Auftragsverarbeitung nach DSGVO

CEMA Gruppe

Anlagen

CEMA GmbH Spezialisten
für Informationstechnologie
Dortmund

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

CEMA GmbH Spezialisten für
Informationstechnologie
Dortmund

Anlage 1: Liste der Hauptverträge

Diese Anlage beschreibt die konkret vereinbarten Rahmenbedingungen der geplanten Verarbeitungen und dient der Umsetzung der jeweils geltenden gesetzlichen Anforderungen durch konkrete Festlegungen.

Bezeichnung des Vertrages	Vertragsbeginn	Laufzeit bis	Vertragsinhalt

Anlage 2 Angaben des Auftraggebers

Auftraggeber:	
Firma:	
Straße und Hausnummer:	
Postleitzahl und Ort:	
Name des Datenschutzbeauftragten:	
Postanschrift Datenschutzbeauftragter:	Firma, Abteilung:
E-Mail Datenschutzbeauftragter:	Telefonnummer des Datenschutzbeauftragten:
Name der weisungsberechtigten Person/en[1]:	

[1] Nach der DSGVO ist zwingend sicherzustellen, dass alle Weisungen des Auftraggebers zu den näheren Umständen der Datenverarbeitung dokumentiert und strikt befolgt/kontrolliert werden. Deshalb sind diese Weisungen nur an eine konkret benannte und berechtigte Person weiterzuleiten und nur dann verbindlich. Diese Person ist für die Dokumentation jeder Weisung im Verzeichnis von Verarbeitungen (VvV) verantwortlich.

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

Erfolgt die Verarbeitung im Auftrag anderer Verantwortlicher[2] bzw. weiterer Auftraggeber?[3]					
JA	☐	NEIN	☐	Wenn ja, Kontaktdaten der weiteren Auftraggeber[4]:	
Zweck/e/Rechtsgrundlagen der Datenverarbeitung[5]:					
betroffener Personenkreis[6]:					
voraussichtliche Anzahl von Datensätzen[7]:					

[2] Verantwortlicher für eine Datenverarbeitung ist immer diejenige Organisation, die über die Zwecke und Mittel der Datenverarbeitung entscheidet, also in der Regel der Vertragspartner des Betroffenen bei Endkunden oder der Arbeitgeber bei der Verarbeitung von Beschäftigtendaten.

[3] Datenschutzrechtlich Verantwortlicher ist derjenige, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Im Fall einer Unterbeauftragung ist es erforderlich, die Angaben des Verantwortlichen zu erfassen.

[4] Soweit die weiteren Auftraggeber noch nicht oder nur mit erheblichem Aufwand jeweils aktuell benannt werden können, ist das Verfahren gemäß Absatz 10 Punkt 3 Anwendungsbereich und Verantwortlichkeiten zu vereinbaren.

[5] Bitte den Zweck und die Rechtsgrundlage für die dem Auftrag zugrundeliegende Datenverarbeitung aus Sicht des Auftraggebers mitteilen, zum Beispiel: elektronische Speicherung und Verarbeitung von Patientendaten zur Durchführung ärztlicher Behandlungen.

[6] Betroffene sind immer diejenige, deren Daten verarbeitet werden. Hierzu gehören nicht nur Kundendaten, sondern auch Beschäftigtendaten in technischen Protokolldaten.

[7] Hier geht es um eine grobe Schätzung des maximalen Umfangs betroffener Personen für die Datenschutzfolgenabschätzung/Risikobewertung.

Geschäftsführer: Johannes Tewes, Markus Radtke
Amtsgericht: Dortmund HR: 24141
Commerzbank AG; COBADEFFXXX
DE15 6704 0031 0620 7005 00

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

CEMA GmbH Spezialisten für Informationstechnologie Dortmund

Kategorien von Daten und Datenverarbeitungen: (Zutreffendes JA/NEIN ankreuzen)		
JA		NEIN
	Personenbezogene oder personenbeziehbare Daten?	
☐	„personenbezogene Daten“: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.	☐
	Besondere Kategorien personenbezogener Daten?	
☐	Daten über rassische und ethnische Herkunft	☐
☐	Daten über politische Meinungen	☐
☐	Daten über religiöse oder weltanschauliche Überzeugungen	☐
☐	Daten zur Gewerkschaftszugehörigkeit	☐
☐	Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person	☐
☐	Gesundheitsdaten: personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen	☐
☐	biometrische Daten: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten, (Videoaufzeichnungen, Fingerabdrucksensoren, Gesichtsbilder)	☐
☐	genetische Daten: personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser	☐

	natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.	
☐	Angaben zu Bank- oder Kreditkartenkonten	☐
☐	Einkommens- oder Vermögensangaben	☐
☐	personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln	☐
☐	Daten für eine automatisierte Entscheidungsfindung einschließlich Profiling	☐
☐	Sonstiges:	☐

Ist im Rahmen dieses Auftrages eine Übermittlung von Daten in ein Drittland oder eine internationale Organisation vorgesehen?					
JA	☐	NEIN	☐	Wenn ja, welche?	

Anlage 3: Angaben des Auftragnehmers/Auftragsverarbeiters

Auftragnehmer/Auftragsverarbeiter:	
Firma:	
CEMA GmbH Spezialisten für Informationstechnologie	
Postanschrift:	
Freie-Vogel-Straße 369 44269 Dortmund	
Name und Vorname des Datenschutzbeauftragten:	
Clemens Dorner	
Postanschrift Datenschutzbeauftragter:	Firma, Abteilung:
Joseph-Schumpeter-Allee 25 53227 Bonn	2B Advice GmbH
E-Mail Datenschutzbeauftragter:	Telefonnummer des Datenschutzbeauftragten:
CEMA@2b-advice.com	+49 228 926165 120
Name der berechtigten Weisungsempfänger:[8]	
Rolf Braun	
E-Mail berechtigte Weisungsempfänger:	Telefonnummer der berechtigten Weisungsempfänger:
DSGVO@cema.de	0621-3398-121

[8] Nach der DSGVO ist zwingend sicherzustellen, dass alle Weisungen des Auftraggebers zu den näheren Umständen der Datenverarbeitung dokumentiert und strikt befolgt/kontrolliert werden. Deshalb sind diese Weisungen nur an eine konkret benannte und berechtigte Person weiterzuleiten und nur dann verbindlich. Diese Person ist für die Dokumentation jeder Weisung im Verzeichnis von Verarbeitungen (VvV) verantwortlich.

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

CEMA GmbH Spezialisten für Informationstechnologie Dortmund

Ort/e der Datenverarbeitung (Postanschrift/en):					
s.o. wie Auftragnehmer und Harrlachweg 5, 68163 Mannheim					
Löschfristen:					
Vertragsende unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen					
Ist eine Übermittlung von Daten in ein Drittland oder eine internationale Organisation vorgesehen?					
JA	☐	NEIN	☒	Wenn ja, welche?	
Wenn JA: Gibt es hier einen Angemessenheitsbeschluss oder welche anderen geeigneten Garantien (Art. 46, 47) bzw. Gründe für eine Ausnahme (Art. 49)?					

Anlage 4: Unterauftragsverarbeiter

Der Auftraggeber genehmigt den Einsatz folgender weiterer (Unter-)Auftragsverarbeiter:

Name Auftragverarbeiter	Orte der Datenverarbeitung (Land, Ort)	Art der Datenverarbeitung	Rechtsgrundlage bei Drittlandübermittlung
Global Access Internet Services GmbH Potsdamer Str. 3 80802 München	München, Deutschland	Cloud, IaaS	Nicht erforderlich
QualityHosting AG Uferweg 40-42 63571 Gelnhausen	Frankfurt, Deutschland	Managed Exchange	Nicht erforderlich
PfalzKom, Gesellschaft für Telekommunikation mbH Koschatplatz 1 67061 Ludwigshafen	Mutterstadt, Deutschland	Housing, Cloud, IaaS	Nicht erforderlich
wusys GmbH Vilbeler Landstraße 255 60388 Frankfurt am Main	Offenbach, Deutschland	Housing	Nicht erforderlich
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Weltweit	Sharepoint, Exchange, OneDrive	EU-US-Privacy Shield EU--Standardvertragsklauseln
A E1NS IT GmbH Am kleinen Rotenberg 21 54516 Wittlich	Wittlich, Deutschland	Cloud	Nicht erforderlich

NTT DATA Romania S.A. Str. Constanta Nr. 19-21 400158 Cluj-Napoca, Rumänien	Cluj-Napoca, Rumänien	Managed Services	Nicht erforderlich
ADN GmbH Josef-Haumann-Str. 10 44866 Bochum	Bochum, Deutschland	Cloud	Nicht erforderlich

Anlage 5: Technische und organisatorische Maßnahmen

Liegt eine Datenverarbeitung im Auftrag vor, ist der Auftragsverarbeiter nicht Dritter im Sinne der Datenschutzgesetzgebung und der Auftraggeber bleibt im Außenverhältnis datenschutzrechtlich Verantwortlicher.

Der Auftraggeber ist deshalb verpflichtet sich davon zu überzeugen, dass beim Datenverarbeiter die technischen und organisatorischen Maßnahmen getroffen werden, die für die Art der Verarbeitung angemessen und erforderlich sind.

Diese Anlage beschreibt die bei dem Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, mit denen die Umsetzung der technisch-organisatorischen Maßnahmen gemäß § 9 BDSG / Art. 32 DSGVO gewährleistet sind.

Die Darstellung bezeichnet konkrete Maßnahmen, die eingesetzt werden, um im Verhältnis zum Schutzzweck und der Art der Daten, die verarbeiteten Daten vor einem möglichen Missbrauch zu schützen.

Zutrittskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Die Zutrittskontrolle verlangt, Unbefugten den körperlichen Zutritt zur Datenverarbeitungsanlage, mit der personenbezogene Daten verarbeitet werden, zu verwehren. Es soll verhindert werden, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen kommen. **Ziel:** Durch die Zutrittskontrolle soll von vornherein die Möglichkeit unbefugter Kenntnis- und Einflussnahme, aber auch eine Zerstörung der Anlage(n) ausgeschlossen werden.	• Bauliche Absicherung *(Gebäudesicherheitskonzept, Protokollierung Zu- und Abgänge)* • Organisatorische Absicherung *(Schlüsselordnung, Codekarten, Besucherausweise)* • Rechnerräume Closed Shop Betrieb *(Raumüberwachung, Aufstellungsort Server, Bewegungsfreiheit Wartungspersonal)*
Bei dem Auftragsverarbeiter realisierte Maßnahmen: Das neue Gebäude ist Vermieterseitig mit einem Zutrittskontrollsystem ausgestattet: Token für Mitarbeiter der Mietparteien und Lesegeräte an Außentüren, den Etagenzugängen sowie an weiteren	

Sicherheitsbereichen, z.B. Serverraum. Die Büros der Geschäftsführer der CEMA Gesellschaften sind mit Schlüsseln einer Schließanlage ausgestattet. Die Räume der CEMA Gesellschaften sind zusätzlich mit Alarmanlage und Bewegungsmelder ausgestattet.

Außentüren sind außerhalb der üblichen Dienstzeiten verschlossen; Besucher müssen sich über Türsprechanlage und Klingel am Empfang anmelden. Der Empfang ist durch eine Mitarbeiterin besetzt.

Prinzipiell wird nur der Zugang beim Vermieter protokolliert, jedoch bei zusätzlicher Alarmanlagenüberwachung das Ein- und Ausschalten mittels der gleichen Token auf Seiten CEMA.

Eine Auswertung der Zutrittsprotokollierung findet nur bei besonderer Veranlassung statt.

Der Serverraum hat eine zutrittsgesicherte Türe.

Bewegungsmelder zur Alarmanlage ist installiert. Codierte Token für Serverraum; IT Betriebs Mitarbeiter (6 Personen) sowie Feuerwehr (Generaltoken für Gebäude) sind befugt

Besucher und Wartungsdienste werden begleitet. Die Reinigungskraft wird begleitet, falls erforderlich.

Jeder Besucher muss sich am Empfang melden, da Etagentüren und Serverraum verschlossen sind. Jeder Besucher muss sich ausweisen und erhält einen Besucherausweis.

Zugangskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Im Gegensatz zur Zutrittskontrolle ist hiermit der Schutz vor einem Eindringen unbefugter Personen in das EDV System selbst, also dessen Benutzung, beabsichtigt. Es müssen daher Maßnahmen getroffen werden, die das unberechtigte Eindringen in die EDV-Systeme verhindern. **Ziel:** Die Zugangskontrolle soll die unbefugte Nutzung von Datenverarbeitungssystemen verhindern.	• Kontrollmaßnahmen *(Regelwerk, Benutzerregistrierung)* • Netzwerk *(Freigabe von Netzzugängen, Penetrationstests.)* • Wartung *(Verbindungsaufbau Fernwartung, Mitnahmen DV-Equipment zu Wartungszwecken)*
Bei dem Auftragsverarbeiter realisierte Maßnahmen Auf Gruppenebene bekommen Mitarbeiter die erforderlichen Zugangsrechte über Infopath -Workflow mit Vorgesetztenfreigabe der Anforderung, Ticket zur Realisierung im Ticketsystem und Rückantwort an anfordernden Vorgesetzten. Alle Administrationszugriffe erfolgen mit NamedUser Administrationskonten. Für Gäste gibt es ein Gast W-LAN. Betriebsfremde Hardware darf ausschließlich im Gast WLAN genutzt werden. Benutzung des internen Netzwerks ist nur nach interner Freischaltung möglich.	

Zugriffskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Maßnahmen der Zugriffskontrolle müssen geeignet sein, zu gewährleisten, dass ausschließlich die zur Benutzung des Systems berechtigten Personen auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. **Ziel:** Personenbezogene Daten sollen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	• Zugriffsschutzmaßnahmen *(Clean Desk, Sicherheitssoftware, Verschlüsselung)* • Sicher Entsorgung *(Entsorgung von Papierdokumenten, Beachtung von Aufbewahrungsfristen)*

Bei dem Auftragsverarbeiter realisierte Maßnahmen

Passwortschutz ist Pflicht; komplexes PWD und 60 Tage PWD Wechselintervall.

Auf Gruppenebene bekommen Mitarbeiter die erforderlichen Zugangsrechte über Infopath -Workflow mit Vorgesetztenfreigabe der Anforderung, Ticket zur Realisierung im Ticketsystem und Rückantwort an anfordernden Vorgesetzten.

Alle Administrationszugriffe erfolgen mit NamedUser Administrationskonten

Alle notwendigen Administrationskennworte sind Mandanten separat in einem Password Safe hinterlegt, mittels Login Kontrolle und über spezifische Berechtigungen nur an Betriebsmitarbeiter im Zugriff.

Das WLAN ist über WPA 2 Verschlüsselung mit Zertifikat sowie durch Prüfung mit Active Directory geschützt.

Papierdokumente werden nach Ablauf der gesetzlichen Aufbewahrungsfrist im Shredder bzw. über einen Dienstleister datenschutzgerecht vernichtet. EDV Geräte werden ebenfalls fachgerecht entsorgt.

Weitergabekontrolle

Anforderung und Ziel	Beispiele
Anforderung: Maßnahmen zur Weitergabekontrolle müssen geeignet sein, um sicherzustellen, das personenbezogene Daten bei der Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zu diesen Maßnahmen gehört regelmäßig auch die überprüfbare Dokumentation, welche Empfänger personenbezogene Daten erhalten haben. **Ziel:** Es soll verhindert werden, dass unberechtigte Dritte Kenntnis von personenbezogenen Daten erhalten. Es soll ermöglicht werden zu überprüfen und festzustellen, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind.	• Physische Datenübergabe *(Weitergabe von Datenträgern, Belege Datenübergabe, Richtigkeit Adressat)* • Elektronische Datenübermittlung *(Protokollierung, Datenverschlüsselung)*
Bei dem Auftragsverarbeiter realisierte Maßnahmen Eine physikalische Datenübergabe findet nicht statt. Elektronische Daten werden in sich verschlüsselt und über VPN Tunnel verschlüsselt übertragen. Alle in der Cloud befindlichen Daten, werden in einer deutschen Cloud gespeichert und niemals im Ausland.	

Eingabekontrolle

Anforderung und Ziel	Beispiele
Anforderung: Die Maßnahmen zur Eingabekontrolle müssen gewährleisten, dass alle sicherheitsrelevanten Abläufe und alle Vorgänge, die personenbezogene Daten betreffen, durch das System protokolliert (geloggt) werden. **Ziel:** Mit der Eingabekontrolle soll gewährleistet werden, dass (durch den DSB oder die Aufsichtsbehörde) nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.	• Protokolle *(Auswertungsarten, Bearbeitung Sicherheitsverstöße, Aufbewahrung)*
Bei dem Auftragsverarbeiter realisierte Maßnahmen Es findet keine Eingabekontrolle oder -protokollierung statt, da diese nicht erforderlich ist. Das CEMA genutzte ITSM Tool ist revisionssicher eingerichtet und die Daten bleiben bis Vertragende gespeichert.	

Auftragskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Die Auftragskontrolle verpflichtet den Auftragsverarbeiter, den Auftrag, bei den personenbezogenen Daten verarbeitet oder genutzt werden, gemäß den Vorschriften des Datenschutzes und den Vorgaben des Auftraggebers abzuwickeln und dem Auftraggeber als verantwortliche Stelle Kontrollen vor Ort zu ermöglichen. Maßnahmen zur Auftragskontrolle müssen sicherstellen, dass die überlassenen Daten nur im Rahmen des Auftrages verarbeitet werden können. **Ziel:** Unklare Regelungen sollen vermieden und Datenschutzverstöße durch unsachgemäßen Umgang mit Daten bei dem Auftragsverarbeiter ausgeschlossen werden.	• Weisungsgemäße Auftragsverarbeitung *(Kontrolle Einhaltung Weisungen, Vereinbarung Subunternehmer)* • Meldung Datenschutzverstöße *(Meldesystem, Schulung)*

Bei dem Auftragsverarbeiter realisierte Maßnahmen

Es werden keine Dienstleister in die Abarbeitung von Kundenaufträgen einbezogen. Die CEMA Mitarbeiter werden regelmäßig geschult und verpflichten sich auf sachgemäßen Umgang mit den Ihnen im Rahmen Ihrer Aufgaben zur Verfügung gestellten Daten. Führungskräfte weisen Ihre Mitarbeiter regelmäßig auf den sachgemäßen Umgang und die Datenschutzverordnung hin und überprüfen die Einhaltung stichprobenartig.

Verfügbarkeitskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Maßnahmen zur Verfügbarkeitskontrolle müssen sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder „verloren“ gehen. **Ziel:** Negative Auswirkungen für den Betroffenen durch die unbeabsichtigte Löschung von Daten sollen verhindert werden. Die Verfügbarkeit der Daten ist für die ordnungsgemäße Erfüllung der Verarbeitungszwecke notwendige Voraussetzung. Dazu gehören ausreichende Kapazitäten auch bei einer Überlast und die Fähigkeit zur Wiederherstellbarkeit der Funktionsfähigkeit in einem angemessenen Zeitraum.	• Risiko und Schwachstellenanalyse *(Existenz, Prozess Beseitigung von Schwachstellen)* • USV, Überspannungsschutz *(Sicherheitsmaßnahmen, Dokumentation, Überwachung)* • Branderkennung *(Frühwarnsystem, Rufanlage, Aufbewahrung, Schlüssel im Alarmfall)* • Backupkonzept *(Verantwortlichkeiten, Schutz- vor Diebstahl, Funktionalitätstest)*

Bei dem Auftragsverarbeiter realisierte Maßnahmen

Gebäude ist nicht direkt durch Überschwemmung gefährdet. Dennoch hat man für den Serverraum im Keller einen zusätzlichen Hohlraumboden gebaut, um gegen Starkregenfolgen / Überschwemmungen der Tiefgarage geschützt zu sein.

Alle Datenleitungen, Stromversorgung sowie Leitungen für Wärme und Wasser sind unterirdisch bis zum Gebäude verlegt.

Die Serverräume sind im 1. TG im Inneren des Gebäudes in einem eigenständigen Brandabschnitt untergebracht. Alle Geräte hängen an USV; USV stellt den geregelten Shut Down der Systeme sicher.

Notbetrieb ist über Handys und Notebooks möglich.

Die Alarmanlage ist an die Leitstelle des Wachdienstes angeschlossen,

Die Brandschutzmeldeanlage hat eine direkte Anbindung an die Feuerwehr.

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

CEMA GmbH Spezialisten für
Informationstechnologie
Dortmund

Es existiert ein Notfallhandbuch das verschiedene Szenarien abdeckt. U.a. ein Wiederanlaufplan bei einem Totalausfall.

Das Backup-Konzept ist dokumentiert und wird kontinuierlich erweitert. Teil des Konzepts, ist die Auslagerung der Daten auf Magnetbänder. Diese werden außerhalb der der Immobilie in einem Tresor gesichert.

Geschäftsführer: Johannes Tewes, Markus Radtke
Amtsgericht: Dortmund HR: 24141
Commerzbank AG; COBADEFFXXX
DE15 6704 0031 0620 7005 00

Trennungskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Maßnahmen der Trennungskontrolle müssen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können. Eine Trennung darf nicht nur auf einem System oder nur auf dem Hauptsystem realisiert sein, sondern muss für die davon betroffenen Verfahren insgesamt durchgängig umgesetzt sein. **Ziel:** Die Trennungskontrolle dient der technischen Umsetzung des Prinzips der Zweckbindung und der Datensparsamkeit. Es soll verhindert werden, dass Personen Daten verarbeiten, welche für die Zweckerreichung nicht erforderlich sind.	• Mandantenfähigkeit *(Durchgängigkeit, Dokumentation)* • Trennung von Produktiv-, Entwicklungs- und Testsystemen *(Netztrennung, Anonymisierung*)
Bei dem Auftragsverarbeiter realisierte Maßnahmen Es gibt eine durchgängige Mandantentrennung, die eine Vermischung von Daten verhindert. Die Trennung der technischen und personenbezogenen Daten des Auftraggebers wird durch den Auftraggeber selbst realisiert. Die logische Trennung von Produktiv-, Entwicklungs- und Testsystemen wird gemeinsam mit dem Auftraggeber erarbeitet.	

Wirksamkeitskontrolle

Anforderung und Ziel	Beispiele
Anforderung: Maßnahmen der Wirksamkeitskontrolle müssen gewährleisten, dass die Fähigkeit, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherstellt, regelmäßig überprüft, bewertet und evaluiert wird. Dazu gehört die Sicherstellung der Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen durch die Einführung von Überwachungsmaßnahmen die geeignet sind, Schutzverletzungen und deren Auswirkungen rechtzeitigt festzustellen und deren mögliche Auswirkungen zu bestimmen. **Ziel:** Durch regelmäßige Prüfungen und Neubewertungen der Risiken werden die Maßnahmen auf dem Stand der Technik gehalten und der Nachweis für eine fortlaufende Sicherstellung der Angemessenheit des Schutzniveaus erbracht. Die Meldepflicht an die Aufsichtsbehörde bei Verletzungen des Schutzes personenbezogener Daten muss umfassend und rechtzeitig (innerhalb von 72 Stunden) gewährleistet werden.	• regelmäßige interne Audits *(Dokumentation)* • regelmäßige externe Audits • Notfallübungen • Datenschutzfolgenabschätzungen • SDM, ISMS o.ä. „Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
Bei dem Auftragsverarbeiter realisierte Maßnahmen: Regelmäßige externe Audits im Rahmen des Datenschutzes. Installation von Sicherheitskritischen Updates und Hotfixes nach CERT Prozess. Prüfung der Systeme im Rahmen von Wartungsfenstern.	

Freie-Vogel-Str. 369
D-44269 Dortmund
+49 231 4773 27-60
+49 231 4773 27-66
Dortmund@cema.de
www.cema.de

CEMA GmbH Spezialisten für
Informationstechnologie
Dortmund

Abschlusserklärung

Der Auftragsverarbeiter erklärt, die weiteren Auftragsverarbeiter sorgfältig ausgewählt, in erforderlicher Weise vertraglich gebunden zu haben und entsprechend zu überwachen.

Die Angaben dieser Anlage basieren auf der Auskunft des Auftragsverarbeiters. Der Auftragsverarbeiter bestätigt die Richtigkeit der oben gemachten Angaben und hat zur Kenntnis genommen, dass er Änderungen unverzüglich mitteilen und nachdokumentieren muss.

_____ _____

Ort, Datum Unterschrift