GDI

DATENSCHUTZ MIT AUGENMAß

GDI – ZERTIFIKAT

DATENSCHUTZAUDIT 2023

Bild: Pixabay

Wir, die GDI mbH, bestätigen dem Unternehmen

HUPFER® Metallwerke GmbH & Co. KG
Dieselstraße 20, 48653 Coesfeld

ein angemessenes Datenschutzniveau.

Das Unternehmen wurde am ***26.09.2023***
von uns einer jährlichen Datenschutzprüfung unterzogen.

Die Forderungen der EU-Datenschutzgrundverordnung und der deutschen Bundes- und ggf. Landesdatenschutzgesetze sind umgesetzt.

Hagen, den 05.10.2023

i. A. Herr Lau
Ass. Jur.

GDI
Gesellschaft für Datenschutz und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

GDI

DATENSCHUTZ MIT AUGENMAß

GDI CERTIFICATE

DATA PROTECTION AUDIT 2023

Bild: Pixabay

We, the GDI mbH, confirm to the company

HUPFER® Metallwerke GmbH & Co. KG
Dieselstraße 20, 48653 Coesfeld

has achieved an adequate level of data privacy.

The company was subjected to an annual inspection
by us on ***26.09.2023***

The requirements of the EU General Data Protection Regulation and German federal and, where applicable, state data protection laws have been implemented.

Hagen, 05/10/23

i. A. Herr Lau
Ass. Jur.

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

EU-DSGVO

Maßnahmenbericht zum datenschutzrechtlichen Audit

Jahr 2023

GDI
DATENSCHUTZ MIT AUGENMAß

für das Unternehmen:

HUPFER® Metallwerke GmbH & Co. KG

Dokumenteninformation	
Stand	*05.10.2023*
Dokumenten-version	*2.4.6.1*
Vorlagen-version	*03/23*
Bearbeitet	*Lau*
Sicherheit	*Vertraulich*
Berechtigung	*Datenschutzkoordinator, Geschäftsführung, IT-Abteilung*
Versendung des Auditberichts	*digital und Papierform*

Auditinformationen	
Kunde	HUPFER® Metallwerke GmbH & Co. KG
Kunden-ID	5006,0
Kunden-Adresse	Dieselstraße 20, 48653 Coesfeld
Branche	Produktionsbetrieb
Branchenkategorie	F
Abteilung	----------
Ansprechpartner:in	Herr Gäbel, Herr Koch
Auditor:in	Herr Lau
Auditdatum	26.09.2023
Durchführung:	Videokonferenz
Umfang	10:00 - 12:25
Schulung	./.
Ergebnis	**Das Unternehmen hat ein angemessenes Datenschutzniveau.**

HUPFER

Dokumentenechtheit

Hagen, den *05.10.2023*

Unterschrift Auditor:in

GDI
Gesellschaft für Datenschutz und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

Firmenstempel

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	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 2023

Maßnahmen aus dem Jahresaudit 2023

ID	Frage	Antwort	Priorität	Themenschwer-punkt	Bearbeitung bis zum:	Maßnahme / Hinweis	Notizen für den Kunden
Wiederkehrendes							**Notizen**
W 1.0	**Vorjahres-Audit:** Wie viele Mitarbeiter hatte das Unternehmen im letzten Jahr?		400	Anzahl der Mitarbeiter			
W 1.1	**Vorjahres-Audit:** Wie viele davon arbeiten mit personenbezogenen Daten?		200	Anzahl der Mitarbeiter			
W 1.2	**Erst-Audit / Wiederholungs-audit:** Wie viele Mitarbeiter hat das Unternehmen aktuell?		400	Anzahl der Mitarbeiter			
W 1.3	**Erst-Audit / Wiederholungs-audit:** Wie viele Personen arbeiten mit personenbezogenen Daten?		200	Anzahl der Mitarbeiter			
W 1.10	Gibt es neue Softwaresysteme?	*Ja*	Kurzfristig	Anschaffung neuer Softwaresysteme zur Datenverarbeitung	26.12.2023	Die Anschaffung neuer Software sollte im Vorhinein mit dem DSB des Unternehmens koordiniert werden. Der DSB prüft die Software hinsichtlich einer datenschutzkonformen Datenverarbeitung. Die vorherige Prüfung und Freigabe neuer Software ist von Art. 25 und 32 DS-GVO erfasst. Je höher die Risiken für den Betroffenen durch die (geplante) Verarbeitung voraussichtlich sind, muss vorab eine Datenschutzfolgenabschätzung erfolgen.	*Testphase Viva Engage (Derivat MS 365)* *Es soll eine Informationsplattform geschaffen werden zwischen Niederlassung und Zentrale*
Grundlegende Anforderungen der DSGVO							**Notizen**
Allgemeines							
A 1.1	Haben Sie die Datenschutz-hinweise für Ihre Mitarbeiter dokumentiert bekannt gegeben?	*Ja*	Langfristig	Transparenzpflicht	26.09.2024	Alle Datenverarbeitungen des Unternehmens müssen den betroffenen Personengruppen gegenüber transparent dargestellt und offengelegt werden.	

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

A 1.2	Wie ist die Bekanntgabe erfolgt?			Bekanntgabe	*über Wiki*		
A 1.3	Haben Sie die Datenschutz-hinweise für Ihre Kunden dokumentiert bekannt gegeben?	*Ja*	Langfristig	Transparenzpflicht	26.09.2024	Alle Datenverarbeitungen des Unternehmens müssen den betroffenen Personengruppen gegenüber transparent dargestellt und offengelegt werden.	
A 1.4	Wie ist die Bekanntgabe erfolgt?			Bekanntgabe	*Stehen auf der Homepage, kein Hinweis in E-Mails und geschäftlichen Briefen*		
A 1.5	Haben Sie die Datenschutz-hinweise für Bewerber dokumentiert bekannt gegeben?	*Ja*	Langfristig	Transparenzpflicht	26.09.2024	Alle Datenverarbeitungen des Unternehmens müssen den betroffenen Personengruppen gegenüber transparent dargestellt und offengelegt werden.	
A 1.6	Wie ist die Bekanntgabe erfolgt?			Bekanntgabe	*Eingestellt auf der Webseite*		*Die Datenschutzhinweise für Bewerber sollten in der jeweiligen Stellenanzeige auf der Webseite verlinkt werden.*
A 1.7	Sind die Beschäftigten schriftlich auf die Vertraulichkeit verpflichtet worden?	*Nein*	Kurzfristig	Vertraulichkeit	26.12.2023	Alle Beschäftigten, die personenbezogene Daten verarbeiten oder mit diesen in Berührung kommen, müssen auf die Vertraulichkeit verpflichtet werden.	*Auszug aus dem Arbeitsvertrag:* *"§ 10 Verschwiegenheitspflicht* *Über alle betrieblichen Angelegenheiten, die Ihnen im Rahmen oder aus Anlass Ihrer Tätigkeit bei HUPFER® zur Kenntnis gelangen, verpflichten Sie sich -auch nach Ihrem Ausscheiden- Stillschweigen zu bewahren. Bei Beendigung des Arbeitsverhältnisses sind alle betrieblichen Unterlagen, Urkunden, Aufzeichnungen, Notizen, Entwürfe oder hiervon gefertigte Durchschriften oder Kopien, gleichgültig auf welchem Datenträger, an HUPFER® herauszugeben.* *§ 14 Datenverarbeitung und Datenschutz* *Zur Unterstützung der internen betrieblichen Abläufe werden persönlichen Daten und Ihre Anwesenheits-, Fehl- und Urlaubszeiten unseren Mitarbeitern systemtechnisch als Planungsinstrument und zu Informationszwecken zur Verfügung gestellt und hierdurch intern veröffentlicht sowie gespeichert. Das Bundesdatenschutzgesetz findet Anwendung.*

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

IT-Sicherheit und TOM							Notizen
IT-Sicherheit : Grundlagen							
WT 1.5	Haben Sie Ihre eigenen TOM entsprechend Art. 32 DSGVO dokumentiert?	*UP*	Mittelfristig	Dokumentation TOM	26.03.2024	Bitte prüfen Sie, ob für das Unternehmen die eingerichteten technischen und organisatorischen Maßnahmen dokumentiert wurden.	*Das Notfallhandbuch enthält keine Dokumentation der technischen und organisatorischen Maßnahmen, lediglich Beschreibungen von Prozessabläufen. Eine Dokumentation der TOM findet sich aber im Verzeichnis der Verarbeitungstätigkeiten.*
WT 1.6	Haben sich Ihre TOM (Maßnahmen, Verfahren oder Techniken zur Datensicherung oder zur allgemeinen Unternehmenssicherheit, z.B. Außenschutz, Zutrittskontrolle, Benutzeridentifizierung, Datenzugriff, Verschlüsselung, Schlüsselrechte etc.) geändert? Haben Sie diese Änderungen dokumentiert?	*Nein*	Mittelfristig	Dokumentation der Änderungen der TOM	26.03.2024	Änderungen/Anpassungen der technischen und organisatorischen Maßnahmen sollten immer in der Dokumentation ergänzt werden.	
WT 1.7	Ist eine regelmäßige Prüfung der technischen und organisatorischen Maßnahmen auf Aktualität gewährleistet?	*Hinweis*	Langfristig	Maßnahmen auf Stand der Technik	26.09.2024	Es sollte ein geeigneter Kontrollmechanismus etabliert werden, um zu gewährleisten, dass die technischen und organisatorischen Maßnahmen des Unternehmens auf dem Stand der Technik sind.	

Auftragsverarbeitung							Notizen
Auftraggeber der Auftragsverarbeiter							
AV 4.0	Gibt es eine Liste aller Auftrags-verarbeiter?	*Ja*	Mittelfristig	Liste aller Auftragsverarbeiter	26.03.2024	Es muss eine Liste aller Auftragsverarbeiter des Unternehmens erstellt werden.	
AV 4.3	Liegen regelmäßige Sicherheits-nachweise der Auftragnehmer vor? Wird die Funktionsweise der TOMs bestätigt? Hat der Auftragnehmer ein Datenschutz-Zertifikat vorgelegt?	*UP*	Langfristig	Sicherheitsnach-weise / Nachweise der Funktions-fähigkeit der Sicherungsmaßnahme n	26.09.2024	Es sollte sichergestellt werden, dass alle Auftragsverarbeiter regelmäßig Sicherheitsnachweise und Nachweise über die Funktionsfähigkeit Ihrer technischen und organisatorischen Maßnahmen vorlegen. Bitte überprüfen Sie, ob Sicherheitsnachweise und Nachweise vorliegen oder ob der Auftragsverarbeiter, soweit vorhanden, ein regelmäßig aktualisiertes Datenschutz-Zertifikat vorlegen kann.	
AV 4.4	Sind Kontrollen etabliert, ob der Dienstleister seine Verträge auch erfüllt und einhält?	*Hinweis*	Langfristig	Kontrollen und Überprüfungen der Dienstleister	26.09.2024	Es sollten eigene Kontrollen eingerichtet werden, ob Dienstleister des Unternehmens auch Ihre zugesicherten Sicherheitsmaßnahmen im Alltag einhalten.	

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

Personal						Notizen
Zeiterfassung						
AZD 1.0	Erfassen Sie Arbeitszeitdaten Ihrer Mitarbeiter?	*Ja*	Kurzfristig	Zeiterfassung	26.12.2023	*In seinem Beschluss vom 13.09.2022 (Az.: ABR 22/21) interpretiert das Bundesarbeitsgericht (BAG) den § 3 Abs. 2 Nr. 1 ArbSchG unionrechtskonform dahingehend, dass alle Arbeitgeber, als eine der erforderlichen Maßnahme zum Gesundheitsschutz, ein System zur Arbeitszeiterfassung einführen müssen. Das Ziel ist eine systematisch, korrekte, objektive und genaue Erfassung. Die Arbeitszeiterfassung kann auf die unterschiedlichsten Arten durchgeführt werden: der klassische Stundenzettel, die Stempeluhr, Softwares, Apps. Da es sich auch bei diesen Daten um personenbezogene Daten i.S.d. DSGVO handelt, sind die datenschutzrechtlichen Anforderungen zu beachten.*	
AZD 1.1	Wenn ja: Erfolgt die Erfassung in Papierform oder digital?	*digital*		Art der Zeiterfassung			
AZD 1.4	Werden die erfassten Arbeitszeitdaten gem. § 16 Abs. 2 ArbZG nach spätestens 2 Jahren gelöscht?	*Hinweis*	Langfristig	Aufbewahrungsfrist	26.09.2024	Für die erfassten Arbeitszeitdaten sollte eine Aufbewahrungsfrist festgelegt werden. Nach § 16 Abs. 2 ArbZG ist der Arbeitgeber verpflichtet, die Dokumentation der Überstunden mindestens 2 Jahre aufzubewahren. Im Übrigen können steuerrechtliche Aufbewahrungspflichten anwendbar sein (bspw. im Rahmen der Abgabenordnung), weshalb steuerrelevante Daten der Arbeitszeiterfassung für 10 Jahre aufbewahrt werden müssen. Sonstige Abwesenheitszeiten sollten bis zu 2 Jahre aufbewahrt werden.	
Nutzung der Infrastruktur des Unternehmens						
P 1.2	Wird das Versenden von Massenmails unterbunden?	*UP*	Mittelfristig	Verbot von Massenmails	26.03.2024	Bitte prüfen Sie, ob der Versand von Massenmails unterbunden wird.	
P 1.3	Sind Maßnahmen eingerichtet worden, die das Risiko, eine E-Mail an einen falschen Empfänger zu versenden, verringern?	*UP*	Kurzfristig	E-Mail: falscher Empfänger	26.12.2023	Bitte prüfen Sie, ob Maßnahmen eingerichtet sind, die das Risiko, eine E-Mail an einen falschen Empfänger zu versenden, verringern. Der Versand einer E-Mail an einen falschen Empfänger kann einen, ggf. meldepflichtigen, Datenschutzvorfall darstellen. Als Maßnahme kommt z.B. in Betracht, die "Erinnerungsfunkton" des E-Mail-Programm an bereits genutzte E-Mail-Adressen auszuschalten.	
Einsatz von Videokonferenz-Tools im Unternehmen						
VK 1.0	Setzen Sie aktiv Videokonferenz-Tools im Unternehmen ein (z.B. WebEx, Teams, Zoom, etc.)	*Ja*	Mittelfristig	*MS Teams*		

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

VK 1.1	Bietet das Tool eine Ende-zu-Ende-Verschlüsselung an?	*UP*	Kurzfristig	Ende-zu-Ende-Verschlüsselung	26.12.2023	Bitte prüfen Sie, ob das eingesetzte Videokonferenztool eine Ende-zu-Ende-Verschlüsselung ermöglicht. Bei einer Ende-zu-Ende-Verschlüsselung kann niemand außer den Teilnehmern einer Videokonferenz auf die Audio- und Video-Daten zugreifen, d.h. weder bei der Übertragung noch die Software auf den Endgeräten (Browser oder Apps). Bitte beachten Sie, dass die Ende-zu-Ende-Verschlüsselung ggf. nicht voreingestellt ist, sondern aktiviert werden muss. Nehmen Sie zur Fragen hierzu Kontakt zu Ihrem System-Administrator auf.	
VK 1.6	Stellen Sie den Teilnehmern der Videokonferenz, die von Ihrem Unternehmen angesetzt wurde, die Datenschutzhinweise zur Verfügung?	*Nein*	Kurzfristig	Datenschutzhin-weise für Teilnehmer	26.12.2023	Bei Durchführung einer Videokonferenz müssen den Teilnehmern Datenschutzhinweise gem. Art. 13 DS-GVO zur Verfügung stellen. Dies erfolgt z.B. mit der Einladung.	
Home-Office Arbeitsplätze / Mobiles Arbeiten							
HO 1.0	Bieten Sie für ihre Mitarbeiter Home Office oder mobiles Arbeiten an?	Home Office und Mobiles Arbeiten		*Außendienst macht Home Office*			
HO 1.3	Arbeitszimmer abschließbar?	*Hinweis*	Kurzfristig	Home Office	26.12.2023	Das Arbeitszimmer im Home Office sollte separat abschließbar sein.	
Infrastruktur und IT-Sicherheit im Gebrauch							**Notizen**
Serverraum							
SR 1.0	Verfügen Sie über einen eigenen Serverraum oder ist der Serverstandort ausgelagert?	*im Haus*				2 Brandabschnitte, arbreiten redundant	
SR 1.3	Sind im Serverraum wasserführende Leitungen, z.B. Heizung?	*UP*	Langfristig	Wasserführende Leitungen			
SR 1.4	*Wenn Ja:* Führen diese Leitungen über den Serverschrank oder seitlich an ihm vorbei?	*UP*	Langfristig	Schutz gegen austretendes Wasser	26.09.2024	Bitte prüfen Sie, ob der Server unter oder neben wasserführenden Leitungen steht. Wenn ein Wasserrohr platzt, kann Wasser in den Server laufen und diesen zerstören. Wenn eine Umstellung nicht möglich ist, müssen Maßnahmen eingerichtet werden, die ein Eindringen von Wasser in den Server unterbinden. Des Weiteren sollte dann Feuchtigkeitsmesser am Boden angebracht werden.	
SR 1.9	Ist die Zugangstür zum Serverraum eine Feuerschutztür?	*UP*	Langfristig	Feuerschutztür	26.09.2024	Bitte prüfen Sie, ob die Zugangstür zum Serverraum eine Feuerschutztür ist.	

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

Umgang mit Smartphones / Tablets

SP 1.0	Wie viele dienstliche Smartphones und Tablets werden im Unternehmen eingesetzt?			dienstliche Smartphones und Tablets	*ca. 135*	
SP 1.2	*Bei mehr als 20 dienstlichen Geräten:* Werden dienstliche Smartphones und Tablets über eine Mobile-Device-Management-Lösung verwaltet?	*Nein*	Mittelfristig	MDM	26.03.2024	Über ein Mobile-Device-Management können unternehmensweite Sicherheitsstandards für Benutzer, Geräte und Netzwerke an zentraler Stelle für alle Geräte festgelegt und angewendet werden. So lassen sich z.B. globale Vorgaben für die Passwortlänge, für den Zugriff auf WLAN-Netzwerke, für die Nutzung von Schnittstellen wie Bluetooth oder Kameras, Installation von Apps, etc. setzen. Sämtliche Daten können zudem verschlüsselt und so vor unberechtigtem Zugriff geschützt werden. Im Fall von Diebstahl oder Verlust kann über das MDM auf das entsprechende Gerät zugegriffen werden. So ist möglich, den Zugriff auf die Daten innerhalb des gesicherten Workspace über die Fernverwaltung zu sperren oder die Daten vollständig zu löschen.
SP 1.7	Ist die Nutzung von WhatsApp auf dienstlichen Geräten verboten?	*Nein*	Mittelfristig	Verbot von WhatsApp	26.03.2024	Die Nutzung von WhatsApp auf dienstlichen Smartphones sollte aus datenschutzrechtlichen (und rechtlichen) Gründen verboten werden. WhatsApp sendet die im Telefonbuch enthaltenen Telefonnummern beim Start an Server in den USA. Dies geht aber nur mit einer Einwilligung der jeweiligen Kontakte, die das Unternehmen i.d.R. nicht hat.
SP 1.8	Einwilligung, wenn Applikationen wie z.B. WhatsApp Kontakt-informationen liest?	*Nein*	Kurzfristig	Einwilligung bei Datenweitergabe an Dritte	26.12.2023	Bitte stellen Sie sicher, dass berufliche und private Kontakte auf dem dienstlichen Smartphone getrennt gespeichert werden und dass diese beruflichen Kontakte nicht ohne Einwilligung durch eine Messenger-Applikation wie WhatsApp gelesen und in ein unsicheres Drittland übertragen werden.

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0

Sonstige Bemerkungen / Hinweise	
S1	Die GDI bietet zur Schulung der Mitarbeiter:innen Online-Webinare an, die zu individuellen Daten und Zeiten zur Verfügung gestellt werden können. Wir übermitteln einen Stundenplan mit den angebotenen Inhalten. Es eignen sich insbesondere die "Grundlagenschulung zur Sensibilisierung" und die "Sensibilisierung Datenschutzprozesse". Kontaktieren Sie uns gerne unter datenschutz@gdi-mbh.eu um einen Termin zu vereinbaren.
S2	Die Einladung zur Teilnahme an der Moodle-Schulung wird an Herrn Gäbel und Herrn Koch versendet.
S3	
S4	
S5	

GDI
Gesellschaft für Datenschutz
und Informationssicherheit mbH
Körnerstraße 45
D- 58095 Hagen
Tel.: +49 (0) 2331 356832-0