Gestaltungsbüro Kowarzik, Susanne Kowarzik, Im Hahnböhl 1, 64342 Seeheim-Jugenheim

Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche

Angaben zum Verantwortlichen	
Name bzw. Unternehmensbezeichnung inkl. Rechtsformzusatz	Einzelunternehmer
ggf. vertretungsberechtigte Person des Unternehmens (z.B. GmbH-Geschäftsführer):	Susanne Kowarzik
Anschrift:	Im Hahnböhl 1, 64342 Seeheim-Jugenheim
Telefonnr.:	Telefon 06257 91 88 191
E-Mail-Adresse:	susanne@gestaltungsbuero-kowarzik.de
Angaben zum Datenschutzbeauftragten (DSB):	
Vor- und Nachname:	Susanne Kowarzik
Anschrift:	Im Hahnböhl 1, 64342 Seeheim-Jugenheim
Telefonnr.:	Telefon 06257 91 88 191
E-Mail-Adresse:	susanne@gestaltungsbuero-kowarzik.de
interner oder externer DSB?	intern

- Verarbeitungstätigkeiten -

Datum der Anlegung: 23.05.2018	Datum der letzten Änderung: 23.05.2018
Beschreibung der Verarbeitungstätigkeit:	Finanzbuchhaltung
Zweck der Verarbeitungstätigkeit:	- Durchführung der Finanzbuchhaltung - Umsetzung der gesetzlichen Vorgaben (GoBD)
Kategorien betroffener Personen:	☐ Beschäftigte ☐ Kunden ☐ Interessenten ☐ Lieferanten ☐ Steuerberater ☐ Kreditoren ☐ Debitoren
Kategorien personenbezogener Daten:	☐ Name ☐ Adressdaten ☐ Kontaktdaten ☐ Bankverbindung ☐ Geburtsdatum ☐ Beschäftigtendaten ☐ Lieferantendaten ☐ Kundendaten ☐ Buchungsdaten ☐ Daten Mahnwesen ☐ Saldenlisten ☐ Bilanzen
Kategorien besonderer personenbezogener Daten:	☐ Keine
Kategorien von Empfängern der personenbezogenen Daten:	☐ intern: Buchhaltung, Geschäftsführung ☐ extern: Finanzbehörden, Mitarbeiter bezüglich: Sozialversicherungen Krankenversicherungen Zahlungsdienstleister (Hausbank)
Übermittlung der Daten an Dritte:	☐ findet nicht statt und ist auch nicht geplant
Fristen zur Löschung der versch. Datenkategorien:	☐ 10 Jahre gem. Steuerrecht

Beschreibung der technischen und organisatorischen Maßnahmen (TOM):	s. Anhang am Ende dieses Dokuments (ab S. 7)
Rechtsgrundlage für die Verarbeitungstätigkeit:	☐ Erteilung eines Auftrags ☐ Durchführung vorvertraglicher Maßnahmen (Angebotserstellung) ☐ Einwilligung in das Angebot als Auftrag (Zustimmungserklärung des Betroffenen) ☐ Einwilligung dokumentiert ☐ Erfüllung einer rechtlichen Verpflichtung (Aufbewahrungsfrist gem. Steuerrecht)
Rechtsgrundlage für die Verarbeitung von besonderen personenbezogenen Daten:	☐ Einwilligung (Zustimmungserklärung des Betroffenen) ☐ Einwilligung dokumentiert ☐ aufgrund Arbeitsrecht / Sozialrecht (Daten von Beschäftigten) ☐ vom Betroffenen offensichtlich öffentlich gemachte Daten (Daten von öffentlich zugänglichem Facebook-Profil und oder Instagram-Profil des Betroffenen) ☐ Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Durchführung eines Mahnverfahrens)
Dokumentation allg. Informationspflicht:	☐ Datenschutzhinweise bei Erstkontakt übermittelt, und zwar ☐ per E-Mail (PDF-Anhang) ☐ per Website-Link ☐ telefonisch ☐ persönlich ☐ Datenschutzhinweise bei Einholung der Einwilligung erteilt ☐ Beschäftigte erhalten Datenschutzhinweise zusammen mit Arbeitsvertag
Dokumentation Prozess Auskunftsanfragen:	Betroffene Personen erhalten auf Anfrage Auskunft über die im Unternehmen verarbeiteten personenbezogenen Daten sowie folgende Informationen: - Zwecke der Verarbeitung - Kategorien personenbezogener Daten - Empfänger oder Kategorien von Empfängern - geplante Speicherdauer (falls möglich) oder Kriterien für Festlegung der Speicherdauer der personenbezogenen Daten - Recht auf Berichtigung, Löschung, Widerspruch, Einschränkung der Verarbeitung und Beschwerde bei zuständiger Aufsichtsbehörde - Herkunft der Daten (soweit diese nicht direkt bei der betroffenen Person erhoben wurden,

	sondern als Empfehlung durch Dritte die Kontaktaufnahme erfolgt.)
Umsetzung Grundsatz Speicherbegrenzung:	Die Daten der betroffenen Personen werden nur so lange gespeichert, wie dies zur Erfüllung des Zwecks des jeweiligen Datenverarbeitungsvorgangs erforderlich ist und soweit der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen.
Auftragsverarbeiter (AV):	☐ es werden keine AV eingesetzt
Konkrete Maßnahmen zur Sicherheit dieser Verarbeitungstätigkeit:	☐ TOMs (s. Anhang) ☐ zusätzlich werden bei dieser Verarbeitungstätigkeit folgende Maßnahmen umgesetzt: - Kommunikation ausschließlich über zertifizierte und verschlüsselte E-Mails (GMX mit Mailvelope)
Dokumentation Prozess Datenpannen:	Der Prozess für die Reaktion auf etwaige Datenschutzverletzungen ist installiert und dokumentiert, insbesondere kennen alle beteiligten Personen im Unternehmen die gesetzlich vorgesehenen Reaktionsfristen. Es existiert eine Vorlage für ein entsprechendes Info-Schreiben an die Aufsichtsbehörde bzw. an die Betroffenen. In jedem Fall werden die Geschäftsführung und der System-Administrator so schnell wie möglich nach Erkennen der Datenschutzverletzung über diese informiert. Sodann werden alle wesentlichen Informationen über die Datenschutzverletzung gesammelt und analysiert. Anschließend werden die erforderlichen Informationen für eine evtl. Benachrichtigung der Aufsichtsbehörde bzw. der betroffenen Personen zusammengestellt. Besteht ein konkretes Risiko für Betroffene, dann wird die zuständige Aufsichtsbehörde unverzüglich, aber spätestens binnen 72 Std. informiert. Bei einem voraussichtlich hohen Risiko werden die von der Datenschutzverletzung betroffenen Personen unverzüglich darüber informiert.
Datenschutz-Folgenabschätzung (DSFA):	☐ keine DSFA erforderlich aus sonstigen Gründen: zu geringe Daten
Dokumentation Sensibilisierung / Unterrichtung der Beschäftigten:	Alle Beschäftigten erhalten zu Beginn ihrer Tätigkeit im Unternehmen zusammen mit ihrem

	Arbeitsvertrag ein Info-Blatt zum Datenschutz. Außerdem müssen sie eine Verpflichtungserklärung zur Vertraulichkeit unterzeichnen. Für alle Beschäftigten erfolgt eine Unterweisung bzgl. der Grundlagen des Datenschutzes durch eine entsprechende Arbeitsanweisung,. Es finden regelmäßig (mind. 2x jährlich) Meetings mit allen Beschäftigten statt, in denen u.a. auch Infos bzgl. des Datenschutzes erfolgen. Die Teilnahme der Beschäftigten an diesen Meetings wird durch ihre Unterschrift unter dem Meeting-Protokoll dokumentiert.

Anhang zum Verarbeitungsverzeichnis – TOM

1. Gewährleistung der Vertraulichkeit

Zutrittskontrolle:	- mechanische Fenstersicherungen - Absicherung von Gebäudeschächten - manuelles Schließsystem - Schließsystem mit Sicherheitsschlössern - Bewegungsmelder - Schlüsselregelung Beschäftigte - Verschließen der Türen bei Abwesenheit
Zugangskontrolle:	- Der stationäre PC ist passwortgesichert und befindet sich in einem separaten Büro, das von Laufkundschaft nicht betreten werden kann.
Zugriffskontrolle:	- Nutzer-Berechtigungskonzept - Verwaltung der Nutzerrechte durch Systemadministrator - Anzahl der Administratoren auf das Notwendigste reduziert - Verwenden einer Passwortrichtlinie - Protokollierung von Zugriffen auf Anwendungen - physische Löschung von Datenträgern vor Wiederverwendung - ordnungsgemäße Vernichtung von Datenträgern - Einsatz von Aktenvernichtern
Trennungsgebot:	- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
Auftragskontrolle: *(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)*	- sorgfältige Auswahl des Auftragnehmers (Überprüfung des Dienstleisters) - vorherige Prüfung und Dokumentation der beim Auftragnehmer existierenden TOMs - schriftliche Vereinbarung mit dem Auftragnehmer - Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit - Datenschutzbeauftragter beim Auftragnehmer - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags - vertraglich festgelegte Kontrollrechte gegenüber dem Auftragnehmer - regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten - vertraglich festgelegte Vertragsstrafen bei Verstößen

Pseudonymisierung:	- Nutzung von pseudonymisierten Daten bei Datenübermittlung an externe Dienstleister
Verschlüsselung:	- Datenträgerverschlüsselung unter Windows 10 mittels Bitlocker - Nutzung von hardwareseitig verschlüsselten USB-Festplatten

2. Gewährleistung der Integrität

Eingabekontrolle:	- Protokollierung der Eingabe, Änderung und Löschung von Daten im System - sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden - Nachvollziehbarkeit durch Berechtigungskonzept
Weitergabekontrolle:	- Nutzung von Standleitungen bzw. VPN-Tunneln - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form (wenn möglich) - verschlüsselte E-Mail-Übertragung (SSL/TLS) - Verschlüsselung E-Mail-Inhalte (Software-Zertifikat) - vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe - festgelegte Löschfristen - sichere Transportverpackungen

3. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle:	- Schutzsteckdosenleisten für EDV-Geräte - Feuer- bzw. Rauchmeldeanlagen - Feuerlöschgeräte an mehreren, entsprechend gekennzeichneten Stellen im Gebäude und regelmäßige Wartung durch eine zertifizierte Wartungsfirma - regelmäßige Datensicherung - Notfallkonzept - Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort

4. Gewährleistung der Belastbarkeit der Systeme

Belastbarkeit der IT-Systeme:	- Antiviren-Software - Hardware-Firewall - Software-Firewall

5. Wiederherstellung der Verfügbarkeit

Wiederherstellbarkeit von IT-Systemen:	- sorgfältig ausgewählter interner System-Administrator

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Informations-Sicherheits-Management-System (ISMS):	- regelmäßige Prüfung der TOM (mind. 2x jährlich) durch Geschäftsführer und System-Administrator