Crewmeister

DPA - Exhibit II

- Technical and organisational measures -

All offices and all group companies of CREWMEISTER Software AG use the entire IT infrastructure of the company headquarters in Munich. All activities - including remote activities - are carried out exclusively with IT resources and equipment provided and centrally controlled by CREWMEISTER Software AG. The internal data center is located in Munich.

The technical and organizational measures taken by CREWMEISTER with regard to the internal IT systems and internal business processes of the offices and group companies of CREWMEISTER Software AG are listed below. Depending on the respective CREWMEISTER location, (minor) deviations are possible.

I. CONFIDENTIALITY

1. Physical access control

Measures suitable for preventing unauthorized persons from access to office buildings, workplaces, and internal data processing systems.

I.1.1	**Office building and workplaces**	
	Technical measures	**Organizational measures**
	☒Intrusion alarm system (IAS) ☒ Electronic locking system ☒ Access technologies (e.g. RFID, PIN, or mechanical keys) with person-specific allocation ☒ Mechanical locking system for the building / offices ☒ Smart cards ☒ Bell system with camera ☒ Video surveillance of the entrance areas ☒ Motion detector, attack reporter ☒ Guard duty	☒ Site office managers ☒ Issuance of keys is protocolled by means of issuance and return protocols ☒ Security zones ☒ Reception/visitor areas ☒ Restriction of access for persons not belonging to the company (e.g. visitors*)* ☒ Visitor management process, incl. registration, deregistration, visitor passes, and accompaniment by staff ☒ Due care in the selection of the guard service
I.1.2	**Internal data center**	
	Technical measures	**Organizational measures**
	☒ Operation of the internal data center by the CREWMEISTER IT department ☒ Intrusion alarm system (IAS) ☒ Electronic locking system ☒ Access technology (e.g. RFID and mechanical keys) with person-specific allocation ☒ Video surveillance	☒ Limitation of key issuance and restriction of access rights to the data center to privileged personnel of the CREWMEISTER IT department ☒ Issuance of keys is protocolled by means of issuance and return protocols ☒ Visitor management process, incl. registration, deregistration, visitor passes, and accompaniment by staff

2. Digital access control

Measures suitable to prevent internal data processing systems and information from being used by unauthorized persons.

I.2	Internal systems, applications, notebooks, smartphones	
	Technical measures	**Organizational measures**
	☒ Connection of the offices and group companies via an encrypted server network (domain controller) ☒ Exclusive use of IT equipment, applications, and systems that have been approved internally by CREWMEISTER ☒ Ban on BYOD ☒ BIOS-supported hard disk authentication of mobile end devices (e.g. notebooks, tablets) ☒ Housing lock ☒ Login with personalized user accounts + password ☒ Login with privileged accounts + password + 2nd factor ☒ Logging of logins and logouts, login attempts ☒ Automatic password-protected desktop / screen lock ☒ Prohibition with exception for use of hardware-encrypted removable media (e.g. USB sticks with 256-bit AES) ☒ Use of VPN connection for remote access ☒ Mobile device management ☒ Hard disk encryption (256-bit AES) ☒ Virus, spyware, malware protection ☒ SIEM ☒ Firewalls ☒ Spam filter ☒ Proxy (incl. virus protection) ☒ Intrusion prevention system (IPS) ☒ Password server ☒ Encryption of data transfer (e.g. BIOS passwords, VPN connections, Ironkeys incl. virus scanner) ☒ Applications are checked for the technical possibility to prevent or close interfaces	☒ User and authorization management ☒ Password management ☒ Limitation of login attempts and automatic access blocking ☒ Policy for handling passwords and access protection ☒ Specifications for manual locking ☒ Password history ☒ Policy on handling company assets, incl. erasure / destruction ☒ Policy on data protection and information security in the organization ☒ Smart phone policy ☒ Social media policy ☒ Control and storage of the logs ☒ Security updates ☒ Penetration tests (annually) ☒ Incident management ☒ Change management ☒ IT emergency management

3. Access control

Measures to ensure that those authorized to use internal data processing systems can only access the information subject to their access authorization and that information cannot be read, copied, modified, or removed by unauthorized persons during processing, use and after storage.

I.3	Information (irrespective, whether in electronic or physical form)	
	Technical measures	**Organizational measures**
	☒ Access authorizations are defined, coordinated, and controlled by a central Microsoft Active Directory or a company's own domain. ☒ Logging of access to applications (entry, modification, and erasure of access authorizations) ☒ Data protection safe ☒ Staff lockers ☒ Destruction of electronic data carriers by an external disposal service provider (standard DIN 66399-3) ☒ Disposal of classified documents in sealed data bins ☒ Document destruction and emptying by an external disposal service provider	☒ Role-based authorization concept ☒ User and authorization management (incl. specifications for entry, change of function, departure) ☒ Limited number of administrators / privileged user accounts ☒ Policy on handling company assets, incl. erasure / destruction ☒ Clean desk policy ☒ Issuance of staff locker keys is protocolled by means of issuance and return protocols ☒ Control and storage of the logs ☒ Due care in the selection of the disposal service provider ☒ Separate access points for external IT systems

4. Separation control

Measures to ensure that data collected for different purposes are processed separately either logically or physically.

I.4	System control / storage control	
	Technical measures	**Organizational measures**
	☒ Separation of personal data of the CUSTOMER in terms of commissioned data processing and other internal business information ☒ Separation of productive and test environments ☒ Multi-tenant capability of relevant applications ☒ Testing of software / hardware takes place in isolated virtual environments (sandboxing)	☒ Prohibition of transmitting personal data of the CUSTOMER in the sense of commissioned data processing outside defined transmission and communication channels to CREWMEISTER ☒ Definition of internal database rights ☒ Internal domain management ☒ Internal network topology plans ☒ Change management

II. INTEGRITY

1. Input control

Measures to ensure it is possible to check and retrospectively determine whether information has been entered into internal data processing systems, modified while in those systems, or removed from them, and by whom.

II.1	Logging (e.g., operating systems, networks, firewalls, databases, applications)	
	Technical measures	**Organizational measures**
	☒ Technical logging of user logins and logouts on CREWMEISTER internal data processing systems ☒ Central storage of log data in relation to CREWMEISTER internal data processing systems ☒ Clock synchronization / timeserver	☒ Role-based input, modification and erasure restrictions are managed and controlled via user and authorization management ☒ Retention of logs in accordance with legal requirements ☒ Manual or automated control of logs

2. Transfer control

Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or during their transport or storage on data media, and that it is possible to verify and establish the bodies to which personal data are intended to be transmitted by data transmission equipment.

II.2	Electronic and physical data transfers	
	Technical measures	**Organizational measures**
	☒ E-mail encryption (S/MIME, TLS, certificates) ☒ Content filter for e-mail and web ☒ Telephony encryption (SAML, TLS, certificates) ☒ Use of VPN on mobile devices ☒ Ban on using hardware-encrypted removable media (e.g., USB sticks with 256-bit AES) without special permission ☒ Locked letterboxes ☒ Use of predefined communication and transmission channels	☒ Policy for dealing with external files ☒ Collection of letter post exclusively by the company's in-house reception staff ☒ Personal distribution for external letter post ☒ Personal distribution for internal, (very) confidentially marked letter mail / documents ☒ Deliveries of goods only within delivery zones with personal acceptance ☒ Defined specifications for remote access (see supplementary information below*) ☒ Prevention / erasure of transmissions of non-anonymized personal data of the CUSTOMER outside of agreed and specified transmission paths (see supplementary information*).

***Supplementary information:**

The transmission of non-anonymized personal data of the CUSTOMER may only be carried out by the CUSTOMER itself, either via the established transmission paths in the CREWMEISTER Cloud Services or on the CUSTOMER's own IT systems. The sending of non-anonymized personal data of the CUSTOMER via e-mail traffic to recipients at CREWMEISTER is to be refrained from.

For the provision of parameterization, software maintenance and hotline services with access to the licensed customer installation, the CUSTOMER must ensure access and transfer control through appropriate configurations in user management:

- The registration or deregistration of users (including CREWMEISTER hotline and customer service consultants) can only be carried out by the CUSTOMER and monitored in accordance with test cycles specified by the CUSTOMER.
- Parameterization, software maintenance and hotline services with access to the licensed customer installation on the CUSTOMER's IT systems on site or by remote access require prior user authorization or activation by the CUSTOMER.
- Parameterization, software maintenance and hotline services via remote access shall be provided exclusively via secure connections and in compliance with the technical and organizational measures for the protection of personal data described in this Exhibit.
- To the extent necessary, CREWMEISTER hotline and customer service consultants shall cooperate in the configuration of technical control devices on the instructions of the CUSTOMER. If remote access is to be made to the CUSTOMER's own IT systems, the CUSTOMER shall provide a suitable software solution for remote access (e.g. VPN, desktop sharing) that is executable on current Windows server operating systems (including the necessary license). Remote access is controlled and managed by the CREWMEISTER Remote Access Services (RAS) department.
- The CUSTOMER is authorized to monitor remote accesses and to stop them at any time.
- Personal data of the CUSTOMER may be stored on removable data storage devices of CREWMEISTER only on the explicit instruction of the CUSTOMER. Corresponding copies are deleted by CREWMEISTER after completion of the specific access.

III. AVAILABILITY

Measures to ensure that personal data are protected against accidental destruction or loss.

I.1.1	**Office building and workplaces, hardware, IT resources**	
	Technical measures	**Organizational measures**
	☒ Fire protection precautions (e.g., fire and smoke detection systems) ☒ Fire doors and escape routes ☒ Emergency power supply ☒ Certified and approved electrical installations (including surge protection and area-oriented power distribution) ☒ Synchronized UPS system ☒ Telecommunication and provider connections via at least two fiber optic connections and separate transmission technology ☒ Redundant connection of all important components ☒ Electrical revision (VDS)	☒ Electrical checks of all electronic devices according to the test cycle from the manufacturer ☒ Regular functional tests ☒ Performance of maintenance and due care by service providers ☒ Due care in the selection of service providers ☒ Documentation of the switch ports ☒ Security updates ☒ Incident management ☒ Change management ☒ IT emergency management

	☒ Structured wiring ☒ Separate "network cabinet" for connection and network ☒ Computer-controlled monitoring system of the connections	
I.1.2	**Internal data center**	
	Technical measures	**Organizational measures**
	☒ Fire protection precautions (e.g., through a proprietary fire protection section, connection to fire alarm center, smoke detectors) ☒ Humidity sensors ☒ Smoke aspiration system (RAS) ☒ Redundant air conditioning ☒ Emergency power system (NEA, diesel generator) ☒ Redundant uninterruptible power supply ☒ Separate circuits ☒ Telecommunication and provider connections via at least two fiber optic connections and separate transmission technology. ☒ Redundant connection of all important components ☒ Electrical revision (VDS) ☒ Structured LAN cabling ☒ Separate "network cabinet" for connection and network ☒ Computer-controlled monitoring system of the connections ☒ Redundant internal storage systems ☒ Backup tapes, retention of backups in redundant storage system in the data center ☒ Security service at another location	☒ Backup and disaster recovery plan ☒ Geographical separation of the backup storage locations from the location of the primary server ☒ Data backups are carried out several times a day (for relevant internal IT systems) ☒ Backups are encrypted ☒ Regular data recovery tests and logging of results ☒ Backups are created via real-time mirroring ☒ Transport of the security tapes by security service ☒ Due care in the selection of the security service ☒ Security updates ☒ Incident management ☒ Change management ☒ IT emergency management

IV. ENCRYPTION AND PSEUDONYMIZATION

☒ The electronic transmission of e-mail traffic is encrypted.

☒ The electronic transmission of personal data may only take place via encrypted and defined transmission and communication channels. The transmission of non-anonymized, personal CUSTOMER DATA (e.g., test data, employee master data, etc.) via transmission and communication channels that have not been jointly defined in advance is not permitted.

☒ Personal data shall be stored on IT systems of the CUSTOMER or in the CREWMEISTER Cloud Services.

☒ The storage of personal data in the CREWMEISTER internal business operations shall be encrypted.

☒ All data on mobile computers and storage media are encrypted.

☒ All encryption technologies used productively are state of the art*.

☒ The management of the key material is defined and documented for the relevant IT systems.

☒ Transport encryption is implemented exclusively end-to-end.

☒ A set of rules with requirements for encryption strength, algorithm, and key management is implemented.

☒ Pseudonymization of personal data using one-way functions.

☒ Pseudonymization by assignment tables, these are separated from the rest of the data processing.

**Definition* - state of the art comprises the technical knowledge gained up to the respective point in time, which has found its way into operational practice and is generally recognized.

V. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT, AND EVALUATION

1. Data protection management

IV.1	**Compliance with and verification of the measures**	
	Technical measures	**Organizational measures**
	☒ A review of the effectiveness of the technical and organizational protection measures is carried out at least once a year (external GDPR audit). ☒ Tool-supported control of regular staff training and attendance	☒ Internal data protection officer (contact details are posted on the **CREWMEISTER website**) ☒ Staff training concept ☒ Regular sensitization of employees (at least annually) ☒ Compliance with the information obligations pursuant to Art. 13 and Art. 14 GDPR ☒ Formalized process for handling data protection requests and notifications (also with regard to the obligation to notify supervisory authorities) ☒ Data protection impact assessments (DPIAs) are carried out as required. ☒ Involvement of data protection officers in internal and external data protection matters

2. Processor control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the CUSTOMER's instructions.

IV.3	**Authorized sub processors**	
	Technical measures	**Organizational measures**
	☒ Certified, documented security measures of (hosting) service providers	☒ Due care in the selection of CREWMEISTER sub processors ☒ Submission and verification of evidence of control measures and GDPR compliance of (hosting) service providers (e.g. audit reports, certificates) ☒ Conclusion of a data processing agreement ☒ Documentation of instructions ☒ Obligation of CREWMEISTER sub processors to confidentiality and data secrecy ☒ Conclusion of EU standard contractual clauses or other guarantees under Art. 46 GDPR (if required) ☒ Regular audits of sub processors with regard to data protection and information security ☒ Obligation of sub processors that a transfer impact assessment has been carried out regarding the further sub processors in the event of third country transfers and that the result of this assessment is positive / GDPR-compliant.

***