrolle zu ermitteln[50].

Damit geht einher, dass beispielsweise Kontrollen für Notfallzugriffe, bzw. bzgl. Zugriffen auf ggf. stigmatisierende Daten psychische oder sexuell übertragbare Erkrankungen sowie auf Betroffenenkreise mit erhöhtem Schutzbedarf (im öffentlichen Interesse stehende Personen, Mitarbeiter als Patienten) ggf. häufiger angesetzt werden als die Zufallskontrollen im Normalbetrieb.

9.3 Prüfung bei Verletzung des Schutzes personenbezogener Daten

Gemäß Art. 33 Abs. 5 DS-GVO muss der Verantwortliche alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller mit dieser Verletzung im Zusammenhang stehenden Fakten dokumentieren. Dies ist nur unter Nutzung der Protokolldaten möglich, da nur hier festgehalten ist, wer wann von wo auf welche Daten zugegriffen hat.

Gibt es einen Verdacht auf die Verletzung des Schutzes der personenbezogenen Daten, kann der Verantwortliche die Protokolldaten nutzen, um den Sachverhalt zu klären.

Gibt es eine betrieblich notwendige „Schwachstelle“ in den Schutzmaßnahmen wie z. B. die Möglichkeit eines Notfallzugriffs mit erweiterten Zugriffsrechten durch spezielle Mitarbeiter, muss hier eine regelhafte Prüfung der entsprechenden Protokolldaten beschrieben werden.

[48] Österreichische Datenschutzbehörde GZ: DSB-D213.471/0005-DSB/2016 vom 31.1.2017 [Zitiert 2020-08-14] Verfügbar unter https://www.ris.bka.gv.at/JudikaturEntscheidung.wxe?Abfrage=Dsk&Dokumentnummer=DSBT_20170131_DSB_D213_471_0005_DSB_2016_00

[49] Gesetz über Statistiken im Dienstleistungsbereich (Dienstleistungsstatistikgesetz - DlStatG). [Online] 2015 [Zitiert 2020-08-15] Verfügbar unter https://www.gesetze-im-internet.de/dlstatg/index.html#BJNR176510000BJNE000100305

[50] Einen Hinweis zum Vorgehen findet man im Aufsatz von Berg/Bihler zum Zensus 2011. [Online] 2011 [Zitiert 2020-08-01] Verfügbar unter https://www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2011/04/stichprobendesign-42011.pdf?__blob=publicationFile

9.4 Gewährleistung der Sicherheit der Verarbeitung

Entsprechend Art. 32 Abs. 1 lit. d DS-GVO ist es zur Gewährleistung der Sicherheit der Verarbeitung erforderlich, dass ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Um die Einhaltung der Vorgaben des Berechtigungskonzeptes zu prüfen, muss zwingend eine Protokollierung der Zugriffe sowie eine stichprobenartige Kontrolle erfolgen. Auch unberechtigte Zugriffe bzw. Zugriffsversuche können nur durch eine Protokollierung sowie eine entsprechende Auswertung der Protokolldateien festgestellt werden.

Die somit letztlich gesetzliche geforderte Protokollierung muss aber durch im Protokollierungskonzept beschriebene Auswertungen begleitet werden, damit die Nutzung der Protokolldaten für betroffene Personen – insbesondere auch Beschäftigte – transparent erfolgt. Das Bundesamt für Sicherheit in der Informationstechnik sieht in einer Protokollierung eine Grundlage für die Gewährleistung eines verlässlichen IT-Betriebes[51].

9.5 Gewährleistung der Verfügbarkeit der Anwendung

Art. 32 Abs. 1 lit. b DS-GVO fordert die dauerhafte Sicherstellung der Verfügbarkeit der zur Verarbeitung personenbezogener Daten eingesetzten Systeme und Dienste. Das Schutzziel Verfügbarkeit wird dann eingehalten, wenn gewährleistet ist, dass die Systeme jederzeit betriebsbereit sind und die Verarbeitung der Daten korrekt abläuft.

Hierzu ist insbesondere bei vernetzten IT-Geräten der Ressourcenverbrauch sowie die Auslastung der Systeme und Dienste zu überwachen, damit für die Datenübertragung eine ausreichende Bandbreite zur Verfügung steht. Somit muss sowohl die Anzahl der Anwender als auch die Menge an Daten im zeitlichen Verlauf überwacht und hinsichtlich der Anforderung an die Netzwerkleistung bewertet werden. Aber auch innerhalb von Systemen und Diensten ist ein entsprechendes Monitoring erforderlich, z. B. damit für die Anzahl Anwender auch eine ausreichende Anzahl an Datenbanklizenzen zur Verfügung stehen.

Im Protokollierungskonzept muss festgehalten werden, welches Monitoring mittels einer Protokollierung zur Gewährleistung der Verfügbarkeit eingesetzt wird.

10 Sicherheit der Verarbeitung

10.1 Vertraulichkeit: Nur berechtigte Anwender

Unbefugten ist der Zutritt zu Räumlichkeiten, aus denen heraus ein physikalischer Zugriff auf die Server mit den Protokollierungsdateien möglich ist, zu verwehren. Daher ist festzulegen, welche Voraussetzung eine Person erfüllen muss, um Zutritt zu erhalten. Der Kreis der Berechtigten ist auf das notwendige Minimum zu beschränken.

Nur berechtigte Personen dürfen Zugriff auf die Protokolldaten erhalten. Es muss daher ein Berechtigungs- und Rollenkonzept erstellt und gepflegt werden, aus dem eindeutig abzulesen ist, wer welche Rolle (funktionell und/oder strukturell) und die mit der Rolle verbundene Rechte bzgl. des

[51] Bundesamt für Sicherheit in der Informationstechnik (BSI: IT-Grundschutz Kompendium - OPS.1.1.5 Protokollierung. [Online] 2020 [Zitiert 2020-06-04] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html

Zugriffs auf die Protokolldaten hat. Bzgl. der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept ist zwingend das Need-to-know-Prinzip anzuwenden.

10.2 Integrität: Manipulationssichere Erzeugung und Speicherung

Das protokollierende System bzw. der/die Server muss gegen Manipulationsmöglichkeit geschützt werden. Dies kann u. a. durch den Einsatz entsprechender Sicherheitssysteme wie Virenscanner, Firewalls, Intrusion-Detection-System oder auch Intrusion-Prevention-System erfolgen.

Idealerweise werden bei der Erzeugung kryptographische Hashwerte erzeugt, sodass nachträgliche Manipulationen der Protokolldaten zuverlässig erkannt werden können. Dabei muss sichergestellt werden, dass bei Verwendung von Hash-Funktionen ein Salt benutzt und dieser geheim gehalten wird. Und natürlich dürfen ausschließlich Standard-Hash-Funktionen verwendet werden, für die es keine bekannten Schwachstellen gibt.

Im Idealfall werden die Protokolldaten bei der Erzeugung direkt auf einem WORM-Medium, welches das Löschen, Überschreiben und Ändern von Daten dauerhaft ausschließt, gespeichert. Häufig werden Protokolldaten jedoch in temporären Blöcken verarbeitet, sodass in diesen Fällen erst eine spätere Übertragung von Protokolldaten auf einem entsprechenden Medium möglich ist. Dabei erscheint die Nutzbarkeit eines Software-WORMs ausreichend für den Schutz von Protokolldaten.

10.3 Verfügbarkeit

Um die Verfügbarkeit der Protokolldaten zu gewährleisten, müssen die Daten insbesondere regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept vorhanden sein, das befugte Personen in die Lage versetzt, die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung zu stellen.

Backups müssen dabei regelmäßig auf Datenvollständigkeit kontrolliert werden, desgleichen muss regelmäßig überprüft werden, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist.

10.4 Auditierung der Einhaltung dieser Vorgaben

Verantwortliche müssen die Sicherheitsmaßnahmen nicht nur einmalig planen und umsetzen, sie müssen die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen und ggf. die Maßnahmen anpassen[52] („Überprüfung, Bewertung und Evaluierung der Wirksamkeit“). Art. 32 Abs. 1 lit. d DS-GVO fordert vom Normadressaten letztlich die Etablierung eines Prozesses, der einen Demingkreis bestehend aus den Komponenten „Plan – Do – Check – Act“ abbildet[53].

Dabei wird die „Regelmäßigkeit“ nicht vom Normgeber konkret vorgegeben, sondern muss vom jeweiligen Normadressaten entsprechend der jeweiligen Notwendigkeit festgelegt werden.

10.5 Pseudonymisierung

Art. 32 DS-GVO verlangt, dass Pseudonymisierung hinsichtlich der zu ergreifenden Maßnahmen berücksichtigt werden muss. Dies heißt nicht, dass immer eine Pseudonymisierung durchgeführt werden muss. Aber im Zweifelsfall muss begründet werden, warum eine Pseudonymisierung nicht genutzt wird.

---

[52] Jandt S. Art 32 Rn. 29 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702

[53] Piltz C. Art. 32 Rn. 37 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

In einer Protokollierung wird regelhaft mit Identifikatoren („Identifiern“, abgekürzt „IDs“) gearbeitet, nicht mit Klarnamen. D. h. die Nutzung von Pseudonymisierung bei der Protokollierung ist eher die Regel als die Ausnahme. Dennoch kann es vorkommen, dass auch in Protokolldaten Klarnamen enthalten sind, z. B. wenn die konkrete Abfrage von Daten zu einem bestimmten Patienten im Protokoll gespeichert wird.

Zu beachten: Wird eine Pseudonymisierung eingesetzt, so verlangt Art. 4 Ziff. 5 DS-GVO, dass technische und organisatorische Maßnahmen gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

11 Inkrafttreten

Mit dem Zeitpunkt des Inkrafttretens beginnt grundsätzlich die Wirksamkeit, d. h. die Geltung der Regelungen. Um den Anwender zu verdeutlichen, ab wann sie bzw. er die Regelungen zu beachten hat, gehört ein entsprechender Abschnitt in jedes Protokollierungskonzept; dies folgt aus dem Gebot der Rechtsklarheit.

12 Abkürzungen

Abs.	Absatz
Art.	Artikel (Einzahl)
Artt.	Artikel (Mehrzahl)
ATNA	Audit Trail and Node Authentication
BbgDSG	Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz)
BDSG	Bundesdatenschutzgesetz
BlnDSG	Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz)
BremDSGVOAG	Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bvitg	Bundesverband Gesundheits-IT e. V.
DICOM	Digital Imaging and Communications in Medicine
DIN	Deutsche Institut für Normung e. V.
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt)
DS-GVO	Datenschutz-Grundverordnung
DSG	Datenschutzgesetz
ECHR	Europäischer Gerichtshof für Menschenrechte
EN	Europäische Norm
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HmbBfDI	Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
ID	Identifier, Identifikator
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
ISO	Internationale Organisation für Normung
IT	Informationstechnik, informationstechnisches…
KIS	Krankenhausinformationssystem
LDSG	Landesdatenschutzgesetz
lit.	littera (lat. „Buchstabe“)
NDSG	Niedersächsisches Datenschutzgesetz
OWiG	Gesetz über Ordnungswidrigkeiten
PHI	Protected health information
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz)
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SOP	Service-Object Pair (DICOM-Standard)
TLS	Transport Layer Security
TOM	Technisch-organisatorische Maßnahmen
WORM	„write once read many“ oder „write once read multiple“

13 Glossar

Begriff	Erklärung
Audit	Systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Audit-Trail	Chronologische Aufzeichnung der Aktivitäten von Nutzern eines Informationssystems, die die getreue Wiederherstellung früherer Zustände der betreffenden Informationen ermöglicht. (Quelle: DIN CEN ISO/TS 14265)
Aufzeichnung	Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt. (Quelle: DIN ISO IEC 27000)
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. (Quelle: DIN EN ISO 22600-1)
Authentisierung, starke	Siehe „starke Authentisierung“
Autorisierung	Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen. (Quelle: DIN EN ISO 22600-1)
Beschäftigte	Beschäftigte sind: 1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher, 2. zu ihrer Berufsbildung Beschäftigte, 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden), 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte, 5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten, 6. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten, 7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte. (Quelle: § 26 Abs. 8 BDSG)
Betroffener	Betroffener ist eine Bezeichnung eines Menschen, der betroffen ist von einer Sache. Im Sinne des Datenschutzes ist ein Betroffener eine bestimmte oder bestimmbare natürliche Person, zu welcher Daten über persönliche oder sachliche Verhältnisse beziehbar sind (Art. 4 Ziff. 1 DS-GVO)
Datenlöschung	Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt. (Quelle: DIN CEN ISO/TS 14265)

Begriff	Erklärung
Datenschutzkontrolle	Technische und organisatorische Maßnahmen, die dazu dienen, Risiken zu minimieren, die zu Datenschutzverletzungen führen könnten (Quelle: DIN CEN ISO/TS 14265)
Datenschutzverletzung	Situation, in der Daten einer Person auf illegale Weise oder unter Verletzung einer oder mehrerer relevanter Datenschutzbestimmungen verarbeitet wurde (Quelle: DIN CEN ISO/TS 14265)
Entität	Natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Identifikation	Erkennung einer Person in einem bestimmten Bereich mithilfe einer Reihe ihrer Attribute. (Quelle: DIN CEN ISO/TS 14441)
Identifizierbare Person	Person, die direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind. (Quelle: DIN EN 14484)
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen. (Quelle: DIN EN ISO 22600-1)
Korrekturmaßnahme	Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation. (Quelle: DIN ISO IEC 27000)
Maßnahme	Mittel zum Management von Risiken, einschließlich von Leitlinien, Verfahren, Richtlinien, Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können. (Quelle: DIN ISO IEC 27000)
Maßnahmenziel	Beschreibung, was durch die Umsetzung von Maßnahmen als Ergebnis erreicht werden soll. (Quelle: DIN ISO IEC 27000)
Notfallzugriff	Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen. (Quelle: DIN CEN ISO/TS 14265)
Protokolldaten	Jedes Datum, welches im Rahmen einer Protokollierung erhoben wird.
Protokollierung	Eine Aufzeichnung, welche mindestens den Zeitpunkt, die ausgeführte Handlung und den Handelnden beinhaltet
Pseudonymisieren	Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Ziff. 5 DS-GVO)

Begriff	Erklärung
Revisionssicherheit	Der Begriff „Revisionssicherheit“ bezieht sich die Anforderungen a) des Handelsgesetzbuches (§§ 239, 257 HGB) b) der Abgabenordnung (§§ 146, 147 AO), c) der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) d) ... d. h., auf praktisch ausnahmslos steuerrechtliche bzw. handelsrechtliche Vorgaben. Andere gesetzlichen Vorgaben werden hierbei nicht beachtet. Die revisionssichere Archivierung ist nur ein Bestandteil der rechtssicheren Archivierung. So beinhaltet eine revisionssichere Archivierung beispielsweise keine datenschutzrechtlichen Vorgaben, z. B. bzgl. des Zugriffs auf die archivierten Daten. Hingegen beinhaltet eine revisions- und rechtssichere Archivierung auch alle rechtlichen Anforderungen.
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen (Quelle: DIN EN ISO 22600-1)
Starke Authentisierung	Authentisierung mittels kryptographisch abgeleiteter multifaktorieller Identitätsnachweise. (Quelle: DIN EN ISO 22600-1)
Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden (Art. 4 Ziff. 7 DS-GVO)
Verfügbarkeit	Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein (Quelle: DIN EN ISO 22600-1)

14 Literatur

14.1 Datenschutz-Aufsichtsbehörden

- Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe „Protokollierung“. [Online] 2009 [Zitiert 2020-06-04] Verfügbar unter https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Protokollierung.pdf?__blob=publicationFile&v=4 1f
- Arbeitskreis Gesundheit und Soziales / Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: „Empfehlung zur Protokollierung in zentralen IT-Verfahren der gesetzlichen Krankenversicherung“. [Online] 2010 [Zitiert 2020-06-04] Verfügbar unter https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_ProtokollierungshilfeGKV.pdf?__blob=publicationFile&v=4
- Arbeitskreise „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe Krankenhausinformationssysteme, 2. Fassung März 2014. Teil 2, Abschnitt 7.10. [Online] 2014 [Zitiert 2020-06-04] Verfügbar unter https://www.datenschutzzentrum.de/uploads/medizin/OH_KIS.pdf

14.2 Internet, sonstige

- Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium Edition 2020 - OPS.1.1.5 Protokollierung. [Online] 2020 [Zitiert 2020-06-04] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen. [Online] 2018 [Zitiert 2020-07-06] Verfügbar unter https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/PDCA/PDCA.html

14.3 Normen

- Digital Imaging and Communications in Medicine (DICOM): Suppl. 95 „Audit Trail Messages“. [Online] 2009 [Zitiert 2020-06-04] Verfügbar unter https://www.dicomstandard.org/supplements/ bzw. direkt pdf-Datei unter ftp://medical.nema.org/medical/dicom/final/sup95_ft.pdf
- Digital Imaging and Communications in Medicine (DICOM): DICOM PS3.15 2020b – „Security and SystemManagement Profiles“, Abschnitt „A.5 Audit Trail Message Format Profile“. [Online] 2020 [Zitiert 2020-06-04] Verfügbar unter https://www.dicomstandard.org/current/ bzw. direkt pdf-Datei unter http://dicom.nema.org/medical/dicom/current/output/pdf/part15.pdf
- DIN EN ISO 27789: Audit-Trails für elektronische Gesundheitsakten. (Stand: 2013-06)
- RFC 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-06-04] Verfügbar unter https://www.rfc-editor.org/info/rfc3881

14.4 Zeitschriften

- Arasteh AR, Debbabi M, Sakha A, Saleh M. (2007) Analyzing multiple logs for forensic evidence. Digital Investigation: S82-S91 (https://doi.org/10.1016/j.diin.2007.06.013)
- Azkia et al. (2015) Deployment of a posteriori access control using IHE ATNA. Int. J. Inf. Secur.: 471–483 (https://doi.org/10.1007/s10207-014-0265-6)
- Baldwin A, Shiu S. (2005) Enabling shared audit data. Int J Inf Secur: 263–276 (https://doi.org/10.1007/s10207-004-0061-9)
- Behrendt H. (2006) Protokollierung in der Praxis - Datenschutzvorschriften richtig umsetzen. DuD: 298-300
- Bizer J. (2006) Das Recht der Protokollierung. DuD: 270-273
- Coenen C, Dreger U. (2006)Einführung eAkte – Herausforderung Protokollierung. DuD: 301-303
- Cruz-Correia et al. (2013) Analysis of the quality of hospital information systems audit trails. BMC Medical Informatics and Decision Making: 84 (http://www.biomedcentral.com/1472-6947/13/84)
- Czernik A. (2016) Software-Customizing datenschutzkonform umsetzen. ZD-Aktuell: 05029
- Gerhards R. (2009) Neuere Entwicklungen in der Syslog-Protokollierung. DuD: 723-727
- Gregg B, D_Agostino H, Toledo EG. (2006) Creating an IHE ATNA-Based Audit Repository. Journal of Digital Imaging: 307-315
- Hale M, Gamble R. (2017) Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. Requirements Engineering: 365–402 (https://doi.org/10.1007/s00766-017-0287-5)
- Heidrich J, Wegener C. (2015) Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten Problemfall Logging. MMR: 487-493
- Jaeger S. (2004)Wie viel Logfile ist erlaubt? Kes: 65
- Knorr M. (2006) Datenschutzkonforme Protokollierung. DuD: 268-269
- Kort M. (2011) Datenschutzrechtliche und betriebsverfassungsrechtliche Fragen bei IT-Sicherheitsmaßnahmen. NZA: 1319-1324
- Leopold N. (2006)Protokollierung und Mitarbeiterdatenschutz. DuD: 274-276
- Masi M, Pugliese R, Tiezzi F. (2012) Security Analysis of Standards-Driven Communication Protocols for Healthcare Scenarios. J Med Syst:3695–3711 (https://doi.org/10.1007/s10916-012-9843-1)
- Mannhardt et al. (2019) Privacy-preserving Process Mining: Differential - Privacy for Event Logs. Informatik Spektrum: 349-351
- Meints M. (2006) Protokollierung bei Identitätsmanagementsystemen. DuD: 304-307
- Meints M, Thomsen S. (2007) Protokollierung in Sicherheitsstandards. DuD: 749-751
- Leopold N. (2006) Protokollierung und Mitarbeiterdatenschutz. DuD: 274-276
- Piltz C. (2018) Die neuen Protokollierungspflichten nach der Richtlinie 2016/680/EU für öffentliche Stellen. NVwZ: 696-702
- Ringelstein C. (2007) Protokollierung in service-orientierten Architekturen. DuD:736-739
- Rost M. (2007) Funktion und Zweck des Protokollierens. DuD: 731-735
- Runge G. (1994) Protokolldateien zwischen Sicherheit und Rechtmäßigkeit. CR: 710-714
- Schaar P, Schläger U. (1993) Sicherheitsprotokollierung und Arbeitnehmerdatenschutz. CR: 435-439
- Schulte L, Wambach T. (2020) Zielkonflikte zwischen Datenschutz und IT-Sicherheit im Kontext der Aufklärung von Sicherheitsvorfällen. Datenschutz Datensich 44, 462–468

- Sürmeli J, Der U, Jähnichen S, Vogelsang A. (2017) Ein Rahmenwerk zur Protokollierung von Transaktionen in Distributed Ledgers. Informatik Spektrum 40, 595–601
- Thomsen S, Rost M. (2006) Zentraler Protokollservice. DuD: 292-294
- Wedde P. (2007) Protokollierung und Arbeitnehmerdatenschutz. DuD: 752-755
- Wolthusen S. (2006) Revisionssichere Protokollierung in Standardbetriebssystemen. DuD: 281-284
- Wolthusen S. (2007) Vertrauenswürdig Protokollierung. DuD: 740-743

Anhang 1: IHE ATNA

Audit Trail and Node Authentication (ATNA) wird im Technical Framework der Domäne IT Infrastructure (ITI) beschrieben[54]. ATNA spezifiziert für das „event audit logging“:

- Ein Standard-Schema zur Abbildung des Ereignisses.
- Zu protokollierende Standard-Ereignisse
  - Ereignisse, die Systemaktivitäten abbilden, z. B. „Login Fehlversuch“
  - Ereignisse, die zu IHE Transaktionen gehören; die Beschreibung hierzu findet sich in den jeweiligen Abschnitten des jeweiligen Technical Framework.
- Ein Audit Record Repository, wo Audit-Berichte gesammelt und ausgewertet werden.
- Zwei Alternativen, wie ein Ereignisbericht zu einem Audit Record Repository trans-portiert wird.

Anhang 1.1:Zu protokollierende Ereignisse bei IHE-Transaktionen

Die Ereignisse, die eine Ereignisprotokollierung auslösen, finden sich in IHE IT Infrastructure Technical Framework, Volume 2a Kapitel 3.20 (Abschnitt 4.1.1.1) in Tabelle Table 3.20.4.1.1.1-1 Audit Event triggers:

Audit Event Trigger	Description
Actor-start-stop	Startup and shutdown of any actor. Applies to all actors. Is distinct from hardware powerup and shutdown.
Audit-Log-Used	The audit trail repository has been accessed or modified by something other than the arrival of audit trail messages.
Begin-storing-instances	Begin storing SOP Instances for a study. This may be a mix of instances.
Health-service-event	Health services scheduled and performed within an instance or episode of care. This includes scheduling, initiation, updates or amendments, performing or completing the act, and cancellation.
Instances-deleted	SOP Instances are deleted from a specific study. One event covers all instances deleted for the particular study.
Instances-Stored	Instances for a particular study have been stored on this system. One event covers all instances stored for the particular study.
Medication	Medication orders and administration within an instance or episode of care. This includes initial order, dispensing, delivery, and cancellation.
Mobile-machine-event	Mobile machine joins or leaves secure domain.
Node-Authentication-failure	A secure node authentication failure has occurred during TLS negotiation, e.g., invalid certificate.
Order-record-event	Order record created, accessed, modified or deleted. Involved actors: Order Placer. This includes initial order, updates or amendments, delivery, completion, and cancellation.
Patient-care-assignment	Staffing or participant assignment actions relevant to the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a

[54] IHE International: Technical Frameworks - IT Infrastructure Technical Framework. [Online] 2019 [Zitiert 2020-06-04] Verfügbar unter https://www.ihe.net/resources/technical_frameworks/#IT

- Vol. 1: [Online] 2019 [Zitiert 2020-06-04] Verfügbar unter https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
- Vol. 2a: [Online] 2019 [Zitiert 2020-06-04] Verfügbar unter https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf

Audit Event Trigger	Description
	patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment.
Patient-care-episode	Specific patient care episodes or problems that occur within an instance of care. This includes initial assignment, updates or amendments, resolution, completion, and cancellation.
Patient-care-protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation.
Patient-record-event	Patient record created, modified, or accessed.
PHI-export	Any export of PHI on media, either removable physical media such as CD-ROM or electronic transfer of files such as email. Any printing activity, paper or film, local or remote, which prints PHI.
PHI-import	Any import of PHI on media, either removable physical media such as CD-ROM or electronic transfers of files such as email.
Procedure-record-event	Procedure record created, modified, accessed or deleted.
Query Information	A query has been received, either as part of an IHE transaction, or as part other products functions. For example: 1) Modality Worklist Query 2) Instance or Image Availability Query 3) PIX, PDQ, or XDS Query Notes: The general guidance is to log the query event with the query parameters and not the result of the query. The result of a query may be very large and is likely to be of limited value vs. the overhead. The query parameters can be used effectively to detect bad behavior and the expectation is that given the query parameters the result could be regenerated if necessary.
Security Alert	Security Administrative actions create, modify, delete, query, and display the following: Configuration and other changes, e.g., software updates that affect any software that processes protected information. Hardware changes may also be reported in this event. 1. Security attributes and auditable events for the application functions used for patient management, clinical processes, registry of business objects and methods (e.g., WSDL, UDDI), program creation and maintenance, etc. 2. Security domains according to various organizational categories such as entity-wide, institutional, departmental, etc. 3. Security categories or groupings for functions and data such as patient management, nursing, clinical, etc. 4. The allowable access permissions associated with functions and data, such as create, read, update, delete, and execution of specific functional units or object access or manipulation methods. 5. Security roles according to various task-grouping categories such as security administration, admissions desk, nurses, physicians, clinical specialists, etc. It also includes the association of permissions with roles for role-based access control.

Audit Event Trigger	Description
	6. User accounts. This includes assigning or changing password or other authentication data. It also includes the association of roles with users for role-based access control, or permissions with users for user-based access control. 7. Unauthorized user attempt to use security administration functions. 8. Audit enabling and disabling. 9. User authentication revocation. 10. Emergency Mode Access (aka Break-Glass) Security administration events should always be audited.
User Authentication	This message describes the event of a user log on or log off, whether successful or not. No Participant Objects are needed for this message.
Study-Object-Event	Study is created, modified, accessed, or deleted. This reports on addition of new instances to existing studies as well as creation of new studies.
Study-used	SOP Instances from a specific study are created, modified or accessed. One event covers all instances used for the particular study.

Bei Bedarf können ergänzend noch eigene Trigger-Ereignisse definiert werden.

Anhang 1.2:Inhalt eines Ereigniseintrags

Der Inhalt, der bei einem Ereignis protokolliert wird, findet sich in IHE IT Infrastructure Technical Framework, Volume 2a Kapitel 3.20 Record Audit Event.

Grundsätzlich beinhaltet das Protokoll Angaben zum Ereignis selbst (z. B. EventID), aber natürlich auch benutzerbezogene Angaben, wobei benutzerbezogen sich sowohl auf natürliche Personen wie auch auf Systeme/Prozesse beziehen kann.

Die bei den Auditeinträgen angegebene Optionalität ist wie folgt zu interpretieren:

M = obligatorisch
U = optional
M/U = obligatorisch oder optional in Bezug auf Ereignisse

Anhang 1.3:Nachweis der Erforderlichkeit der protokollierten Daten

Die im Protokoll gespeicherten Informationen richten sich nach den Vorgaben von IHE IT Infrastructure Technical Framework, Volume 2a Kapitel 3.20. Daher werden im Protokoll folgende Daten verarbeitet:

Anhang 1.3.1: Ereignisbezogene Protokollierung

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Event AuditMessage/ EventIdentification	EventID	M	EV(110106, DCM, “Export”)	ID des auditierten Ereignisses	Ohne eindeutige Identifizierung des auslösenden Ereignisses kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung zwischen Ereignis und ggf. verarbeitete personenbezogene Daten kaum möglich
	EventActionCode	M	“R” (Read) for Export	Art der während des auditierten Ereignisses durchgeführten Aktion	Zur Nachverfolgbarkeit der Verarbeitung insbesondere auch der Änderung von Daten erforderlich
	EventDateTime	M	not specialized	Datum/Uhrzeit des Auftretens des auditierten Ereignisses	Zur Nachverfolgbarkeit, wann Daten verarbeitet wurden, erforderlich
	EventOutcomeIndicator	M	not specialized	Erfolg oder Misserfolg des Ereignisses	Zur Nachverfolgbarkeit, ob Daten verarbeitet wurden, erforderlich
	PurposeOfUse	M	why was the data disclosed	Code für den Verwendungszweck des Datenzugriffs	Zur Nachverfolgbarkeit, warum Daten verarbeitet wurden, erforderlich
	EventTypeCode	M	EV(IHE0006, “IHE”, “Disclosure”) - indicates type	Ereigniskategorie	Die Nutzung des Eintrags in Verbindung mit einem entsprechendem Codesystem ermöglicht die Zuordnung des Ereignisses zu einer Ereigniskategorie

Die Quelle (=Source, Document Repository), d.h. wo die jeweiligen Daten gespeichert sind, sowie der Empfänger (=Destination, Document Consumer) der Daten werden ebenfalls immer angegeben.

In Abhängigkeit des Ereignisses werden weitere Protokolleinträge erzeugt (in den Klammern ist jeweils die Multiplizität der Einträge angegeben):

- Benutzerbezogene Protokolleinträge
  - ActiveParticipant - Releasing Agents (0..*)
  - ActiveParticipant - Custodian (0..1)
  - ActiveParticipant - Authorizing Agent (0..n)
  - ActiveParticipant - Receiving Agent (1..n)
- Auditbezogene Protokolleinträge
  - Audit Source (1)
- Teilnehmerbezogene Protokolleinträge
  - ParticipantObject – Patient (1)
  - ParticipantObject – Data (Document) released (1..n)

Anhang 1.3.2: Benutzerbezogene Protokollierung

Hier gibt es vier Möglichkeiten, was in einem Auditeintrag vorkommen kann:

- Releasing Agent (0..*)
- Custodian (0..1)
- Authorizing Agent (0..n)
- Receiving Agent (1..n)

Der grundsätzliche Protokolleintrag kann folgende Daten beinhalten:

Feldname	Beschreibung
UserID	ID der Person oder des Prozesses
AlternateUserID	Alternative ID des Benutzers oder Prozesses
UserName	Benutzer- oder Prozessname
UserIsRequestor	Indikator dafür, dass der Benutzer der Anfragende ist/nicht der Anfragende ist
RoleIDCode	Spezifikation der Rolle, die der Benutzer bei der Ausführung des Ereignisses innehat
PurposeOfUse	Code für den Verwendungszweck des Datenzugriffs[55]
NetworkAccessPointTypeCode	Art des Netzwerkzugriffspunkts
NetworkAccessPointID	ID des Netzwerkzugriffspunkts

[55] Idealerweise wird hier auf DIN CEN ISO/TS 14265 „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“ zurückgegriffen

Anhang 1.3.2.1: Releasing Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Releasing Agent AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the Disclosure.	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	UserName	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserIsRequestor	M	“true”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(110153, DCM, “Source”)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe des Netzwerks; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe der Netzwerk ID; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden

Anhang 1.3.2.2: Custodian

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Custodian (if known) AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized		Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	UserName	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(159541003, SNOMED CT, “Record keeping/library clerk")	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe des Netzwerks; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe der Netzwerk ID; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden

Anhang 1.3.2.3: Authorizing Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Authorizing Agent (if known) AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	UserName	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(429577009, SNOMED CT, "Patient Advocate")	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe des Netzwerks; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe der Netzwerk ID; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden

Anhang 1.3.2.4: Receiving Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Receiving Agent AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	AlternativeUserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserName	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(110152, DCM, “Destination”)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Angabe der Netzwerk ID; kann zur Nachverfolgung von Sicherheitsvorfällen genutzt werden
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.

Anhang 1.3.3: Auditsystembezogene Protokollierung

	Field Name	Opt	Value	Zweck	Begründung Erforderlichkeit
Audit Source AuditMessage/ AuditSourceIdentification	AuditSourceID	U	not specialized.	Eindeutige ID der Auditquelle - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Quelle, die einen Auditeintrag auslöste, kann keine Zuordnung des Ursprungs für den Auditeintrag erfolgen, wodurch eine Zuordnung zwischen dem Ursprung des Ereignisses und den dort ggf. verarbeitete personenbezogene Daten kaum möglich wäre
	AuditEnterpriseSiteID	U	not specialized	Standort- bzw. Unternehmens-ID der den Auditeintrag auslösenden Stelle : - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Mittels dieses Eintrags kann bei einrichtungsübergreifender Kommunikation festgestellt werden, von welcher Einrichtung oder Unternehmen das Ereignis, welches den Auditeintrag hervorrief, verursacht wurde
	AuditSourceTypeCode	U	not specialized	Typcode der Auditquelle: - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.3 „Audit Source Type Code“[56]: 1 Endbenutzer-Schnittstelle 2 Datenerfassungsgerät oder -instrument 3 Webserver-Prozess-Schicht in einem multi-tier System 4 Anwendungsserver-Prozess-Schicht in einem multi-tier System 5 Datenbankserver-Prozess-Schicht in einem multi-tier System 6 Sicherheitsserver, z. B. ein Domänencontroller 7 Netzwerkkomponente der ISO-Ebene 1-3 8 Betriebssoftware auf ISO-Ebene 4-6 9 Externe Quelle, anderer oder unbekannter Typ Der Eintrag ist zur Nachverfolgbarkeit des Ablaufs eines Sicherheitsvorfalles erforderlich.

[56] Request for Comments 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-07-29] Verfügbar unter https://tools.ietf.org/html/rfc3881

Anhang 1.3.4: Teilnehmerobjektbezogene Protokollierung

Der grundsätzliche Protokolleintrag einer teilnehmerbezogenen Protokollierung folgende Daten beinhalten:

Feldname	Beschreibung
ParticipantObjectTypeCode	Code des Teilnehmerobjekttyps
ParticipantObjectTypeCodeRole	Objekttypcode der Rolle
ParticipantObjectDataLifeCycle	Bezeichner für die Lebenszyklusphase der Daten des Teilnehmerobjekts
ParticipantObjectIDTypeCode	Typcode der Teilnehmerobjekt-ID
ParticipantObjectPolicySet	Leitliniensatz für die Zulassung für Teilnehmerobjekt-ID
ParticipantObjectSensitivity	Durch die Leitlinie definierte Sensibilität der ParticipantObjectID (Teilnehmerobjekt-ID)
ParticipantObjectID	Identifiziert eine bestimmte Instanz des Teilnehmerobjekts
ParticipantObjectName	Objektname des Teilnehmers, zum Beispiel der Name einer Person
ParticipantObjectQuery	Inhalt der Abfrage für das Teilnehmerobjekt

Anhang 1.3.4.1: Patient

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Patient (AuditMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"1" (Person)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Erkennung, ob es sich bei den Daten um personenbezogene Daten handelt
	ParticipantObjectTypeCodeRole	M	"1" (Patient)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob es sich bei den Daten um personenbezogene Daten handelt, erforderlich
	ParticipantObjectDataLifeCycle	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wie Daten verarbeitet wurden, erforderlich (Import, Export von Daten, Archivierung usw.)
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.4 „Participant Object ID Type Code"[57] und dienen der Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectSensitivity	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Sensibilität der Daten (Psychatrische Erkrankung, HIV, …) erforderlich
	ParticipantObjectID	M	The patient ID in HL7 CX format.	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectName	U	not specialized	- Auskunft - Nachverfolgbarkeit	Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID

[57] Request for Comments 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-07-29] Verfügbar unter https://tools.ietf.org/html/rfc3881

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
				- Sicherheit - Verfügbarkeit-Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	erfolgen kann
	ParticipantObjectQuery	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich
	ParticipantObjectDetail	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich

Anhang 1.3.4.2: Dokument

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Data (Document) Released (AuditMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	“2” (System)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Erkennung, ob es sich bei den Daten um personenbezogene Daten handelt
	ParticipantObjectTypeCodeRole	M	“3” (report)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob es sich bei den Daten um personenbezogene Daten handelt, erforderlich
	ParticipantObjectDataLifeCycle	M	Shall be: 11 = disclosure	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wie Daten verarbeitet wurden, erforderlich (Import, Export von Daten, Archivierung usw.)
	ParticipantObjectIDTypeCode	M	Shall be: 9 = Report Number	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.4 „Participant Object ID Type Code“[58] und dienen der Nachverfolgbarkeit, von wem in welcher Rolle Daten verarbeitet wurden, erforderlich
	ParticipantObjectSensitivity	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Sensibilität der Daten (Psychiatrische Erkrankung, HIV, …) erforderlich
	ParticipantObjectID	M	The value of <ihe:DocumentUniqueId/>	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectName	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht

[58] Request for Comments 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-07-29] Verfügbar unter https://tools.ietf.org/html/rfc3881

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
					erforderlich, da eine Identifizierung über die ID erfolgen kann
	ParticipantObjectQuery	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich
	ParticipantObjectDetail	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich

Anhang 2: Protokollierung nach der DIN EN ISO 27789

DIN EN ISO 27789 beruht, ebenso wie ATNA, in weiten Teilen auf dem RFC 3881[59] der Internet Engineering Task Force (IETF) sowie DICOM Supplement 95[60]. Allerdings wurde DICOM Supplement 95 in den eigentlichen Standard in Part 15 integriert[61].

Anhang 2.1:Zu protokollierende Ereignisse

Die Ereignisse, die eine Protokollierung auslösen, werden in Kapitel 6 der Norm beschrieben; die Norm nennt diese auslösenden Ereignisse „Auditereignisse“. Die Norm kennt zwei obligatorische Ereignistypen:

1) Zugriffereignisse auf persönliche Gesundheitsinformationen; „Zugriff“ bedeutet in Sinne der Norm das Erzeugen, Lesen, Aktualisieren und Löschen von Daten.
2) Abfrageereignisse zu persönlichen Gesundheitsinformationen, wobei die Abfrageaktion selbst das Abfrageereignis darstellt, während die sich aus der Abfrage ergebende Verweisung auf die personenbezogenen Daten als das Zugriffereignis angesehen wird.

Die Norm nennt einige Beispiele wie Authentisierungsereignisse oder auch Softwareaktualisierungsereignisse, um zu verdeutlichen, was darunter zu verstehen ist. Bei den Beispielen orientiert sie sich an den Vorgaben von IHE ATNA (siehe Anhang 1.1: jedoch sind es aufgrund des Beispielcharakters der Nennung keine verpflichtenden eine Protokollierung auslösenden Ereignisse. Die genannten Beispiele sind:

- Start- und Stoppereignisse des Anwendungsprogramms;
- Authentisierungsereignisse, die die Benutzerauthentisierung einschließen;
- Eingabe- und Ausgabeereignisse in die/aus der externen Umgebung;
- Zugriffereignisse auf andere Informationen als persönliche Gesundheitsinformationen;
- Sicherheitswarnereignisse im Zusammenhang mit den Anwendungsprogrammen;
- Zugriffereignisse auf das in den Anwendungsprogrammen aufbewahrte Auditprotokoll;
- vom Betriebssystem, der Middleware usw. generierte Ereignisse;
- durch Verwendung von Systemprogrammen generierte Zugriffereignisse;
- Verbindungs-/Trennungsereignisse zwischen Geräten und Netzwerk;
- Start-/Stoppereignisse der Schutzsysteme, zum Beispiel Virenschutzsysteme;
- Softwareaktualisierungsereignisse, die eine Softwaremodifikation oder Patches umfassen.

Anhang 2.2:Inhalt eines Ereigniseintrags

Die Einzelheiten zu Auditeinträgen werden in Kapitel 7 („Einzelheiten zum Auditeintrag“) i. V. m. Kapitel 8 („Auditeinträge für einzelne Ereignisse“) der Norm beschrieben, wobei die Norm sogar Codes für die einzutragenden Items vorgibt.

[59] RFC 3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-06-04] Verfügbar unter https://www.rfc-editor.org/info/rfc3881

[60] Digital Imaging and Communications in Medicine (DICOM): Suppl. 95 „Audit Trail Messages“. [Online] 2009 [Zitiert 2020-06-04] Verfügbar unter https://www.dicomstandard.org/supplements/ bzw. direkt pdf-Datei unter ftp://medical.nema.org/medical/dicom/final/sup95_ft.pdf

[61] Digital Imaging and Communications in Medicine (DICOM): DICOM PS3.15 2020b – „Security and System Management Profiles“, Abschnitt „A.5 Audit Trail Message Format Profile“. [Online] 2020 [Zitiert 2020-06-04] Verfügbar unter https://www.dicomstandard.org/current/ bzw. direkt pdf-Datei unter http://dicom.nema.org/medical/dicom/current/output/pdf/part15.pdf

Anhang 2.3:Nachweis der Erforderlichkeit der protokollierten Daten

Typ	Feldname	Optionalität	Beschreibung	Zweck	Begründung Erforderlichkeit
Ereignis-bezogen	EventID	M	ID des auditierten Ereignisses; eindeutiger Bezeichner eines bestimmten auditierten Ereignisses	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne Identifizierung des auslösenden Ereignisses kann keine Aussage über die Relevanz des Auditeintrages erfolgen
	EventActionCode	M	Art der während des auditierten Ereignisses durchgeführten Aktion (read, write, …)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Änderung von Daten erforderlich
	EventDateTime	M	Datum/Uhrzeit des Auftretens des auditierten Ereignisses	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wann Daten verarbeitet wurden, erforderlich
	EventOutcomeIndicator	U	Erfolg oder Misserfolg des Ereignisses	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob Daten verarbeitet wurden, erforderlich
	EventTypeCode	U	Ereigniskategorie	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Nutzung des Eintrags in Verbindung mit einem entsprechendem Codesystem ermöglicht die Zuordnung des Ereignisses zu einer Ereigniskategorie

Typ	Feldname	Optionalität	Beschreibung	Zweck	Begründung Erforderlichkeit
Benutzer-bezogen	UserID	M	ID der Person oder des Prozesses	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wer Daten verarbeitete, erforderlich
	AlternateUserID	U	Alternative ID des Benutzers oder Prozesses		Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	UserName	U	Benutzer- oder Prozessname		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	UserIsRequestor	U	Indikator dafür, dass der Benutzer der Anfragende ist/nicht der Anfragende ist	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	U	Spezifikation der Rolle, die der Benutzer bei der Ausführung des Ereignisses innehat	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wer in welcher Eigenschaft/Rolle Daten verarbeitete, erforderlich
	PurposeOfUse	U	Code für den Verwendungszweck des Datenzugriffs	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, warum Daten verarbeitet wurden, erforderlich
	NetworkAccessPointTypeCode	U	Art des Netzwerkzugriffspunkts Art ist eine von 3 Möglichkeiten: IP-Adresse, Telefonnummer, Rechner-DNS-Name	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, mit welchem Gerät Daten verarbeitet wurden, erforderlich
	NetworkAccessPointID	U	ID des Netzwerkzugriffspunkts Hier steht IP-Adresse, Telefonnummer usw.	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, mit welchem Gerät Daten verarbeitet wurden, erforderlich

Typ	Feldname	Optionalität	Beschreibung	Zweck	Begründung Erforderlichkeit
Audit-bezogen	AuditEnterpriseSiteID	U	Standort- bzw. Unternehmens-ID der den Auditeintrag auslösenden Stelle	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, von wo Daten verarbeitet wurden, erforderlich
	AuditSourceID	M	Eindeutige ID der Auditquelle	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, von wo Daten verarbeitet wurden, erforderlich
	AuditSourceTypeCode	U	Typcode der Auditquelle Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.3 „Audit Source Type Code“[62]: 1 Endbenutzer-Schnittstelle 2 Datenerfassungsgerät oder -instrument 3 Webserver-Prozess-Schicht in einem multi-tier System 4 Anwendungsserver-Prozess-Schicht in einem multi-tier System 5 Datenbankserver-Prozess-Schicht in einem multi-tier System 6 Sicherheitsserver, z. B. ein Domänencontroller 7 Netzwerkkomponente der ISO-Ebene 1-3 8 Betriebssoftware auf ISO-Ebene 4-6 9 Externe Quelle, anderer oder unbekannter Typ	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, von wem Daten verarbeitet wurden, erforderlich

[62] Request for Comments 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-07-29] Verfügbar unter https://tools.ietf.org/html/rfc3881

Typ	Feldname	Optionalität	Beschreibung	Zweck	Begründung Erforderlichkeit
Teilnehmer-objekt-bezogen	ParticipantObjectTypeCode	M	Code des Teilnehmerobjekttyps Person, Systemobjekt, Organisation, Sonstiges	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Erkennung, ob es sich bei den Daten um personenbezogene Daten handelt
	ParticipantObjectTypeCodeRole	M	Objekttypcode der Rolle	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob es sich bei den Daten um personenbezogene Daten handelt, erforderlich
	ParticipantObjectDataLifeCycle	U	Bezeichner für die Lebenszyklusphase der Daten des Teilnehmerobjekts	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wie Daten verarbeitet wurden, erforderlich (Import, Export von Daten, Archivierung usw.)
	ParticipantObjectIDTypeCode	M	Typcode der Teilnehmerobjekt-ID Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.4 „Participant Object ID Type Code“[63]	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, von wem in welcher Rolle Daten verarbeitet wurden, erforderlich
	ParticipantObjectPolicySet	U	Leitliniensatz für die Zulassung für Teilnehmerobjekt-ID	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, mit welcher Berechtigung bzw. aufgrund welcher Berechtigungs-Leitlinie Daten verarbeitet wurden, erforderlich
	ParticipantObjectSensitivity	U	Durch die Leitlinie definierte Sensibilität der ParticipantObjectID (Teilnehmerobjekt-ID)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Sensibilität der Daten (Psychiatrische Erkrankung, HIV, …) erforderlich
	ParticipantObjectID	M	Identifiziert eine bestimmte Instanz des Teilnehmerobjekts	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectName	U	Objektname des Teilnehmers, zum Beispiel der Name einer Person		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann

[63] Request for Comments 3881: Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications. [Online] 2004 [Zitiert 2020-07-29] Verfügbar unter https://tools.ietf.org/html/rfc3881

Typ	Feldname	Optionalität	Beschreibung	Zweck	Begründung Erforderlichkeit
	ParticipantObjectQuery	M/U	Inhalt der Abfrage für das Teilnehmerobjekt	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich
	ParticipantObjectDetail	U	Einzelheiten zum Teilnehmerobjekt	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich

Anhang 3: Beispiele für Protokoll-Auswertungen

Anhang 3.1:Gewährleistung der Verfügbarkeit eines IT-Systems

Protokolldaten können genutzt werden, um durch eine genaue Nachstellung von Arbeitsabläufen eine Analyse von Programmfehlverhalten zu ermöglichen. Dadurch kann entsprechend qualifiziertes Wartungspersonal (i. d. R. des Herstellers des IT-Systems) das Programmfehlverhalten beseitigen, z. B. durch Bereitstellung eines Software-Patches. Hierdurch wird einerseits die Verfügbarkeit des IT-Systems gewährleistet, letzten Endes aber auch die Integrität der Anwendung gewährleistet.

Weiterhin werden die Protokolldaten genutzt, um die Systemleistung zu überwachen und hiermit eine Kapazitätsplanung zu ermöglichen bzw. zu unterstützen. Damit das Antwortverhalten des Systems eine sinnvolle Nutzung durch Anwender ermöglicht, müssen Anfragen der Anwender zeitnah vom System abgearbeitet werden. Dazu ist eine Überwachung der Anzahl der angemeldeten Anwender und die Menge ihrer Anfragen zu überwachen (Auswirkung auf CPU und Arbeitsspeicher), die zu verarbeitende Datenmenge muss im Auge behalten werden (Größe des Speicherplatzes wie auch Prefetching und Caching) und natürlich muss auch die Netzwerkverbindung eine hinreichende Performanz aufweisen und daher ständig die Netzwerkauslastung im Auge behalten werden.

Anhang 3.2:Gewährleistung der Sicherheit der Verarbeitung

Protokolldaten müssen regelmäßig insbesondere hinsichtlich auffälliger Ereignisse überwacht werden, welche einen Angriff auf das IT-System oder auch das Vorliegen von Cyberkriminalität vermuten lassen. Dazu gehören insbesondere folgende Ereignisse:

- Ein- und Ausschaltung der Protokollierung,
- Kommunikation über unverschlüsselte Kanäle,
- Gehäuft auftretende Anfragen an Ports, auf denen keine Dienste laufen,
- Software-Aktualisierungen, die aus einem nicht vertrauenswürdigem Netz heraus oder außerhalb der festgelegten Zeiten erfolgen,
- Konfigurationsänderungen, die aus einem nicht vertrauenswürdigem Netz heraus erfolgen,
- Nicht erfolgreiche Zugriffsversuche auf Komponenten oder Dienste eines Servers,
- Eintreffende Pakete mit IP-Adressen aus einem vertrauenswürdigen Netz mit nicht-vertrauenswürdigen IP-Adressen,
- Unautorisierter Zugriff auf Benutzer-Authentifikationsdaten,
- Zugriffsversuche auf Mechanismen zum Management von Authentifikationsdaten,
- Erweiterung von Berechtigungen einer Person zu Administrationsprivilegien,
- Ereignisse, welche auf ein Systemverhalten hinweisen, welches nicht den Erwartungen an den regelhaften Betrieb entspricht und somit potentiell eine Gefährdung für die Sicherheit der Verarbeitung darstellen kann,
- Autorisierungsverstöße.

Anhang 3.3: Stichprobenartige Datenschutzkontrolle

Im Rahmen von stichprobenartigen Kontrollen hinsichtlich der Rechtmäßigkeit der Verarbeitung durch den Datenschutzbeauftragten werden insbesondere die folgenden Auswertungen durchgeführt:

- Wer hat wann aus welchen Gründen auf welche Daten zugegriffen? Z. B.
    - zu Zwecken der Abrechnung oder der Versorgung auf Patientendaten,
    - zu Zwecken der Administration von Zugriffsrechten auf Beschäftigtendaten,
    - zu Zwecken der Datenschutzkontrolle
- Wer hat auf die Daten von Patienten des öffentlichen Lebens oder Daten von Mitarbeitern als Patienten zugegriffen?
- Ermöglichung der stichprobenartigen Auswertung von Protokolldateien hinsichtlich Ereignissen, welche potenziell auf Datenschutzverstöße hinweisen. Hierzu **können** insbesondere gehören:
    - Mehrfache Anmeldung des Benutzers, wobei „mehrfach“ durch den Verantwortlichen festgelegt wird
    - Änderung Systemrichtlinien
    - Anmeldung außerhalb der Dienstzeit
    - Anmeldung im Subsystem außerhalb des KIS- Kontextes, aber mit KIS-Zugangsdaten
    - Anzahl Fehlanmeldungen > 3
    - Druck > 1 Dokument ohne Begründung
    - Erweitern der Benutzerberechtigung zu administrativen Rechten
    - Export > 1 Dokument ohne Begründung
    - Löschen von Dokumenten
    - Löschen von Dokumenten ohne Begründung
    - Notfallanmeldung ohne Begründung
    - Suche über mehrere Patienten
    - Suche über mehrere Patienten über Abteilungsgrenzen hinweg
    - Veränderung am Regelwerk zur Protokollierung
    - Veränderung am Regelwerk zur Protokollierung ohne Begründung
    - Zugriff auf Auditprotokoll
    - Zugriff auf Auditprotokoll ohne Begründung
    - Zugriff auf Patientendaten außerhalb des Behandlungskontextes
    - Zugriff auf VIP-Daten (bzw. entsprechend geschützte Daten) außerhalb des Behandlungskontextes
    - Zugriff mit „Super-User“-Rechten außerhalb der Arbeit an der Systemkonfiguration
- Die Ermöglichung der Überprüfung, wer wann welche Protokolldaten aus welchem Grund ausgewertet hat.
- Suche nach Systemanwendern, die seit x Tage kein Login hatten (z. B. wegen Ausscheiden aus dem Unternehmen)

Dabei ist zu beachten bzw. zu klären, ob die entsprechenden Informationen in den Protokollen zur Verfügung stehen oder ob die Protokollierung vielleicht den Vorgaben bzgl. der Protokollierung nicht genügt.

Es gibt weitere stichprobenartige Kontrollen, die nur teilweise durch die Auswertung von Protokolldaten unterstützt werden können, die aber im Rahmen der Kontrolle der Einhaltung der Vorgaben bzgl. Protokollierung mit überprüft werden sollten. Dazu gehören beispielsweise:

- Wer hat welche Rechte hinsichtlich welcher Verarbeitung von welchen personenbezogenen Daten? Dies beinhaltet eine Überprüfung bezüglich
    - Welche Rechte hat welche Person?
    - Welche Rechte hat welche Rolle?
    - Welche Rollen sind welcher Person zugeordnet?
    - Wer darf auf Daten eines bestimmten Patienten zugreifen?
- Wird die Sicherheit der Verarbeitung ausreichend gewährleistet? Hier sollte insbesondere geprüft werden:
    - Richtlinien hinsichtlich Vergabe von Passwörtern/Passphrasen (Stichwort „Kennwortkomplexität“)
    - Vorgaben bzgl. automatischer Abmeldung bei Inaktivität
    - Suche nach inaktiven Benutzern, wobei die Zeitdauer der Inaktivität individuell einstellbar sein muss

Anhang 4: Beispiel für eine Betriebsvereinbarung zur Protokollierung

Betriebsvereinbarung

Zwischen

…

– im Folgenden „Unternehmen“ genannt –

und

…

dem Betriebsrat der Fa. , vertreten durch den Betriebsratsvorsitzenden

– im Folgenden „Betriebsrat“ genannt –

wird folgende Betriebsvereinbarung geschlossen:

§ 1 Zweck und Gegenstand

Vorliegendes Regelwerk definiert die Rahmenbedingungen für den Umgang von in IT-Systemen anfallenden Log- und Protokolldateien des Unternehmens. Sofern einzelne Einheiten des Unternehmens hiervon abweichen wollen, erstellen sie hierfür eine eigene Regelung, die mit der oder dem Datenschutzbeauftragten des Unternehmens abzustimmen und allgemein zugänglich zu dokumentieren ist.

Ausnahmen müssen begründet und dem Betriebsrat zur Mitbestimmung vorgelegt werden, die Vorlage muss eine Verfahrensbeschreibung und eine Risikoanalyse beinhalten.

Diese Betriebsvereinbarung ist ein selbstständiger datenschutzrechtlicher Erlaubnistatbestand (i. S. v. Artt. 6 Abs. 1 lit c, 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 3, 4 BDSG) zur erforderlichen Verarbeitung personenbezogener Daten im Zusammenhang mit der Protokollierung. Anderweitige Erlaubnistatbestände nach DS-GVO und bzw. oder BDSG bleiben davon unberührt.

§ 2 Geltungsbereich

Diese Betriebsvereinbarung gilt für alle Beschäftigten unabhängig von Art und Umfang ihrer Beschäftigung, insbesondere auch für Mitarbeiter auf Zeit. In örtlicher Hinsicht gilt diese Betriebsvereinbarung für alle in Deutschland gelegenen Betriebe des Arbeitgebers.

§ 3 Zielsetzung und Abgrenzung

Mithilfe dieses Regelwerks soll ein Standard für den Umgang mit Log- und Protokolldateien geschaffen werden, welches einerseits für die vom Rechenzentrum betriebenen Systeme verbindlich ist und andererseits eine Orientierung für die vom Unternehmen betriebenen Verfahren bietet. Das Regelwerk ersetzt nicht die vom Datenschutzgesetz geforderte Dokumentation im Verzeichnis der Verarbeitungstätigkeiten oder die Datenschutzfolgenabschätzung und deren Abstimmung mit der oder dem zuständigen Datenschutzbeauftragten.

§ 4 Verarbeitete Datenarten

Im Rahmen der Nutzung von angebotenen IT-Diensten wie Email und Internet durch Beschäftigte des Unternehmens werden insbesondere Verbindungs- und Nutzungsdaten protokolliert. Hierzu zählt auch die IP-Adresse des Rechners, von dem eine Internetverbindung hergestellt wird - ein Datum, zu dem sich in der Regel ein Personenbezug herstellen lässt. Zu jedem ein IT-System muss in einem Protokollierungskonzept abschließend dargestellt werden, welche personenbezogenen Daten protokolliert werden.

§ 5 Zweckbestimmung

Log- und Protokolldaten werden im Zusammenhang mit dem Betrieb von im Unternehmen angebotenen bzw. genutzten IT-Diensten verarbeitet. Die Protokollierung und deren anlasslose und anlassbezogene Auswertung der Protokolldaten hat ausschließlich zu folgenden Zwecken zu erfolgen:

- Datenschutzrechtlichen Fragestellungen insb. dem Beantworten von Betroffenenanfragen,
- vorbeugende Maßnahme der Zugriffskontrolle,
- Maßnahme zur Nachweisbarkeit von Verarbeitungsvorgängen,
- Gewährleistung der Netz- und Systemsicherheit,
- Schutz vor Missbrauch,
- Analyse und Korrektur technischer Fehler,
- Optimierung des Netzes,
- statistische Feststellung des Gesamtnutzungsvolumens,
- für Zwecke der Auswertung nach den Vorgaben dieser Vereinbarung zur Missbrauchskontrolle.

Im Protokollierungskonzept des jeweiligen IT-Systems muss abschließend festgehalten werden, auf welche Ereignisse eine Protokollierung erfolgt.

§ 6 Datenschutz

Die Verarbeitung personenbezogener Daten von Beschäftigten muss den Grundsätzen der Zweckbindung, der Transparenz, der Verhältnismäßigkeit sowie der Datensparsamkeit entsprechen. Eine Datenspeicherung auf Vorrat ist unzulässig.

Der Arbeitgeber trägt Sorge dafür, seinen Informationspflichten aus Art. 12 ff. DS-GVO nachzukommen. Er informiert insbesondere die betroffenen Beschäftigten über ihre Rechte und Pflichten in Bezug auf die elektronische Datenverwendung und über die dazu abgeschlossenen Betriebsvereinbarungen. Informationen und Mitteilungen, die sich auf die Verarbeitung beziehen, sind den betroffenen Beschäftigten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Der Arbeitgeber hat die Pflicht, personenbezogene Daten unverzüglich zu löschen, sofern einer der in Art. 17 DS-GVO genannten Gründe zutrifft. Die personenbezogenen Daten der Mitarbeiter bleiben daher so lange im IT-System gespeichert, bis die Voraussetzungen für ihre Löschung vorliegen. Dies ist insbesondere der Fall, wenn die Daten zur Erfüllung des Zwecks der Erhebung oder Speicherung sowie im Zusammenhang mit der Erfüllung gesetzlicher, kollektivvertraglicher oder einzelvertraglicher Verpflichtungen bzw. der Durchsetzung entsprechender Rechte nicht mehr benötigt werden. Außerdem hat der Arbeitgeber die Pflicht, die Verarbeitung einzuschränken, soweit eine der in Art. 18 DS-GVO genannten Voraussetzungen gegeben ist.

§ 7 Zugriff

Der Zugriff auf Log- und Protokolldaten ist auf den zuständigen IT-Sicherheitsbeauftragten und die Administratoren des jeweiligen Systems zu beschränken. Ihre Auswertung und der Zugriff auf die Ergebnisse der Auswertung erfolgt nach Maßgabe der Bestimmungen des Protokollierungskonzeptes des jeweiligen IT-Systems und dieser Vereinbarung. Bei Nachfragen an den Datenschutzbeauftragten bzgl. Verstöße gegen das Datenschutzrecht oder bei Anfragen zu Auskunftsersuchen erhält der Datenschutzbeauftragte im Beisein des IT-Sicherheitsbeauftragten einen lesenden Zugriff auf die Protokolldateien.

Weiterhin erfolgt eine stichprobenartige Auswertung und Nutzung der Protokolldaten inklusive der Zugriffe auf die Protokolldaten unter Einbeziehung des IT-Sicherheitsbeauftragten und Hinzuziehung des Datenschutzbeauftragten sowie einer Vertretung des Betriebsrates zur Prüfung der Wahrung der datenschutzrechtlichen Vorgaben gem. der Vorgaben im Protokollierungskonzept des jeweiligen IT-Systems..

Der oder die IT-Sicherheitsbeauftragte(n) sowie der oder die Datenschutzbeauftragte(n)sind dem IT-Leiter/-in sowie dem Betriebsrat vom Unternehmen namentlich zu benennen. Die Verantwortung für die Beschränkung des Zugriffs auf die vorstehenden Funktionsträger trägt der Leiter der IT-Abteilung.

Jeder Zugriff auf Protokolldateien wird unter Angabe der folgenden Informationen

- anwesende Personen und deren Funktion,
- Datum und Uhrzeit,
- Anlass und Ziel des Zugriffs bzw. der Auswertung der Protokolldaten,
- Ergebnis des Zugriffs bzw. der Auswertung der Protokolldaten und
- Angabe weiterer geplanter Schritte (sofern zutreffend)

festgehalten, der Betriebsrat ist vom Zugriff in Kenntnis zu setzen. Dem Betriebsrat steht ein Kontrollrecht zu, welches beinhaltet, dass die Übersichten der vergebenen Zugriffsrechte sowie die die Zugriffe auf Protokolle eingesehen werden können.

§ 8 Verhaltens- und Leistungskontrolle

Eine Nutzung der Protokolldaten zum Zweck einer Leistungskontrolle ist unzulässig, es sei denn eine Betriebsvereinbarung erlaubt dies ausdrücklich. Eine Nutzung der Protokolldaten zur Verhaltenskontrolle ist nur dann zulässig, wenn dem Arbeitgeber entweder Hinweise auf arbeitsvertragliche Pflichtverletzungen des Beschäftigten vorliegen oder im Fall des Vorliegens von dokumentierten tatsächlichen Anhaltspunkten für eine vom Beschäftigten im Beschäftigungsverhältnis begangene Straftat unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes.

§ 9 Löschfristen

Die Aufbewahrungsfrist der Log- und Protokolldaten sind im Löschkonzept für das jeweilige IT-System verbindlich zu regeln.

§ 10 Schulungen

Die Dienststelle bietet regelmäßig Awareness-Schulungen hinsichtlich Datenschutz-Themen für IT-Sicherheitsbeauftragte und Systemadministratoren an. Die Schulungen sind verpflichtend. Die IT-Sicherheitsbeauftragten müssen die Schulung vor Übernahme ihrer Aufgabe absolviert haben. Die Systemadministratoren sollen die Schulung vor Übernahme ihrer Aufgabe absolviert haben; wenn dies aus praktischen Gründen nicht möglich ist, so ist die Teilnahme an der zeitlich ersten Schulung nach Übernahme der Aufgabe verpflichtend.

§ 11 Missbrauch

Eine über die in dieser Vereinbarung und in den Protokollierungskonzepten des jeweiligen IT-Systems getroffenen Festlegungen hinausgehende Verarbeitung der Daten zur Verhaltens- oder Leistungskontrolle stellt einen Verstoß gegen datenschutzrechtliche Bestimmungen dar und findet deshalb nicht statt. Ein Verstoß gegen diese Bestimmung kann neben dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

Auch jeder andere Zugriff, der nicht auf eine gesetzliche Regelung oder den in den §§ 6 und 7 genannten Anwendungsszenarien entspricht, wird als Verstoß gewertet und kann neben dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

§ 12 Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 13 Inkrafttreten, Dauer, Nachwirkung

Diese Betriebsvereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Ende eines Kalenderjahres gekündigt werden. Einvernehmliche Änderungen sind jederzeit möglich. Bis zum Abschluss einer neuen Betriebsvereinbarung wirkt diese Betriebsvereinbarung nach.

_____	_____
(Ort, Datum)	(Ort, Datum)
_____	_____
– Unternehmen –	– Betriebsrat –

Anhang 5: Beispiel für ein Protokollierungskonzept

Präambel

Die „Krankenkasse der armen orientierungslosen Studierenden“ (KAOS) betreibt für ihre Mitglieder eine elektronische Patientenakte („ePA“) auf Basis von IHE XDS. Die grundsätzliche Möglichkeit, ihren Mitgliedern eine ePA anbieten zu dürfen, ergibt sich aus den Regelungen des SGB V. Da die Aufgaben inkl. der zu verarbeitenden Daten durch Krankenkassen in den Sozialgesetzbüchern abschließend geregelt ist, darf die KAOS zwar ihren Mitgliedern eine Patientenakte anbieten, selbst aber keinen Zugriff auf die darin gespeicherten Daten haben, da hier neben den bei der KAOS zum Versicherten gespeicherten Daten auch weitergehende Patientendaten von Leistungserbringern gespeichert werden.

Die KAOS beauftragte daher die ePA GmbH, ein Unternehmen, welches sich auf die Einführung und den Betrieb von auf IHE XDS basierenden elektronischen Patientenakten spezialisierte, mit der Einführung und dem Betrieb der KAOS-ePA. Durch vertragliche Gestaltung ist sichergestellt, dass die KAOS selbst keinen Zugriff auf die Daten hat.

Gleichwohl müssen gemäß § 78 SGB X nach einer Übermittlung Sozialdaten in demselben Umfang geschützt werden wie bei der KAOS selbst. Daher muss die KAOS die Gewährleistung des Schutzes der in der ePA gespeicherten Sozialdaten ihrer Versicherten prüfen. Insbesondere, aber nicht ausschließlich hierzu, erfolgt eine Protokollierung von Zugriffen auf die Sozialdaten und das Datenschutz-Team der KAOS nutzt neben regelmäßig stattfindenden Audits die Protokolldaten der ePA zur Überprüfung, ob ein unberechtigter Zugriff auf die in der ePA gespeicherten Sozialdaten erfolgte. Bei einer Sichtung der Protokolldaten wird weiterhin regelmäßig geprüft, ob eine Verarbeitung der Sozialdaten aus einem Drittland heraus erfolgte. Ist dies der Fall, wird untersucht, ob dieser Zugriff durch die jeweilige versicherte Person (statthafter Zugriff), einem Leistungserbringer (ggf. statthafter Zugriff) oder sonstigen dritten (unzulässiger Zugriff) erfolgte.

Protokollierungskonzept zur ePA der KAOS

§ 1 Geltungs- und Anwendungsbereich

Dieses Protokollierungskonzept gilt für den Betrieb elektronischen Patientenakte (ePA) der „Krankenkasse der armen orientierungslosen Studierenden“ (KAOS). Alle Verarbeitungen der in dieser ePa gespeicherten Daten werden protokolliert, dies gilt sowohl für Verarbeitungen in Deutschland wie auch für Zugriffe von außerhalb Deutschlands. Dies heißt insbesondere, dass ggf. auch Daten von Personen außerhalb von Deutschland verarbeitet werden.

§ 2 Begriffsbestimmungen

Audit: systematische und unabhängige Prüfung von Zugriffen auf, Ergänzungen zu oder Änderungen in informationstechnischen Systemen, um zu ermitteln, ob die Aktivitäten und Daten in Übereinstimmung mit den organisationsinternen Standardarbeitsanweisungen und Leitlinien und den geltenden behördlichen Anforderungen ausgeführt bzw. erfasst, verwendet, aufbewahrt oder offenbart wurden.

Notfallzugriff: Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen.

Protokollierung: Manuelle oder automatische Aufzeichnung (Speicherung) ausgewählter betriebs- und sicherheitsrelevante Ereignisse zum Zweck einer späteren Auswertung, welche zumindest mindestens den Zeitpunkt, die ausgeführte Handlung und den Handelnden beinhaltet.

§ 3 Zweck der Protokollierung

Die Zwecke der in diesem Protokollierungskonzept beschriebenen Protokollierung sind:

1. Erteilung einer Auskunft auf Antrag einer betroffenen Person,
2. Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung,
3. Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten,
4. Gewährleistung der Sicherheit der Verarbeitung,
5. Gewährleistung der Verfügbarkeit der Anwendung.

§ 4 Rechtsgrundlage für die Protokollierung

1. Erteilung einer Auskunft auf Antrag einer betroffenen Person:
   Art. 15 DS-GVO i. V. m. § 83 SGB X sowie §§ 32, 33 BDSG
2. Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung:
   § 78 SGB X
3. Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten:
   Artt. 33, 34 DS-GVO i. V. m. § 83a SGB X
4. Gewährleistung der Sicherheit der Verarbeitung:
   Art. 32 DS-GVO i. V. m. § 22 Abs. 2 BDSG
5. Gewährleistung der Verfügbarkeit der Anwendung:
   Art. 32 DS-GVO i. V. m. § 22 Abs. 2 BDSG

§ 5 Art der verarbeiteten Daten

a) Sozialdaten, die von der KAOS selbst hineingestellt werden
b) Patientendaten, welche von Leistungserbringern wie Krankenhäusern oder niedergelassenen Arztpraxen eingestellt werden
c) Daten, welche die jeweilige versicherte Person selbst einstellte

§ 6 Umfang der Protokollierung

Der Umfang sowie die Erforderlichkeit zur Erzielung der dargestellten Zwecke der verarbeiteten Daten wird in Anhang 1 dargestellt.

§ 7 Lebenszyklus der Protokolldaten

§ 7.1 Erzeugung

Protokolldaten werden bei der Nutzung der ePA vom IHE XDS automatisch generiert. Die auslösenden Ereignisse („trigger events“) sind im IHE IT Infrastructure Technical Framework, Volume 2a Kapitel 3.20 (Abschnitt 4.1.1.1) in Tabelle Table 3.20.4.1.1.1-1 Audit Event triggers, aufgeführt.

§ 7.2 Speicherung

Die Protokolldaten werden auf einem Software WORM-Medium („Write-once,read-many“) gespeichert, welches einerseits gewährleistet, dass Protokolldaten nicht nachträglich verändert werden können, andererseits unter definierten Umständen eine nachvollziehbare Löschung der Daten erlaubt, d. h. es kann immer festgestellt werden, dass Daten gelöscht wurden. Ein

Berechtigungskonzept sowie dessen technische Um- und Durchsetzung stellt sicher, dass nur berechtigte Personen Zugriff auf die Protokolldaten haben.

§ 7.3 Nutzung von Protokolldaten, Auswertung

Auswertungen erfolgen grundsätzlich nur, wenn es um mindestens einen der folgenden Zwecken handelt:

1) Erteilung einer Auskunft auf Antrag einer betroffenen Person
2) Stichprobenartige Datenschutzkontrolle bzgl. Ordnungsmäßigkeit der Verarbeitung
3) Prüfung des Sachverhalts bei einer vorliegenden bzw. bei einem Verdacht auf eine vorliegende Verletzung des Schutzes personenbezogener Daten
4) Gewährleistung der Sicherheit der Verarbeitung
5) Gewährleistung der Verfügbarkeit der Anwendung.

Auswertungen erfolgen dabei immer im Vier-Augen-Prinzip. Jeder Zugriff auf Protokolldateien wird unter Angabe der folgenden Informationen

- anwesende Personen und deren Funktion,
- Datum und Uhrzeit,
- Anlass und Ziel des Zugriffs bzw. der Auswertung der Protokolldaten,
- Ergebnis des Zugriffs bzw. der Auswertung der Protokolldaten und
- Angabe weiterer geplanter Schritte (sofern zutreffend)

festgehalten. Die/der Datenschutzbeauftragte der KAOS kann diese Daten jederzeit zu Zwecken der Datenschutzkontrolle einsehen. Einmal jährlich eine stichprobenartige Auswertung und Nutzung der Protokolldaten inklusive der Zugriffe auf die Protokolldaten durch den Datenschutzbeauftragten der ePA GmbH unter Einbeziehung des IT-Sicherheitsbeauftragten der ePA GmbH sowie der/des Datenschutzbeauftragten der KAOS.

§ 7.4 Löschung

Da nach § 41 BDSG für Bußgelder, die nach Art. 83 DS-GVO verhängt werden, die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß gelten und entsprechend § 31 Abs. 2 OWiG die Verfolgung von Ordnungswidrigkeiten in drei Jahren verjährt, werden Protokolle drei Jahre aufbewahrt und anschließend vernichtet.

§ 8 Verarbeitung der Protokolldaten

§ 8.1 Erteilung einer Auskunft auf Antrag einer betroffenen Person

Liegt eine Anfrage einer betroffenen Person bzgl. Zugriffe auf die entsprechenden personenbezogenen Daten vor, erfolgt eine entsprechende Auswertung durch die/den Datenschutzbeauftragten der ePA GmbH unter Einbeziehung des IT-Sicherheitsbeauftragten der ePA GmbH, sodass das Vier-Augen-Prinzip gewährleistet wird.

§ 8.2 Stichprobenartige Datenschutzkontrolle

Die/der Datenschutzbeauftragte der KAOS führt einmal jährlich unter Einbeziehung der/des Datenschutzbeauftragten der ePA GmbH eine stichprobenartige Kontrolle durch. Hierbei wird insbesondere kontrolliert:

- Wer hat welche Rechte hinsichtlich welcher Verarbeitung von welchen personenbezogenen Daten und warum?
- Wer hat wann aus welchen Gründen auf welche Daten zugegriffen?
- Wer hat wann welche Protokolldaten aus welchem Grund ausgewertet?

Die Stichprobengröße errechnet sich dabei nach der Formel[64] $n = \frac{\frac{z^2 \cdot p \cdot (1-p)}{e^2}}{1+[\frac{z^2 \cdot p \cdot (1-p)}{e^2 \cdot N}]}$, mit

N = Gesamtumfang der verarbeiteten Patientendaten pro Prüfungszeitraum, z. B. 10.000 Patienten pro Jahr
z = Konfidenzniveau soll 95 % betragen, woraus resultiert ein z-Wert von 1,96
p = Standardabweichung: 50%
e = Konfidenzintervall (auch Fehlermarge oder Fehlerbereich genannt): 5%

Für die beispielhaft festgelegte Anzahl im zu prüfenden Jahr verarbeiteten Daten resultiert Stichprobengröße von etwa 390 Patienten, wenn man mit einer Wahrscheinlichkeit von 95 Prozent den Wahrheitsgehalt abbilden will bzw. wenn die Abweichung des durch die Stichprobe ermittelten Wertes vom tatsächlichen Wert nicht mehr als 5% betragen soll.

§ 8.3 Prüfung bei Verletzung des Schutzes personenbezogener Daten

Liegt eine Verletzung des Schutzes personenbezogener Daten vor oder auch nur der Verdacht einer entsprechenden Verletzung, erfolgt eine entsprechende Auswertung durch die/den Datenschutzbeauftragten der ePA GmbH unter Einbeziehung des IT-Sicherheitsbeauftragten der ePA GmbH, sodass das Vier-Augen-Prinzip gewährleistet wird.

§ 8.4 Gewährleistung der Sicherheit der Verarbeitung

Intrusion Detection Systeme der ePA GmbH werden automatisiert u. a. die Protokolldaten der ePA bzgl. potentieller Angriffe aus. Sollten sie ein mögliches Angriffsverhalten feststellen, werden automatisiert die/der Datenschutzbeauftragte der ePA GmbH und die/der IT-Sicherheitsbeauftragte der ePA per E-Mail und SMS verständigt.

§ 8.5 Gewährleistung der Verfügbarkeit der Anwendung

Um die Verfügbarkeit der Anwendung zu gewährleisten, werten benannte Beschäftigte der IT-Abteilung die Anzahl der Zugriffe sowie die Geschwindigkeit der Antworten sowie weitere Parameter aus, welche eine Skalierung der Anwendung zur Aufrechterhaltung des Betriebs erlauben. Diese Auswertungen dürfen ausschließlich unter Einbeziehung des/der Datenschutzbeauftragten der ePA GmbH erfolgen.

§ 9 Sicherheit der Verarbeitung

§ 9.1 Vertraulichkeit: Nur berechtigte Anwender

Im Berechtigungskonzept ist festgelegt, wer wann unter welchen Umständen auf welche Daten welchen Zugriff hat. Die Vorgaben des Berechtigungssystems werden durch entsprechende IHE Profile umgesetzt:

- Die Profile EUA/XUA gewährleisten eine sichere Benutzeridentifizierung, sodass hierdurch sichergestellt ist, dass Personen wie auch Prozesse/Systeme eindeutig identifiziert werden.
- Das Profil IUA bildet die Benutzeridentifikation über RESTful Schnittstellen ab.
- Die Profile BPPC/APPC bilden die Vorgaben des Berechtigungskonzeptes ab. D. h. es wird abgebildet, wer unter welchen Umständen wann auf welche Daten von welchem Patienten zugreifen darf.

[64] SurveyMonkey; Berechnen der Anzahl der benötigten Befragten. [Online] 2020 [Zitiert 2020-08-11] Verfügbar unter https://help.surveymonkey.com/articles/de/kb/How-many-respondents-do-I-need

- Das Profil SeR bildet dabei eine zentrale Rechteverwaltung ab, wodurch zwischen Systemen eine „Sphäre des Vertrauens“ aufgebaut wird.
- Das Profil PIX stellt die eindeutige Zuordnung eines Patienten sicher, wodurch alle Dokumente dem richtigen Patienten zugeordnet werden. PIXm erlaubt Gleiches für mobile Anwendungen über eine RESTful Schnittstelle.

§ 9.2 Integrität: Manipulationssichere Erzeugung und Speicherung

Die unter 8.1 beschriebenen IHE Profile erlauben die sichere Identifikation von Benutzern wie auch Patienten, sodass in Protokolldaten nur verifizierte IDS gespeichert werden. Die Speicherung der Protokolldaten selbst erfolgt auf einem Software WORM Medium, welches die Nicht-Änderbarkeit der Protokolldaten gewährleistet.

§ 9.3 Verfügbarkeit

Die Verfügbarkeit des Systems wird durch folgende Maßnahmen gewährleistet:

- Eine redundante Spiegelung des Systems gewährleistet auch bei Ausfall eines Systems die Verfügbarkeit der Anwendung.
- Täglich erfolgte in Backup der Daten, einmal in der Woche ein vollständiges Backup, sechs Tage ein inkrementelles Backup. Die Backups werden nach Erzeugung automatisiert auf Datenvollständigkeit kontrolliert.
- Halbjährlich wird überprüft, ob eine Rekonstruktion der Daten durch das jeweils aktuelle Backup in ausreichend schneller Zeit zur Gewährleistung der Verfügbarkeit möglich ist.

Jede dieser Maßnahmen schließt immer auch die Protokollierung sowie die erzeugten Protokolldaten mit ein.

§ 9.4 Auditierung der Einhaltung dieser Vorgaben

Die/der Datenschutzbeauftragte der ePA GmbH auditiert einmal jährlich die Einhaltung dieser Vorschriften und berichtet der oder dem seitens der KAOS festgelegten Ansprechpartner/-in über die Ergebnisse des Audits. Wird Änderungsbedarf oder gar Verfehlungen festgestellt, wird zusätzlich die Geschäftsführung der ePA GmbH eingeschaltet.

§ 9.5 Pseudonymisierung

In den Protokolldaten werden ausschließlich IDs verwendet, sodass immer nur Pseudonyme verwendet werden.

§ 9.6 Inkrafttreten

Dieses Protokollierungskonzept tritt am Datum seiner Veröffentlichung in Kraft.

Datum der Veröffentlichung: 1. April 2025

Unterschrift:

xYx	xXx
(Dr. Hermine Sanatorius)	(Dr. Harald Sanarius)
Krankenkasse der armen orientierungslosen Studierenden	ePA GmbH
Geschäftsführerin	Geschäftsführer

Anhang 1: Darstellung, welche Daten protokolliert werden sowie der Nachweis der Erforderlichkeit der Protokollierung zur Erreichung der dargestellten Zwecke

Erfolgt analog zu Anhang 1.3: ff dieser Praxishilfe, d.h.:

Ereignisbezogene Protokollierung

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Event AuditMessage/ EventIdentification	EventID	M	EV(110106, DCM, “Export”)	ID des auditierten Ereignisses	Ohne eindeutige Identifizierung des auslösenden Ereignisses kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung zwischen Ereignis und ggf. verarbeitete personenbezogene Daten kaum möglich
	EventActionCode	M	“R” (Read) for Export	Art der während des auditierten Ereignisses durchgeführten Aktion	Zur Nachverfolgbarkeit der Verarbeitung insbesondere auch der Änderung von Daten erforderlich
	EventDateTime	M	not specialized	Datum/Uhrzeit des Auftretens des auditierten Ereignisses	Zur Nachverfolgbarkeit, wann Daten verarbeitet wurden, erforderlich
	EventOutcomeIndicator	M	not specialized	Erfolg oder Misserfolg des Ereignisses	Zur Nachverfolgbarkeit, ob Daten verarbeitet wurden, erforderlich
	PurposeOfUse	M	why was the data disclosed	Code für den Verwendungszweck des Datenzugriffs	Zur Nachverfolgbarkeit, warum Daten verarbeitet wurden, erforderlich
	EventTypeCode	M	EV(IHE0006, “IHE”, “Disclosure”) - indicates type	Ereigniskategorie	Die Nutzung des Eintrags in Verbindung mit einem entsprechendem Codesystem ermöglicht die Zuordnung des Ereignisses zu einer Ereigniskategorie

Releasing Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Releasing Agent AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the Disclosure.	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized		Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	~~UserName~~	U	not specialized		Keine Verwendung
	UserIsRequestor	M	“true”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(110153, DCM, “Source”)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt

Custodian

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Custodian (if known) AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized		Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	~~UserName~~	U	not specialized		Keine Verwendung
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(159541003, SNOMED CT, “Record keeping/library clerk")	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt

Authorizing Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Authorizing Agent (if known) AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Person kann keine Zuordnung bzgl. Ereignis und Auditeintrag erfolgen, insbesondere wäre eine Zuordnung wer ggf. welche personenbezogenen Daten verarbeitete so gut wie unmöglich
	AlternativeUserID	U	not specialized		Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	~~UserName~~	U	not specialized		Keine Verwendung
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(429577009, SNOMED CT, "Patient Advocate")	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt

Receiving Agent

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Receiving Agent AuditMessage/ ActiveParticipant	UserID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Regelhaft eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann; bei einer Kommunikation über Systemgrenzen hinweg kann dieses Feld genutzt werden um die ID des anderen Systems festzuhalten, sodass eine Suche bzgl. Person im anderen System ermöglicht wird.
	AlternativeUserID	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann
	~~UserName~~	U	not specialized		Keine Verwendung
	UserIsRequestor	M	“false”	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Festlegung, ob eine Anfrage bzgl. vorhandener Daten erfolgte oder nicht
	RoleIDCode	M	EV(110152, DCM, “Destination”)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Erforderlich um zu erfahren, mit welcher Rolle und somit welchen an der Rolle verknüpften Rechten die Verarbeitung erfolgte
	NetworkAccessPointTypeCode	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt
	NetworkAccessPointID	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Wird zur Nachverfolgung des Ablaufes bei Sicherheitsvorfällen genutzt

Auditsystembezogene Protokollierung

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Audit Source AuditMessage/ AuditSourceIdentification	AuditSourceID	U	not specialized.	Eindeutige ID der Auditquelle: - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Ohne eindeutige Identifizierung der Quelle, die einen Auditeintrag auslöste, kann keine Zuordnung des Ursprungs für den Auditeintrag erfolgen, wodurch eine Zuordnung zwischen dem Ursprung des Ereignisses und den dort ggf. verarbeitete personenbezogene Daten kaum möglich wäre
	AuditEnterpriseSiteID	U	not specialized	Standort- bzw. Unternehmens-ID der den Auditeintrag auslösenden Stelle: - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Mittels dieses Eintrags kann bei einrichtungsübergreifender Kommunikation festgestellt werden, von welcher Einrichtung oder Unternehmen das Ereignis, welches den Auditeintrag hervorrief, verursacht wurde
	AuditSourceTypeCode	U	not specialized	Typcode der Auditquelle - Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.3 „Audit Source Type Code“: 1 Endbenutzer-Schnittstelle 2 Datenerfassungsgerät oder -instrument 3 Webserver-Prozess-Schicht in einem multi-tier System 4 Anwendungsserver-Prozess-Schicht in einem multi-tier System 5 Datenbankserver-Prozess-Schicht in einem multi-tier System 6 Sicherheitsserver, z. B. ein Domänencontroller 7 Netzwerkkomponente der ISO-Ebene 1-3 8 Betriebssoftware auf ISO-Ebene 4-6 9 Externe Quelle, anderer oder unbekannter Typ Der Eintrag ist zur Nachverfolgbarkeit des Ablaufs eines Sicherheitsvorfalles erforderlich.

Patient

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Patient (AuditMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	“1” (Person)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Erkennung, ob es sich bei den Daten um personenbezogene Daten handelt
	ParticipantObjectTypeCodeRole	M	“1” (Patient)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob es sich bei den Daten um personenbezogene Daten handelt, erforderlich
	ParticipantObjectDataLifeCycle	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wie Daten verarbeitet wurden, erforderlich (Import, Export von Daten, Archivierung usw.)
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.4 „Participant Object ID Type Code“ und dienen der Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectSensitivity	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Sensibilität der Daten (Psychatrische Erkrankung, HIV, …) erforderlich
	ParticipantObjectID	M	The patient ID in HL7 CX format.	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectName	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit- Auskunft	Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
				- Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	
	ParticipantObjectQuery	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich
	ParticipantObjectDetail	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich

Dokument

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
Data (Document) Released (AuditMessage/ ParticipantObject-Identification)	ParticipantObjectTypeCode	M	“2” (System)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Erkennung, ob es sich bei den Daten um personenbezogene Daten handelt
	ParticipantObjectTypeCodeRole	M	“3” (report)	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, ob es sich bei den Daten um personenbezogene Daten handelt, erforderlich
	ParticipantObjectDataLifeCycle	M	Shall be: 11 = disclosure	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, wie Daten verarbeitet wurden, erforderlich (Import, Export von Daten, Archivierung usw.)
	ParticipantObjectIDTypeCode	M	Shall be: 9 = Report Number	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Die Einträge erfolgen entsprechend RFC 3881, Abschnitt 5.5.4 „Participant Object ID Type Code“ und dienen der Nachverfolgbarkeit, von wem in welcher Rolle Daten verarbeitet wurden, erforderlich
	ParticipantObjectSensitivity	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit der Sensibilität der Daten (Psychiatrische Erkrankung, HIV, …) erforderlich
	ParticipantObjectID	M	The value of <ihe:DocumentUniqueId/>	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, um welchem Patienten es sich handelte
	ParticipantObjectName	U	not specialized		Regelhaft aus Sicht des Datenschutzes eher nicht erforderlich, da eine Identifizierung über die ID erfolgen kann

	Field Name	Opt	Value Constraints	Zweck	Begründung Erforderlichkeit
	ParticipantObjectQuery	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich
	ParticipantObjectDetail	U	not specialized	- Auskunft - Nachverfolgbarkeit - Sicherheit - Verfügbarkeit	Zur Nachverfolgbarkeit, welche Daten abgefragt wurden, erforderlich