Crewmeister

AVV - Anhang II

- Technische und organisatorische Maßnahmen -

Alle Geschäftsstellen sowie alle Konzerngesellschaften der CREWMEISTER Software AG nutzen die gesamte IT-Infrastruktur des Unternehmenssitzes in München. Sämtliche Tätigkeiten - auch via remote - werden ausschließlich mit IT-Ressourcen und Betriebsmitteln durchführt, die von der CREWMEISTER Software AG gestellt und zentral kontrolliert werden. Das interne Rechenzentrum befindet sich in München.

Im Folgenden sind die technischen und organisatorischen Maßnahmen von CREWMEISTER in Bezug auf die internen IT-Systeme und internen Geschäftsprozesse der Geschäftsstellen und der Konzerngesellschaften der CREWMEISTER Software AG aufgeführt. Abhängig vom jeweiligen CREWMEISTER Standort sind (geringfügige) Abweichungen möglich.

I. VERTRAULICHKEIT

1. Physische Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Bürogebäuden, Arbeitsplätzen und internen Datenverarbeitungsanlagen zu verwehren.

I.1.1	**Bürogebäude und Arbeitsplätze**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Einbruchmeldeanlage (EMA) ☒ Elektronisches Schließsystem ☒ Zutrittstechniken (z.B. RFID, PIN oder mechanische Schlüssel) mit personenspezifischer Vergabe ☒ Mechanisches Schließsystem für das Gebäude / die Büroräume ☒ Chipkarten ☒ Klingelanlage mit Kamera ☒ Videoüberwachung der Eingangsbereiche ☒ Bewegungsmelder, Überfallmelder ☒ Wachdienst	☒ Standortverantwortliche ☒ Ausgabe von Schlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Sicherheitszonen ☒ Empfangs-/Besucherbereiche ☒ Beschränkung des Zutritts für betriebsfremde Personen (z. B. Besucherinnen und Besucher*)* ☒ Besucher-Management-Prozess, inkl. (De-) Registrierung, Besucherausweise, Begleitung durch Mitarbeitende ☒ Sorgfalt bei Auswahl des Wachdienstes
I.1.2	**Internes Rechenzentrum**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Betrieb des internen Rechenzentrums durch CREWMEISTER IT-Abteilung ☒ Einbruchmeldeanlage (EMA) ☒ Elektronisches Schließsystem ☒ Zutrittstechnik (z.B. RFID und mechanische Schlüssel) mit personenspezifischer Vergabe ☒ Videoüberwachung	☒ Begrenzung der Schlüsselausgabe und Einschränkung der Zutrittsrechte für den Zugang zum Rechenzentrum auf privilegiertes Personal der CREWMEISTER IT-Abteilung ☒ Ausgabe von Schlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Besucher-Management-Prozess, inkl. (De-) Registrierung, Besucherausweise, Begleitung durch Mitarbeitende

2. Digitale Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass interne Datenverarbeitungsanlagen und Informationen von Unbefugten genutzt werden können.

I.2	**Interne Systeme, Applikationen, Notebooks, Smartphones**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Anbindung der Geschäftsstellen und Konzerngesellschaften per verschlüsseltem Server-Netzwerk (Domänen-Controller) ☒ Nutzung nur von CREWMEISTER intern freigegebenem IT-Equipment und Applikationen, Systemen ☒ Verbot von BYOD ☒ BIOS-gestützte Festplatten-Authentifizierung von mobilen Endgeräten (z.B. Notebooks, Tablets) ☒ Gehäuseverriegelung ☒ Login mit personalisierten Benutzer-Accounts + Passwort ☒ Login mit privilegierten Accounts + Passwort + 2. Faktor ☒ Protokollierung der An- und Abmeldungen, Anmeldeversuche ☒ Automatische passwortgeschützte Desktop- / Bildschirmsperre ☒ Verbot mit Ausnahmevorbehalt für Nutzung von hardwareverschlüsselten Wechselmedien (z.B. USB-Sticks mit 256-bit-AES) ☒ Einsatz VPN-Anbindung bei Fernzugriffen ☒ Mobil Device Management ☒ Verschlüsselung von Festplatten (256-bit AES) ☒ Viren-, Spyware-, Malwareschutz ☒ SIEM ☒ Firewalls ☒ Spamfilter ☒ Proxy (inkl. Virenschutz) ☒ Intrusion Prevention System (IPS) ☒ Passwort-Server ☒ Verschlüsselung des Datentransfers (z.B. BIOS-Passwörter, VPN-Anbindungen, Ironkeys inkl. Virenscanner) ☒ Applikationen werden auf die technische Möglichkeit geprüft, Schnittstellen zu verhindern oder zu schließen	☒ Benutzer- und Berechtigungsmanagement ☒ Passwortmanagement ☒ Begrenzung von Anmeldeversuchen und automatischer Zugangssperrung ☒ Richtlinie zum Umgang mit Passwörtern und Zugangsschutz ☒ Vorgaben zum manuellem Sperren ☒ Passworthistorie ☒ Richtlinie zum Umgang mit Unternehmenswerten, inkl. Löschung/Vernichtung ☒ Richtlinie zum Datenschutz und Informationssicherheit in der Organisation ☒ Richtlinie Smartphones ☒ Richtlinie Social Media ☒ Kontrolle und Aufbewahrung der Protokolle ☒ Sicherheitsupdates ☒ Pentetrationstests (jährlich) ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung von internen Datenverarbeitungssystemen Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Informationen zugreifen können, und dass Informationen bei der Verarbeitung, Nutzung und nach der Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können.

I.3	**Informationen (unabhängig, ob in elektronischer oder physischer Form)**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Zugriffsberechtigungen werden durch ein zentrales Microsoft Active Directory bzw. eine firmeneigene Domäne definiert, koordiniert und kontrolliert. ☒ Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderung und Löschung von Zugriffsberechtigungen) ☒ Datenschutztresor ☒ Mitarbeiterschließfächer ☒ Vernichtung von elektronischen Datenträgern durch einen externen Entsorgungsdienstleister (Standard DIN 66399-3) ☒ Entsorgung von klassifizierten Dokumenten in verschlossenen Datentonnen ☒ Aktenvernichtung und Leerung durch externen Entsorgungsdienstleister	☒ Rollenbasiertes Berechtigungskonzept ☒ Benutzer- und Berechtigungsmanagement (inkl. Vorgaben bei Eintritt, Funktionswechsel, Ausscheiden) ☒ Beschränkte Anzahl von Administratoren / von privilegierten Benutzer-Accounts ☒ Richtlinie zum Umgang mit Unternehmenswerten, inkl. Löschung/Vernichtung ☒ Richtlinie Clean Desk ☒ Ausgabe von Schließfächerschlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Kontrolle und Aufbewahrung der Protokolle ☒ Sorgfalt bei Auswahl des Entsorgungsdienstleisters ☒ Gesonderte Zugangspunkte für externe IT-Systeme

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten logisch oder physikalisch getrennt verarbeitet werden.

I.4	**Systemkontrolle / Speicherkontrolle**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Trennung von personenbezogenen Daten des KUNDEN im Sinne einer Auftragsdatenverarbeitung und von sonstigen internen Geschäftsinformationen ☒ Trennung von Produktiv- und Testumgebungen ☒ Mandantenfähigkeit relevanter Applikationen ☒ Test von Software / Hardware erfolgt in isolierten virtuellen Umgebungen (Sandboxing)	☒ Übermittlungsverbot von personenbezogenen Daten des KUNDEN im Sinne einer Auftragsdatenverarbeitung außerhalb festgelegter Übermittlungs- und Kommunikationswege an CREWMEISTER ☒ Festlegung von internen Datenbankrechten ☒ Interne Domänenverwaltung ☒ Interne Netzwerk--Topologiepläne ☒ Change Management

II. INTEGRITÄT

1. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Informationen in interne Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

II.1	**Protokollierungen / Logging (z.B. Betriebssysteme, Netzwerke, Firewalls, Datenbanken, Applikationen)**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Technische Protokollierung von An- und Abmeldungen von Benutzern auf CREWMEISTER internen Datenverarbeitungssystemen ☒ Zentrale Speicherung der Protokolldaten in Bezug auf CREWMEISTER interne Datenverarbeitungssysteme ☒ Uhrensynchronisation/Timeserver	☒ Rollenbasierte Eingabe-, Änderungs- und Löschbeschränkungen werden über das Benutzer- und Berechtigungsmanagement gesteuert und kontrolliert ☒ Aufbewahrung von Protokollen nach den gesetzlichen Vorgaben ☒ Manuelle oder automatisierte Kontrolle der Protokolle

2. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

II.2	**Elektronische und physische Datenübertragungen**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ E-Mail-Verschlüsselung (S/MIME, TLS, Zertifikate) ☒ Contentfilter für E-Mail und Web ☒ Telefonie-Verschlüsselung (SAML, TLS, Zertifikate) ☒ Einsatz von VPN auf mobilen Endgeräten ☒ Verbot mit Sondererlaubnisvorbehalt für Nutzung von hardwareverschlüsselten Wechselmedien (z.B. USB-Sticks mit 256-bit AES) ☒ Verschlossene Briefkästen ☒ Nutzung von festgelegten Kommunikations- und Übermittlungswegen	☒ Richtlinie zur Informationsübertragungen von und nach extern ☒ Entnahme von Briefpost ausschließlich durch unternehmenseigenes Empfangspersonal ☒ Persönliche Verteilung bei externer Briefpost ☒ Persönliche Verteilung bei interner, (sehr) vertraulich gekennzeichneter Briefpost / Dokumenten ☒ Warenlieferungen nur innerhalb Anlieferungszonen mit persönlicher Entgegenahme ☒ Definierte Vorgaben bei Fernzugriffen (siehe ergänzende Informationen unten*) ☒ Verhinderung / Löschung von Übermittlungen von nicht-anonymisierten personenbezogenen Daten des KUNDEN außerhalb abgestimmter und festgelegter Übertragungswege (siehe ergänzende Informationen*)

***Ergänzende Informationen:**

Die Übermittlung von nicht-anonymisierten personenbezogenen Daten des KUNDEN darf nur durch den KUNDEN selbst, entweder über die eingerichteten Übertragungswege in den CREWMEISTER Cloud Services oder auf den kundeneigenen IT-Systemen erfolgen. Eine Übersendung nicht-anonymisierten personenbezogenen Daten des KUNDEN über E-Mailverkehr an Empfänger bei CREWMEISTER ist zu unterlassen.

Für die Erbringung von Parametrisierung-, Softwarepflege- und Hotline-Leistungen mit Zugriffen auf die lizenzierte Kundeninstallation muss der KUNDE die Zugriffs- und Weitergabekontrolle durch entsprechende Konfigurationen im User Management sicherstellen:

- Die (De-) Registrierung von Nutzern (einschließlich von CREWMEISTER Hotline- und Customer Service Beratern) kann nur vom KUNDEN vorgenommen und nach eigens von ihm festgelegten Prüfzyklen zu überwacht werden.
- Parametrisierung-, Softwarepflege- und Hotline-Leistungen mit Zugriffen auf die lizenzierte Kundeninstallation auf den IT-Systemen des KUNDEN vor Ort oder per Fernzugriff bedürfen einer vorherigen Nutzerberechtigung bzw. Freischaltung durch den KUNDEN.
- Parametrisierung-, Softwarepflege- und Hotline-Leistungen per Fernzugriff erfolgen ausschließlich über gesicherte Verbindungen und unter Berücksichtigung der in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.
- Soweit erforderlich, wirken CREWMEISTER Hotline- und Customer Service Berater auf Weisungen des KUNDEN an der Konfiguration technischer Kontrolleinrichtungen mit. Sofern dabei Fernzugriffe auf den kundeneigenen IT-Systemen erfolgen sollen, stellt der KUNDE eine geeignete Softwarelösung zum Fernzugriff (z.B. VPN, Desktop Sharing), die auf aktuellen Windows Server Betriebssystemen lauffähig ist (inkl. notwendiger Lizenz), bereit. Fernzugriffe werden dabei kontrolliert und betreut durch die CREWMEISTER Remote Access Services (RAS) Abteilung.
- Der KUNDE ist befähigt, Fernzugriffe mitzuverfolgen und jederzeit abzubrechen.
- Personenbezogene Daten des KUNDEN dürfen nur auf ausdrückliche Weisung des KUNDEN auf Wechseldatenträgern von CREWMEISTER gespeichert werden. Entsprechende Kopien werden nach Abschluss des konkreten Zugriffs durch CREWMEISTER gelöscht.

III. VERFÜGBARKEIT

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

I.1.1	**Bürogebäude und Arbeitsplätze, Hardware, IT-Ressourcen**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Brandschutzvorkehrungen (z.B. Feuer- und Rauchmeldeanlagen) ☒ Feuertüren und Fluchtwege ☒ Notstromversorgung ☒ Zertifizierte und abgenommene Elektroinstallationen (inklusive Überspannungsschutz und bereichsorientierte Energieverteilung) ☒ Synchronisierte USV-Anlage ☒ Telekommunikations- und Provideranbindungen über mindestens zwei Glasfaseranbindungen und separater Übertragungstechnik ☒ Redundante Anbindung aller wichtigen	☒ Elektrochecks aller elektronischen Geräte gemäß Prüfzyklus vom Hersteller ☒ Regelmäßige Funktionsprüfungen ☒ Durchführung von Wartungen und Pflege durch Dienstleister ☒ Sorgfalt bei Auswahl von Dienstleistern ☒ Dokumentation der Switch-Ports ☒ Sicherheitsupdates ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management

	Komponenten ☒ Elektrorevision (VDS) ☒ Strukturierte Verkabelung ☒ Separater "Netzwerkschrank" für Anbindung und Netzwerk ☒ Computergesteuertes Überwachungssystem der Verbindungen	
I.1.2	**Internes Rechenzentrum**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Brandschutzvorkehrungen (u.a. durch eigenen Brandschutzabschnitt, Anbindung an Brandmeldezentrale, Rauchmelder) ☒ Feuchtigkeitssensoren ☒ Rauchansaugsystem (RAS) ☒ Redundante Klimatisierung ☒ Netzersatzanlage (NEA, Dieselgenerator) ☒ Redundante unterbrechungsfreie Stromversorgung ☒ Getrennte Stromkreise ☒ Telekommunikations- und Provideranbindungen über mindestens zwei Glasfaseranbindungen und separater Übertragungstechnik. ☒ Redundante Anbindung aller wichtigen Komponenten ☒ Elektrorevision (VDS) ☒ Strukturierte LAN-Verkabelung ☒ Separater "Netzwerkschrank" für Anbindung und Netzwerk ☒ Computergesteuertes Überwachungssystem der Verbindungen ☒ Redundante interne Speichersysteme ☒ Sicherungsbänder, Aufbewahrung der Backups in redundantem Speichersystem im Rechenzentrum ☒ Sicherungsdienst an einem anderen Ort	☒ Backup und Desaster Recovery Konzept ☒ Geographische Trennung der Backupspeicherorte vom Ort des primären Servers ☒ Datensicherungen erfolgen mehrfach täglich (für relevante interne IT-Systeme) ☒ Backups sind verschlüsselt ☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse ☒ Backups werden über Echtzeitspiegelung erstellt ☒ Transport der Sicherungsbänder durch Sicherheitsdienst ☒ Sorgfalt bei Auswahl des Sicherungsdienstes ☒ Sicherheitsupdates ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management

IV. VERSCHLÜSSELUNG UND PSEUDONYMISIERUNG

☒ Die elektronische Übermittlung von Emailverkehr erfolgt verschlüsselt.
☒ Die elektronische Übermittlung von personenbezogenen Daten darf nur auf verschlüsselten und festgelegten Übermittlungs- und Kommunikationswegen erfolgen. Eine Übermittlung von nicht-anonymisierten, personenbezogenen KUNDENDATEN (z. B. Test- daten, Mitarbeiterstammdaten etc.) auf vorab nicht gemeinsam festgelegten Übermittlungs- und Kommunikationswegen ist nicht zulässig.
☒ Die Speicherung von personenbezogenen Daten erfolgt auf IT-Systemen des Kunden oder in den CREWMEISTER Cloud Services.
☒ Die Speicherung von personenbezogenen Daten im CREWMEISTER internen Geschäftsbetrieb erfolgt verschlüsselt.
☒ Alle Daten auf mobilen Rechner und Speichermedien werden verschlüsselt.
☒ Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem *Stand der Technik**
☒ Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert.
☒ Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert.
☒ Ein Regelwerk mit Anforderungen an Verschlüsselungsstärke, -algorithmus und Verwaltung der Schlüssel ist implementiert.
☒ Pseudonymisierung personenbezogener Daten durch Einwegfunktionen.
☒ Pseudonymisierung durch Zuordnungstabellen, diese sind von der übrigen Datenverarbeitung getrennt.

**Definition* - Stand der Technik umfasst die bis zum jeweiligen Zeitpunkt gewonnenen technischen Erkenntnisse, die Eingang in die betriebliche Praxis gefunden haben und allgemein anerkannt sind.

V. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

1. Datenschutz-Management

IV.1	**Einhaltung und Überprüfung der Maßnahmen**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen wird mind. jährlich durchgeführt (externes DSGVO-Audit) ☒ Toolgestützte Kontrolle von regelmäßigen Mitarbeiterschulungen und Teilnahmen	☒ Interne Datenschutzbeauftragte (Kontaktdaten sind auf der **CREWMEISTER Website** bekanntgegeben) ☒ Mitarbeiterschulungskonzept ☒ Regelmäßige Sensibilisierung der Mitarbeitenden (mindestens jährlich) ☒ Einhaltung der Informationspflichten nach Art. 13 und Art. 14 DSGVO ☒ Formalisierter Prozess zur Bearbeitung von Datenschutzanfragen und Meldungen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden) ☒ Datenschutz-Folgenabschätzungen (DSFA) werden bei Bedarf durchgeführt. ☒ Einbindung der Datenschutzbeauftragten in internen und externen Datenschutzangelegenheiten

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des KUNDEN verarbeitet werden können.

IV.3	**Genehmigte Unterauftragsverarbeiter**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Zertifizierte, dokumentierte Sicherheitsmaßnahmen von (Hosting) Service Providern	☒ Sorgfalt bei Auswahl von CREWMEISTER Unterauftragsverarbeitern ☒ Vorlage und Prüfung von Nachweisen über Kontrollmaßnahmen und DSGVO-Konformität von (Hosting) Service Providern (z.B. Prüfreporte, Zertifikate) ☒ Abschluss einer Auftragsverarbeitungsvereinbarung ☒ Dokumentation von Weisungen ☒ Verpflichtung von CREWMEISTER Unterauftragsverarbeitern auf Vertraulichkeit und das Datengeheimnis ☒ Abschluss von EU Standard-Vertragsklauseln oder anderen Garantien nach Art. 46 DSGVO (sofern erforderlich) ☒ Fortlaufende Überprüfungen von Unterauftragsverarbeitern in Bezug auf Datenschutz und Informationssicherheit ☒ Verpflichtung von Unterauftragsverarbeitern im Falle von Drittlandstransfers, dass ein Transfer Impact Assessment bzgl. der weiteren Unter-Unterauftragnehmer durchgeführt wurde und, dass das Ergebnis dieser Bewertung positiv / DSGVO-konform ist.

***