Bär IT-Service, An der Herbstwiese 10, 90556 Seukendorf

Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche (TOM)

- Vorblatt -

Angaben zum Verantwortlichen	
Name bzw. Unternehmensbezeichnung inkl. Rechtsformzusatz	Bär IT-Service
ggf. vertretungsberechtigte Person des Unternehmens (z.B. GmbH-Geschäftsführer):	Michael Bär An der Herbstwiese 10 90556 Seukendorf
Anschrift:	An der Herbstwiese 10 90556 Seukendorf
Telefonnr.:	0911-6213710
Faxnr.:	0911-6213709
E-Mail-Adresse:	info@baer-it.net
Webseite:	www.baer-it.net
Angaben zum Datenschutzbeauftragten (DSB):	Nicht notwendig
Vor- und Nachname:	-
Anschrift:	-
Telefonnr.:	-
E-Mail-Adresse:	-
interner oder externer DSB?	☐ intern ☐ extern ☒ nicht notwendig

- Verarbeitungstätigkeiten -

Datum der Anlegung:	01.05.2018
Datum der letzten Änderung:	01.05.2018
Beschreibung der Verarbeitungstätigkeit:	Erstellung einer IT-Dokumentation (kundenseitig und intern)
Zweck der Verarbeitungstätigkeit:	Kundenseitige IT-Dokumentation: Dokumentation des aktuellen Ist-Zustandes bzgl. IT-Konfiguration, Zugangskennungen, Passwörter, Besonderheiten beim Kunden. Interne IT- und Vorgangsdokumentation: Dokumentation der beim Kunden durchgeführten Tätigkeiten für spätere Recherchen.
Kategorien betroffener Personen:	☒ Kunden ☒ Interessenten
Kategorien personenbezogener Daten:	☒ Name ☒ Adressdaten ☒ Kontaktdaten ☒ Bankverbindung ☒ Geburtsdatum ☒ IT-Daten (z.B. Server, Netzwerk, PC, Zugangskennung, Passwort, etc.)
Kategorien besonderer personenbezogener Daten:	-
Kategorien von Empfängern der personenbezogenen Daten:	☒ intern (Michael Bär) ☒ extern (Internetshops , Hausbank)
Übermittlung der Daten an Dritte:	☒ findet statt, und zwar an: Internetshop (Name, Adressdaten, Kontaktdaten, Bankverbindung, Geburtsdatum) Cloudspeicher-Dienstleister (Name, Adressdaten, Kontaktdaten, Bankverbindung, Geburtsdatum, IT-Daten) ☒ innerhalb Deutschlands ☒ innerhalb der EU / EWR ☒ ggfs. in ein Drittland, sofern Standort des Cloud-Dienstleisters
Fristen zur Löschung der versch. Datenkategorien:	☒ unverzüglich, wenn Einwilligung widerrufen oder Vertragsverhältnis beendet
Beschreibung der technischen und organisatorischen Maßnahmen (TOM):	siehe Anhang „Anhang zum Verarbeitungsverzeichnis - TOM“ ab Seite 3

Anhang zum Verarbeitungsverzeichnis - TOM

Die Firma Bär IT-Service betreibt selbst keinen Handel und fungiert ggü. dem Kunden bei notwendigen Anschaffungen nur in beratender und vermittelnder Funktion. Zu diesem Zweck ist es u.U. notwendig, z.B. im Rahmen einer Bestellung von Hard-/Software, die personenbezogenen Kundendaten (Name, Adressdaten, Kontaktdaten, Bankverbindung, Geburtsdatum) an einen Internetshop weiterzugeben. In diesem Zusammenhang wir die Firma Bär IT-Service eine kundenindividuelle E-Mail-Adresse nach dem Muster kundenname@baer-it.net anlegen und hierüber den Bestellprozess abwickeln.

Um die vom Kunden beauftragten Arbeiten durchführen zu können, ist eine tiefgreifende Kenntnis über die IT-Landschaft des Kunden notwendig. Hierzu gehören vornehmlich folgende Daten:

- Art und Konfiguration des Netzwerkes
- Art und Konfiguration der Server/PCs/Drucker/Mobilen Endgeräte
- Zugangsdaten und Passwörter für Server/PCs/Drucker/Mobilen Endgeräte/E-Mail/Internet/ Router/Firewall/Softwareprogramme
- Zugangsdaten und Passwörter für webbasierte Verwaltung- oder Administrationsdienste
- Zugangsdaten für Fernwartungsdienste
- Zugangsdaten für Internetshops

Die genannten Daten werden von der Firma Bär IT-Service strukturiert in einem kundeneigenen Verzeichnis auf einem geeigneten Speichersystem (NAS oder Server-/PC-Festplatte) abgespeichert.

Um mobil auf die Datenbestände zugreifen zu können, werden die Daten bei einem Cloud-Dienstleister abgelegt. Für den mobilen Zugriff muss das mobile Endgerät spezifisch registriert und gekoppelt werden. Auf dem mobilen Endgerät selbst erfolgt die Absicherung zusätzlich per Passwort und/oder Biometrie.

Die Sicherung der Daten erfolgt täglich passwortgeschützt und verschlüsselt auf eine externe Festplatte und bei einem Cloud-Dienstleister.

Die Speicherung und Sicherung der Daten erfolgt passwortgeschützt/verschlüsselt. Die Verschlüsselung (intern: mittels Dateisystem / Cloud: mittels Software „Cryptomator“, siehe https://cryptomator.org/de/) entspricht hierbei immer dem aktuellen Stand der Technik.

Hinweise zur DSGVO-Konformität von Boxcryptor siehe:
https://cryptomator.org/de/privacy/

1. Gewährleistung der Vertraulichkeit

Zutrittskontrolle: *(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)*	- mechanische Fenstersicherungen - manuelles Schließsystem - Schließsystem mit Sicherheitsschlössern - Videoüberwachung - Bewegungsmelder
Zugangskontrolle: *(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden önnen.)*	- Erstellen von Benutzerprofilen mit unterschiedlichen Berechtigungen - Pflicht zur Passwortnutzung - Authentifikation durch biometrische Verfahren (Fingerabdruck) - Authentifikation durch Benutzername und Passwort

	- Einsatz von VPN-Technologie bei Zugriff von außen auf die internen Systeme - Einsatz von Intrusion-Detection-Systemen - Begrenzung der Fehlversuche bei Anmeldung am System
Zugriffskontrolle: *(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung 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.)*	- 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: *(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)*	- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern - logische Mandantentrennung - Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept - Trennung von Produktiv- und Testsystem
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
Pseudonymisierung:	./.
Verschlüsselung:	- Ggfs. Datenträgerverschlüsselung unter Windows mittels Bitlocker - Datenverschlüsselung beim Cloud-Dienstleister mittels Software „Cryptomator“, siehe: https://cryptomator.org/de/ - Zusätzliche Absicherung auf einem mobilen Endgerät per Passwort und/oder Biometrie
Zertifizierung (z.B. ISO):	./.

2. Gewährleistung der Integrität

Eingabekontrolle: *(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)*	- individuelle Benutzernamen für Nutzer - sichere Aufbewahrung und Entsorgung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden - Nachvollziehbarkeit durch Berechtigungskonzept
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.)*	- Nutzung von Standleitungen bzw. VPN-Tunneln verschlüsselte E-Mail-Übertragung (SSL/TLS) - vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe - festgelegte Löschfristen - sichere Transportverpackungen - sorgfältige Auswahl von Transportpersonal bzw. -dienstleistern - Nutzung von mobilen Datenträgern mit Verschlüsselungsfunktion

3. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle: *(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)*	- Ggfs. unterbrechungsfreie Stromversorgung (USV), zumindest für Server - Ggfs. Schutzsteckdosenleisten für EDV-Geräte - Ggfs. Feuer- bzw. Rauchmeldeanlagen - Datensicherungskonzept - regelmäßiges Testen der Funktionsweise der Datensicherung - Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort durch den Kunden

4. Gewährleistung der Belastbarkeit der Systeme

Belastbarkeit der IT-Systeme:	- Antiviren-Software - Software-Firewall - sorgfältige Auswahl der externen IT-Dienstleister

5. Wiederherstellung der Verfügbarkeit

Wiederherstellbarkeit von IT-Systemen:	- Datensicherung sowohl intern als auch ggfs. in der Cloud

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 Michael Bär