Version: 1.1 | Stand: 22. Mai 2018

Verzeichnis von Verarbeitungstätigkeiten

ideetion GmbH

ÖFFENTLICHES VERFAHRENSVERZEICHNIS

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO):	*ideetion GmbH* *Urbanstr. 104 A, 10967 Berlin*
Ggf. gemeinsamer Verantwortlicher:	
Gesetzlicher Vertreter:	*Stephan Tsoucalas,* *Urbanstr. 104 A, 10967 Berlin;* *sts(@)ideetion(.)de , 0176 31301182*
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO):	
Datenschutzbeauftragter	*DEDIS UG, Ruppiner Chaussee 331-335, 13503 Berlin*

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	• *E-Mailbe- und verarbeitung* • *Allgemeine Kundenverwaltung* • *Lohn- und Gehaltsabrechnung* • *Domainregistrierungen* • *Zertifikathandel*
Verantwortlicher Ansprechpartner:	*Stephan Tsoucalas, Geschäftsleitung* *Urbanstr. 104 A, 10967 Berlin;* *sts(@)ideetion(.)de , 0176 31301182*
Bei gemeinsamer Verantwortlichkeit:	*s. o.*
Status:	*In Betrieb*
Art der Verarbeitung / Name der Software:	*Monkey-Office, Outlook, Auftragsdatenverarbeitung*

Ort der Verarbeitung:	*Hetzner Online GmbH, Rechenzentren in Falkenstein und Nürnberg in Deutschland, zertifiziert nach ISO 27001, Auftragsverarbeitungsvereinbarung liegt vor.*

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	• *Verarbeitungstätigkeit: „E-Mailverarbeitung“ → verfolgte Zweckbestimmungen: „Durchführung der elektronischen Kommunikation, Erfüllung gesetzl. Anforderungen“* • *Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“ → verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung, Inkasso, Erfüllung gesetzl. Anforderungen“* • *Verarbeitungstätigkeit: „Lohn- und Gehaltsabrechnung“ → verfolgte Zweckbestimmungen: „zur Erstellung der Lohnabrechnung; Erfüllung gesetzl. Anforderungen“* • *Webhosting Kundenwebs, Webshops, CRMs, Mailing-Lists, Bereitstellung dedizierter Serversysteme → verfolgte Zweckbestimmungen: „Auftragsverarbeitung für Kunden“* • *Domainregistrierung und Zertifikatehandel → verfolgte Zweckbestimmungen: „Domainhandel und SSL-Zertifikate in öffentlichen CAs“*
Zweckänderung:	*./.*
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO:	*Soweit zutreffend:* • *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)* • *Einwilligung eines Kindes (Art. 6 Abs. 1 lit. a, Art. 8)* • *Vertrag oder Vertragsanbahnung (Art. 6 Abs. 1 lit. b)* • *Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f)* • *Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs.)* • *Sonstige (etwa DSAnpUG-EU)* • *Gesetzliche Aufbewahrungspflicht* • *Emailarchivierung*
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO:	*Die Rechtmäßigkeit orientiert sich neben den Prinzipien „Verhältnismäßigkeit“ (Art. 5 Abs. 1 lit. b), „Transparenz“ (Art. 5 Abs. 1 lit. a), „Datenminimierung“ (Art. 5 Abs. 1 lit. c), „Richtigkeit“ (Art. 5 Abs. 1 lit. d), „Speicherbegrenzung“ (Art. 5 Abs. 1 lit. c) und „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f), insbesondere an dem Prinzip der Zweckbindung (Art. 5 Abs. 1 lit. b)) und den gesetzlichen Vorgaben.*

Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	*Als Risiken stehen menschliches Fehlverhalten und noch nicht bekannte Sicherheitslücken der Hard- und Software immer im Vordergrund und können nicht ausgeschlossen werden. Systeme, die nicht verschlüsselt werden können, da auf ihre Daten ständig zugegriffen werden (Webserver z.B.) unterliegen an sich somit einem erhöhten Risiko.* *Weitere Informationen hierzu finden Sie in den TOM und weiteren nicht öffentlichen Dokumenten, wie dem internen Verfahrensverzeichnis und der Datenschutz-Folgeabschätzung mit Risikobewertung.*

Erhebung der Daten	
Kreis der betroffenen Personengruppen:	*Ausschließlich gewerbliche Kunden, Auftraggeber, Interessenten, Arbeitgeber, Mitarbeiter, Bewerber, Mieter, Lieferanten, Vermieter.*
Art der gespeicherten Daten bzw. Datenkategorien:	• *Abrechnungsdaten* • *Adressdaten* • *Bankverbindungsdaten* • *Bilddaten* • *Domainnamen* • *Geburtsdatum* • *IT-Nutzungsdaten/Log Daten/Protokolldateien* • *IP-Adresse* • *Interessen/Präferenzen* • *Kontaktdaten* • *Lohn-und Gehaltsdaten* • *Lebenslauf* • *Name/Vorname/Anrede/Titel* • *Qualifikationsdaten/Leistungs- und/oder Potenzialbeurteilung* • *Sozialversicherungsdaten* • *SSL Zertifikate* • *Standortdaten* • *Vertragsdaten* • *Vertragsstammdaten* • *Zahlungsdaten* • *Zeiterfassungsdaten*
Herkunft der Daten:	*Von Betroffenen selbst oder/und von Dritten bei der Auftragsverarbeitung*

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger:	*keine Weiteren.*
Externe Empfänger und Dritte:	*Konzerngesellschaft, Geschäftskunde, Finanzamt, Polizei, Staatsanwaltschaft.*

	• *Steuerberatung* • *vorbereitenden Buchhaltung* • *Direktversand* • *Versand-, Logistikunternehmen* • *Registrare, Domainregistrierungen*

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen:	*Geschäftsleitung*
Nachweis:	*Active-Directory, Berechtigungskonzept.*

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter:	*Wird im internen Verfahrensverzeichnis angegeben.*
Schriftlicher datenschutzkonformer Vertrag:	*Sind mit den auftragsverarbeitenden Unternehmen geschlossen. (internes Verfahrensverzeichnis)*
Geeignetheit des Auftragsverarbeiters:	*ISO Zertifizierungen, TOM der AV*
Standort der Verarbeitung:	*In der EU,* *Übermittlung von Daten in die jeweiligen für die TLD verantwortlichen Staaten*

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	*diverse*
Drittstaaten / internationale Organisationen:	*ICANN,* *Andere CCTlds:* *Dies beinhaltet auch die Übermittlung der dafür benötigten Registrierungsdaten in Einklang mit Art.49 Abs. 1b DSGVO.*
Angemessenes Datenschutzniveau durch:	*Nicht zutreffend:* • *Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO* • *Garantien gem. Art. 46 DSGVO* - *Verbindliche interne Datenschutzvorschriften (BCR)* - *EU-Standardvertrag* *andere getroffene nach Art. 49 Abs. 1. Abs. 2 DSGVO)*

Regelfristen für die Löschung der Daten	
Speicherdauer:	*Daten werden nach den gesetzlich vorgegebenen Mindestaufbewahrungsfristen aufbewahrt und nach deren Ablauf gelöscht.* *Sämtliche anderen Daten werden unmittelbar nach einer Karenzfrist von 30 Tagen aus den aktiven Systemen gelöscht. Die automatischen Backups werden entsprechend Ihrem Rotationszyklus bereinigt.*
Nachweis:	*Die Löschung erfolgt immer unmittelbar 30 Tage nach Kundenauftrag oder Vertragsende. Dies wird im Löschkalender und der Auftragsbearbeitung dokumentiert.*

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO):	• *die Pseudonymisierung erfolgt nicht, da keine personenbezogenen Daten länger als gesetzlich vorgeschrieben aufbewahrt und verwendet werden. Verschlüsselung personenbezogener Daten erfolgt über eine Komplettverschlüsselung des Systems, wodurch abgesichert ist, dass auch der Auftragsverarbeiter keinen Zugriff erlangen kann;* • *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sind auf Dauer sichergestellt, Datenverarbeitende Systeme sind zertifikatbasiert verschlüsselt erreichbar (SSL);* • *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen werden durch regelmäßige Backups im Snapshot-Verfahren gesichert und sich erprobte Technologien für eine schnelle Wiederherstellung;* • *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird durch ein umfangreiches Monitoring gesichert. Eine zuverlässige Überwachung der Serversysteme ist damit gewährleistet. Selbst unkritische Unregelmäßigkeiten werden gemeldet und durch Menschen ausgewertet. Bei einem kritischen Ereignis werden sofort entsprechende Maßnahmen eingeleitet.* *Es gelten die gesondert erstellten TOM.*
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM:	*Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit*

	und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche (und der Auftragsverarbeiter) geeignete TOM, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1).

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten:	*Noch nicht erfolgt*
Besteht weiterer Handlungsbedarf?	*ja*
Offene Maßnahmen:	*Internationale Einigung über die Anonymisierung / Pseudonymisierung der Domaininhaberdaten*
Datum der Dokumentation:	22.05.2018

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	*Erfolgt*
Datum, Unterschrift 22.05.2018	

Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, werden weitere Aspekte zur Verarbeitungstätigkeit zu dokumentiert.

- Informationspflichten (Art. 13 und 14 DSGVO);
- Risikobewertung
- Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit (Art. 35 DSGVO)
- Technische und organisatorische Maßnahmen (TOM)

Bei einer Anfrage der Aufsichtsbehörde werden weitere Nachweise vorgelegt.