

E DIN EN ISO/IEC 24970:2025-12 (D/E)

Erscheinungsdatum: 2025-10-31

Künstliche Intelligenz - KI-System-Protokollierung (ISO/IEC DIS 24970:2025);
Deutsche und Englische Fassung prEN ISO/IEC 24970:2025

Artificial intelligence - AI system logging (ISO/IEC DIS 24970:2025); German and
English version prEN ISO/IEC 24970:2025

Inhalt	Seite
Europäisches Vorwort.....	6
Vorwort.....	7
Einleitung.....	8
1 Anwendungsbereich.....	10
2 Normative Verweisungen.....	10
3 Begriffe.....	10
4 Abkürzungen.....	14
5 Protokollierung und Nutzung von Protokollen.....	14
5.1 KI-Systemprotokolle.....	14
5.2 Protokollierungskomponenten.....	15
5.3 Protokollierung im Kontext.....	16
5.4 Protokolleinträge.....	17
5.5 KI-Systemprotokollierung.....	18
5.6 Allgemeine Anforderungen.....	19
5.7 Allgemeines.....	19
5.7.1 Sicherheit und Datenschutz.....	19
5.7.2 Aufzeichnung von Ereignissen.....	19
5.8 Technische Dokumentation.....	19
6 Gestaltung des Protokollierungssystems.....	20
6.1 Allgemeines.....	20
6.2 Rückverfolgbarkeit.....	21
6.3 Zusätzliche Funktionen.....	21
6.4 Überwachung von Anomalien der Protokollierungskomponente.....	21
7 Auslöser für die Protokollierung.....	22
7.1 Allgemeines.....	22
7.2 Auslöser aus dem Betrieb.....	23
7.2.1 Softwarefehler.....	23
7.2.2 Eingabe mit Ausreißer-Werten.....	23
7.2.3 Potentieller Angriff.....	23
7.2.4 Benutzeranfrage.....	23
7.2.5 Ergebnis einer Benutzeranfrage.....	23
7.2.6 Übermittlung von Benutzerinformationen.....	23
7.3 Auslöser aus der automatisierten Überwachung.....	23
7.3.1 Feindlicher Angriff.....	23
7.3.2 Erkennung unerwünschter Verzerrungen.....	24
7.3.3 Eingaben außerhalb der Domäne.....	24
7.3.4 Modellverschiebung.....	24
7.3.5 Protokollierung für die Entwicklung von Modellen für maschinelles Lernen zu Zwecken der Auditierbarkeit.....	24
7.4 Auslöser aus der Aufsicht durch Menschen.....	25

8	Zu protokollierende Informationen.....	25
8.1	Erforderliche Informationen.....	25
8.2	Empfohlene Informationen.....	26
9	Speicherung und Zugriff auf die Protokolle.....	26
9.1	Allgemeines.....	26
9.2	Anforderungen für den Zugriff durch Dritte	27
9.3	Zugriff für KI-Benutzer	27
9.4	Zugriff für KI-Anbieter.....	27
	Anhang A (informativ) Informationsmodell	28
	Literaturhinweise	32

Bilder

Bild 1	— Allgemeine Architektur eines KI-Systems mit Schwerpunkt auf der Nutzung von Daten, einschließlich Protokollen.	16
Bild 2	— Der Zusammenhang zwischen den Protokollierungskonzepten.....	22

Tabellen

Tabelle A.1	— Ereignismodelle	28
--------------------	--------------------------------	-----------