Anlage 3 – Allgemeine technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO

Inhaltsverzeichnis

1 Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Maßnahmen:
☒ Verschlüsselung personenbezogener Daten und schutzwürdiger Daten bei erforderlichem Versand nach extern
☒ Verschlüsselung von mobilen Datenträgern (USB, externe Festplatte etc.)
☒ Verschlüsselung von mobilen Datensystemen (Laptop, etc.)

2 Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

Maßnahmen:
☒ Sicherheitsschlösser
☒ Türen mit Knauf Außenseite
☒ Videoüberwachung der Eingänge

☒ Schlüsselregelung / Liste
☒ Besucher nur in Begleitung durch Mitarbeiter

2.2 Zugangskontrolle
Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden:

Maßnahmen:
☒ Anti-Viren-Software Clients
☒ Firewall
☒ Anti-Viren-Software Server-Cloud
☒ Einsatz VPN bei Remote-Zugriffen
☒ Gehäuseverriegelung
☒ BIOS Schutz (separates Passwort)
☒ Sperre externer Schnittstellen (USB)
☒ Lösch-/Sperrkonzept
☒ Passwortrichtlinie (u. a. zentrale Passwortvergabe, keine Gruppenpasswörter)
☒ Erstellen und Verwalten von Benutzerprofilen
☒ Login mit Benutzername + Passwort
☒ Clean-Desk-Richtlinie (z. B. automatische Desktopsperre, Ausrichtung Bildschirme usw.)

2.3 Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen kopiert, verändert oder entfernt werden können:

Maßnahmen:
☒ Einsatz von Aktenvernichtern (Berücksichtigung der mindestens notwendigen Schutzklasse)
☒ Sichere Aufbewahrung von Datenträgern (z. B. Tresor)
☒ Physische Löschung von Datenträgern
☒ Festlegung und Kontrolle der Nutzung von Kommunikationskanälen (z. B. Messengerdienste)
☒ Einsatz Rechte-/Rollenkonzept
☒ Verwaltung Benutzerrechte durch Administratoren
☒ Auf das notwendige Maß reduzierte Anzahl von Administratoren
☒ Richtlinie Heimarbeits-/mobile Arbeitsplätze

2.4 Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Maßnahmen:
☒ Trennung von Produktiv- und Testsystem
☒ Netzinterne Abgrenzung bei erforderlichen Gastzugriffen

3 Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b) DSGVO)
3.1 Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Maßnahmen:
☒ Verschlüsselter Mailanhang bei relevanten Daten wie Dokumentationen
☒ Einsatz von VPN
☒ Protokollierung der Zugriffe und Abrufe
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https, tls

☒ Nutzung von Signaturverfahren

3.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind:

Maßnahmen:

☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Rechte- und Rollenkonzepts

4 Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b) DSGVO)

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

Maßnahmen:

☒ Feuerlöscher im Serverraum
☒ Geräte zur Überwachung von Temperatur im Serverraum
☒ Serverraum belüftet
☒ USV (redundante unterbrechungsfreie Stromversorgung)
☒ Schutzsteckdosenleisten Serverraum (Überspannungsschutz)
☒ RAID System / Festplattenspiegelung
☒ Zertifizierte Rechenzentren für externe Daten
alle Systeme sind speziell auf die jeweilige Aufgabe ausgewählt und konfiguriert
☒ Videoüberwachung Serverraum
☒ Backup & Recovery-Konzept
☒ Kontrolle des Sicherungsvorgangs
☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

5 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO)

Maßnahmen:

☒ Datensicherungskonzept
☒ Datenwiederherstellungskonzept
☒ tägliche Backups auf gespiegeltem Disksystem (Cloud)
☒ wöchentliche Backup-Disk-to-Disk (Raumtrennung)
☒ Sicherstellung einer schnellen Beschaffung von Hardware durch Einkauf/Partner
☒ regelmäßige Prüfung der Rücksicherung

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO)

6.1 Datenschutz-Management

Maßnahmen:

☒ Datenschutzrichtlinie
☒ Mitarbeiter auf Vertraulichkeit/Datengeheimnis verpflichtet

6.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Maßnahmen:

☒ Einsatz von Firewall und regelmäßige Aktualisierung
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung

☒ Einsatz von Virenscanner und regelmäßige Aktualisierung

6.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Privacy by design / Privacy by default

Maßnahmen:
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind (Datenminimierung Art. 5 Abs. 1 lit. c) DSGVO)

6.4 Auftragskontrolle (Art. 28 DSGVO)
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Maßnahmen:
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. 3S Design GmbH, Schwarzmoorstrasse 28, 26817 Rhauderfehn
GF: Jürgen Bartels, Paul Stratmann
Email: vertrieb@3sdesign.de

Teilleistung: Datensicherung / Cloud Speicher
. Acronis Germany GmbH, Landsberger Straße 110, 80339 München
Telefon: +49 89 613 72 84 — 0, E-Mail: info-de@acronis.com

Teilleistung: Registrierungsstelle für Domains und Hosting
. ALL-INKL.com – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf
Inhaber: René Münnich
Telefon: +49 35872 353-10 E-Mail: info@all-inkl.com

Teilleistung: Übertragung von Lizenzinformationen
. ALLNET GmbH Computersysteme, Maisstrasse 2, 82110 Germering
Geschäftsführer: Wolfang Marcus Bauer
Telefon: +49 89 894 222 – 22 E-Mail: info@allnet.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP / Installation von EDV-Anlagen
. B-ITSEC, St. Veit Str. 21, 96138 Burgebrach
Inhaber: Thomas Kraus
Telefon: +49 9546 595946-0 E-Mail: info@b-itsec.de

Teilleistung: Hosting von WLAN Access Points und Firewall Controller
. CS GmbH, Buchstr. 103, 73525 Schwäbisch Gmünd
Geschäftsführer: Miran Percic
Telefon: +49 71 71 79 80 10, E-Mail: info@csnetworks.de

Teilleistung: Übertragung von Kundeninformationen
. GRÜNZUBLAU, Handthal 28, 97516 Oberschwarzach / OT Handthal
Inhaber: Anja Baumann
Telefon: +49 9382 3100183 E-Mail: ab@gruenzublau.de

Teilleistung: Registrierungsstelle für Domains und Hosting
. Host Europe GmbH, Hansestrasse 111, 51149 Köln
Geschäftsführer: Dr. Claus Boyens, Tobias Mohr
Telefon: +49 2203 9934 1040 E-Mail: info@hosteurope.de

Teilleistung: Übertragung von Lizenzinformationen (Microsoft / Trend Micro)
. Ingram Micro Distribution GmbH, Heisenbergbogen 3, 85609 Dornbach bei München
Geschäftsführer: Alexander Maier (Vorsitzender), Harald Weis, Karel Everaet
Telefon: +49 89 42 08 – 0 E-Mail: webmaster@ingrammicro.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Klaus Raab Datentechnik eK, Friedhofsstrr. 36, 96103 Hallstadt
Inhaber: Klaus Raab
Email: klaus@private-email.de

Teilleistung: Übertragung von Lizenzinformationen Cloudbasierte Back-Office Lösung / Datenspeicher / FIBU-Daten
. Leaf Systems GmbH, Rheingoldplatz 1, 68119 Mannheim
Geschäftsführer: Patrick Marksteiner, Patrick Neulinger
Telefon: +49 621 586 782 69, E-Mail: office@leaf-systems.eu

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. logotel Software e.K., Holzgartenstraße 2, 91207 Lauf
Inhaber: Robert Oertel
Telefon: +49 9123 98 089 – 20, Email: r.oertel@logotel-software.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. MC Gastro GmbH & Co. KG, Unteruttlau 13a, 94542 Haarbach
Geschäftsführer: Walter Brandl
Telefon: +49 8535 9129622 E-Mail: info@mc-gastro.de

Teilleistung: Übertrag von Lizenz- & Kundeninformationen / Digitale Speisekarten
.meisterwork GmbH, Obere Fellacher Straße 17, A-9500 Villach
Geschäftsführer: Georg Kitz
Telefon: +43 660 38 30 196 E-Mail: info@bessa.app

Teilleistung: Übertragung von Lizenzinformationen / Speicherung personenbezogene Daten / Online Gutscheinverwaltung / Online Tischreservierung
. mes.mo GmbH, Herdeweg 16, 73035 Göppingen
Geschäftsführer: Jens Walburg
Telefon: +49 7153 55 89 836, E-Mail: support@gastroguide.de

Teilleistung: Übertragung von Lizenzinformationen Cloudbasierte Back-Office Lösung / Datenspeicher / FIBU-Daten
. MULTI DATA Wedemann Vertriebs GmbH, Schütte-Lanz-Str. 2, 26135 Oldenburg
Geschäftsführer: Thorsten Wedemann, David Wedemann
Telefon: +49 44 1 971 71 - 0, E-Mail: info@multidata-kassen.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Noris Kassensysteme GmbH, Zum Kraftwerk 1, 45527 Hattingen
Geschäftsführer: Heinrich Prygoda
Telefon: +49 23 24 68 01 - 610, E-Mail: mail@noris-kassensysteme.de

Teilleistung: Server Hosting
. Plustech GmbH, Luitpoldstraße 10, 96052 Bamberg
Geschäftsführer: Florian Panzer
Telefon: +49 951 29909716 E-Mail: info@plustech.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Primadruck Kassensysteme GmbH, Escherweg 12, 82140 Olching
Geschäftsführer: Andreas Richtberg, Stefan Löser
Telefon: +49 8142 6511 271 E-Mail: info@primadruck.de

Teilleistung: Übertragung von Lizenzinformationen / Cloudbasierte Back-Office Lösung / Datenspeicher / FIBU-Daten
. Quorion Business Solutions GmbH, Mercedesstraße 8, 72108 Rottenburg-Ergenzingen
Geschäftsführer: Mustafa Yüksel
Telefon: +49 74 57 6 99 98 62, E-Mail: qbs@quorion.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Quorion Data Systems GmbH, An der Klinge 6, 99095 Erfurt
Geschäftsführer: Frank Grüschow
Telefon: +49 362 04 542 0, E-Mail: info@quorion.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Sharp Business Systems Deutschland GmbH, Industriestraße 180, 50999 Köln
Geschäftsführer: Kai Scott, Jun Ashida, Seitaro Nomura
Telefon: +49 22 36 3 23 100 E-Mail: info@sharpbusiness.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. SGO EDV- & Systemberatung, Lichtenfelser Str. 32, 96149 Breitengüßbach
Inhaber: Stephan Obermeder e. K.
Telefon: +49 9544 94 05 33 E-Mail: info@sgo-edv.de

Teilleistung: Übertragung von Lizenzinformationen / Speicherung personenbezogene Daten
. techreach GmbH, Franz-Mayer-Straße 1, 93053 Regensburg
Geschäftsführer: Lea Frank, Tobias Gubo
Telefon: +49 941 46 29 77 31, E-Mail: info@anybill.de

Teilleistung: Übertragung von Lizenzinformationen
. Trend Micro Deutschland GmbH, Parkring 2, 85748 Garching
Inhaber: Frank Schwittay, Norma O'Callaghan
Email: salesinfo_de@trendmicro.com

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. TourOnline AG, Borsigstraße 26. 73249 Wernau
Aufsichtsrat: Günter Heidelberg (Vorsitzender)
Telefon: +49 7153 9250 0 E-Mail: info@dirs21.de

Teilleistung: Übertragung von Lizenzinformationen / Datenreparatur ERP
. Computersysteme Viertl, Salzburgerstraße 22a G6, A-6380 St. Johann in Tirol
Inhaber: Franz Viertel
Telefon: +43 5352 64545 E-Mail: team@viertl-edv.com

Teilleistung: Übertragung von Lizenzinformationen / Cloudbasierter Datenspeicher
. Zyxel Deutschland GmbH, Adenauerstr. 20/B3 | 52146 Würselen
Geschäftsführer: Jannik Haargaard
Telefon: +49 2405 6909-0 E-Mail: sales@zyxel.de