



Maßnahmenbericht zum datenschutzrechtlichen Audit  
Jahr 2026



für das Unternehmen:  
**KAMAT GmbH & Co. KG**

Dokumenteninformation		Auditinformationen		Dokumentenechtheit	
Stand	25.02.2026	Kunde	KAMAT GmbH & Co. KG		
Dokumenten-version	2.4.6.6	Kunden-ID	5030,0		
Vorlagen-version	06/25	Kunden-Adresse	Salinger Feld 10, 58454 Witten	Hagen, den 25.02.2026	
Zuletzt bearbeitet von	Lau	Branche	Produktionsbetrieb	 Unterschrift Auditor:in	
Sicherheit	Vertraulich	Branchenkategorie	F		
Berechtigung	Datenschutzkoordinator, Geschäftsführung, IT-Abteilung	Abteilung	-----		
Versendung des Auditberichts	digital	Ansprechpartner:in	Herr Dr. Wahl, Herr Fintrilakis		
		Auditor:in	Frau Oles	<b>GDI</b> <b>Gesellschaft für Datenschutz und Informationssicherheit mbH</b> Alter Schloßweg 30 D- 58119 Hagen Tel.: +49 (0)2331 3568320 Firmenstempel	
		Auditdatum	24.02.2026		
		Durchführung:	Videokonferenz		
		Umfang	10:00 - 10:50 Uhr		
		Schulung	./.		
		<b>Ergebnis</b>	<b>Agrund der im Datenschutzaudit gegebenen Antworten bestätigen wir dem Unternehmen ein angemessenes Datenschutzniveau.</b>		

Legende		
Antwort	UP	Überprüfung - Bitte prüfen Sie die Umsetzung der beschriebenen Situationen
	N.R.	Nicht Relevant - Die Fragestellung ist für Ihr Unternehmen nicht von Bedeutung.
	Hinweis	Hängt mit Maßnahmen zusammen, die vorher umgesetzt werden müssen. / Ggf. für Sie noch nicht relevant, kann aber ein Thema für Sie werden.
Priorität	Kurzfristig	Diese Maßnahme sollte innerhalb der nächsten drei Monate umgesetzt werden.
	Mittelfristig	Diese Maßnahme sollte innerhalb der nächsten sechs Monate umgesetzt werden.
	Langfristig	Diese Maßnahme sollte innerhalb der nächsten zwölf Monate umgesetzt werden.

## Maßnahmen zu den Abweichungen bzw. Verbesserungspotentialen aus dem Datenschutzaudit 2026

Maßnahmen aus dem Jahresaudit 2026							
ID	Frage	Antwort	Priorität	Themenschwerpunkt	Bearbeitung bis zum:	Maßnahme / Hinweis	Notizen für den Kunden
<b>Wiederkehrendes</b>							<b>Notizen</b>
W 1.2	<b>Wiederholungsaudit:</b> Wie viele Mitarbeitende hat das Unternehmen aktuell?		110	Anzahl der Mitarbeitenden		<i>Das Unternehmen beschäftigt derzeit 110 Mitarbeitende.</i>	
W 1.3	<b>Wiederholungsaudit:</b> Wie viele Personen arbeiten mit personenbezogenen Daten?		40	Anzahl der Mitarbeitenden		<i>Davon arbeiten 40 Mitarbeitende regelmäßig mit personenbezogenen Daten.</i>	
<b>Grundlegende Anforderungen der DSGVO</b>							<b>Notizen</b>
<b>Allgemeines</b>							
A 1.1	Haben Sie die Datenschutzhinweise für Ihre <b>Mitarbeitenden</b> dokumentiert bekannt gegeben?	Ja	Langfristig	Transparenzpflicht	31.12.1900	Die Datenschutzhinweise für Mitarbeitende sind zu aktualisieren. Hintergrund ist die Einführung der elektronischen Arbeitsfähigkeitsbescheinigung (eAU), durch die sich die Quelle der Datenerhebung geändert hat. Zudem sind Datenverarbeitungen im Zusammenhang mit dem Hinweisgeberschutzgesetz (HinSchG) in den Datenschutzhinweisen entsprechend zu berücksichtigen und transparent darzustellen.	<i>Eine <u>aktuelle Vorlage der Datenschutzhinweise für Mitarbeitende</u> wurde Ihnen per E-Mail übermittelt.</i>
A 1.3	Haben Sie die Datenschutzhinweise für Ihre <b>Kunden und Geschäftspartner</b> dokumentiert bekannt gegeben?	Ja	Langfristig	Transparenzpflicht	24.02.2027	Wenn Sie personenbezogene Daten von Kunden oder Geschäftspartnern verarbeiten, müssen diesen Personen entsprechende Datenschutzhinweise zur Verfügung gestellt werden.  Die Datenschutzhinweise sollten auf der Webseite hinterlegt werden. In geschäftlichen E-Mails (z.B. im Footer) sowie in Geschäftsbriefen sollte auf diesen Link verwiesen werden, etwa mit dem Hinweis: „Hinweise zum Datenschutz / Hinweise zum Umgang mit Ihren personenbezogenen Daten finden Sie unter [LINK].“  Darüber hinaus können die Datenschutzhinweise im Empfangsbereich in einem Aufsteller ausgelegt oder durch einen gut sichtbaren Aushang bereitgestellt werden.	<i>Eine <u>Vorlage der Datenschutzhinweise für Kunden und Geschäftspartner</u> wurde Ihnen per E-Mail übermittelt.</i>
A 1.5	Haben Sie die Datenschutzhinweise für <b>Bewerber</b> dokumentiert bekannt gegeben?	Ja	Langfristig	Transparenzpflicht	24.02.2027	Die Datenschutzhinweise für Bewerber sollten auf der Unternehmenswebseite hinterlegt und in Stellenausschreibungen entsprechend verlinkt werden.  Gehen Initiativbewerbungen per E-Mail ein, sollte eine Eingangsbestätigung an den Bewerber versendet werden, die einen Hinweise auf die Datenschutzhinweise enthält, z.B.: „Hinweise zum Umgang mit Ihren personenbezogenen Daten erhalten Sie unter [LINK].“ Alternativ können die Datenschutzhinweise der E-Mail als PDF-Datei im Anhang beigefügt werden.  Werden Bewerbungen in Papierform eingereicht, sollte ebenfalls eine Eingangsbestätigung versendet werden, der die Datenschutzhinweise beigefügt sind.	<i>Die derzeit verwendeten Datenschutzhinweise für Bewerber entsprechen nicht mehr dem aktuellen Stand.  Eine <u>aktuelle Vorlage der Datenschutzhinweise für Bewerber</u> wurde Ihnen per E-Mail übermittelt.</i>
<b>IT-Sicherheit und TOM</b>							<b>Notizen</b>
<b>IT-Sicherheit: Grundlagen</b>							
WT 1.0	Gibt es im Unternehmen ein Branderkennungssystem (insbesondere im Server- und Archivraum) und wird dieses regelmäßig und nachweislich überprüft?	Nein	Langfristig	Branderkennung	24.02.2027	Zur Absicherung kritischer Infrastruktur (insbesondere Server- und Archivräume) sollte ein geeignetes Branderkennungssystem implementiert werden. Die Funktionsfähigkeit der Branderkennung sollte regelmäßig und nachweislich überprüft werden.	

ID	Frage	Antwort	Priorität	Themenschwerpunkt	Bearbeitung bis zum:	Maßnahme / Hinweis	Notizen für den Kunden
<b>Personal</b>							<b>Notizen</b>
<b>Einsatz von Videokonferenz-Tools im Unternehmen</b>							
VK 1.0	Setzen Sie aktiv Videokonferenz-Tools im Unternehmen ein?	Ja	Mittelfristig			<i>Im Unternehmen werden Zoom und Microsoft Teams für die Durchführung von Videokonferenzen genutzt.</i>	
VK 1.6	Stellen Sie den Teilnehmern der Videokonferenz, die von Ihrem Unternehmen angesetzt wurde, die Datenschutzhinweise zur Verfügung?	Nein	Kurzfristig	Datenschutzhinweise für Teilnehmer	24.05.2026	<p>Als verantwortliche Stelle sind Sie bei der Nutzung von Videokonferenz-Tools verpflichtet, Teilnehmende von Videokonferenzen und Online-Meetings über die Datenverarbeitung nach Art.13 DSGVO zu informieren. Diese Verpflichtung besteht immer dann, wenn Sie selbst andere Personen zur Teilnahme einladen, nicht jedoch, wenn Sie lediglich als Teilnehmende eingeladen werden.</p> <p>Die Datenschutzhinweise sollten bereits mit der Einladung zur Videokonferenz übermittelt werden, um die erforderliche Transparenz sicherzustellen.</p> <p><u>Technische Umsetzung Datenschutzhinweise (Microsoft Teams)</u>  Microsoft Teams bietet die Möglichkeit, Datenschutzhinweise für Online-Meetings, sofern diese digital verfügbar sind, direkt in der Einladung unter dem Abschnitt „Datenschutz und Sicherheit“ zu verlinken. Dadurch entfällt die manuelle Beifügung der Hinweise zu jeder Einladung.</p>	<i>Eine Vorlage der Datenschutzhinweise für Teilnehmer von Videokonferenzen wurde Ihnen per E-Mail übermittelt.</i>
<b>Datenerhebungen im Arbeitsverhältnis</b>							
P 4.7	Wird die Kontonummer der Arbeitnehmer auf der Lohn-/Gehaltsabrechnung gekürzt dargestellt?	UP	Kurzfristig	Anonymisierung der Kontonummer	24.05.2026	Zum Schutz der Mitarbeitenden und zur Risikominimierung im Falle einer Fehlversendung von Lohn- oder Gehaltsabrechnungen, sollte die Kontonummer auf der Abrechnung immer gekürzt dargestellt werden.	
<b>Infrastruktur und IT-Sicherheit im Gebrauch</b>							<b>Notizen</b>
<b>Umgang mit Smartphones / Tablets</b>							
SP 1.0	Wie viele dienstliche Smartphones und Tablets werden im Unternehmen eingesetzt?	30		dienstliche Smartphones und Tablets		<i>Im Unternehmen sind ca. 30 dienstliche Smartphones im Einsatz.</i>	
SP 1.1	Ist eine vollständige und aktuelle Liste aller dienstlichen Smartphones, Tablets und sonstigen mobilen Endgeräte samt Betriebssystem und Betriebssystemversion vorhanden?	Nein	Langfristig	Auflistung vorhandener Geräte	24.02.2027	Für einen sicheren und nachvollziehbaren IT-Betrieb ist es erforderlich, jederzeit einen vollständigen Überblick über alle dienstlich genutzten Smartphones, Tablets und mobilen Endgeräte zu haben. Dazu sollte eine zentrale und aktuelle Inventarliste geführt werden, in der jedes Gerät mit Modell, Nutzer:in, Betriebssystem und installierter Version erfasst wird.	
SP 1.2	<i>Bei mehr als 20 dienstlichen Geräten:</i> Werden dienstliche Smartphones und Tablets über eine Mobile-Device-Management-Lösung verwaltet?	Nein	Mittelfristig	MDM	24.08.2026	Es wird empfohlen, eine Mobile-Device-Management-Lösung (MDM) einzuführen, um dienstliche Smartphones und Tablets zentral zu verwalten. Über das MDM können Sicherheitsrichtlinien (z.B. Passwortvorgaben, Verschlüsselung, App-Management, Schnittstellensteuerung) unternehmensweit durchgesetzt werden. Zudem ermöglicht ein MDM im Verlustfall die Fernsperrung oder das Löschen von Unternehmensdaten.	
SP 1.5	Sie die Mitarbeitenden angewiesen, Schnittstellen, die nicht in Gebrauch sind, zu deaktivieren?	UP	Mittelfristig	Deaktivierung von Zugriffspotentialen	24.08.2026	<p>Da mobile Geräte über verschiedene Verbindungs- und Funkfunktionen verfügen, sollten diese nur aktiv sein, wenn sie tatsächlich benötigt werden. Dazu gehören unter anderem Bluetooth, NFC, mobile Hotspots oder GPS. Jede aktivierte Schnittstelle stellt eine potenzielle Angriffsfläche dar und kann von Dritten missbräuchlich ausgenutzt werden – insbesondere dann, wenn sie dauerhaft eingeschaltet bleibt, ohne benötigt zu werden.</p> <p>Mitarbeitende sollten daher angewiesen werden, nur die Schnittstellen zu aktivieren, die sie im konkreten Moment wirklich benötigen, und alle anderen Verbindungsarten auszuschalten. Eine entsprechende interne Anweisung oder Richtlinie unterstützt die Mitarbeitenden dabei, diese Vorsichtsmaßnahmen zuverlässig einzuhalten.</p>	
SP 1.6	Sind Standortberechtigungen der Applikationen ausgeschaltet?	UP	Mittelfristig	Deaktivierung von Standortberechtigungen	24.08.2026	<p>Viele mobile Anwendungen verlangen Zugriff auf Standortdaten, obwohl diese für die tatsächliche Nutzung der App häufig nicht erforderlich sind. Um die Weitergabe und Verarbeitung unnötiger personenbezogener Daten zu vermeiden, sollten Standortberechtigungen grundsätzlich deaktiviert werden, sofern sie nicht zwingend für die Funktion der jeweiligen Anwendung benötigt werden.</p> <p>Mitarbeitende sollten angewiesen werden, Standortzugriffe nur dann zu aktivieren, wenn dies für den konkreten Einsatzzweck notwendig ist, beispielsweise bei Navigations, oder Routenplanungsdiensten. In allen anderen Fällen ist die Standortfreigabe zu verweigern oder auf die Einstellung „Nur während der Nutzung“ zu beschränken.</p>	



DATENSCHUTZ MIT AUGENMAß

# GDI – ZERTIFIKAT

## DATENSCHUTZAUDIT 2026



Bild: Pixabay

Wir, die GDI mbH, bestätigen dem Unternehmen

**KAMAT GmbH & Co. KG**  
Salinger Feld 10, 58454 Witten

aufgrund der im Datenschutzaudit gegebenen Antworten  
ein angemessenes Datenschutzniveau.

Das Unternehmen wurde am **24.02.2026**  
von uns einer jährlichen Datenschutzprüfung unterzogen.

Hagen, den 25.02.2026

i. A.

Frau Oles

*i. A. GDI A. Oles*

**Gesellschaft für Datenschutz  
und Informationssicherheit mbH**

Alter Schloßweg 30  
D- 58119 Hagen  
Tel.: +49 (0)2331 3568320