

Auftrags-Datenverarbeitungs-Vertrag

zwischen

mangoit

- nachstehend Auftraggeber genannt -

und der

Tineon AG mit Sitz an der Uferpromenade 5 in 88709 Meersburg eingetragen im Handelsregister Freiburg i. Brsg. unter HRB 706 986, vertreten durch den alleinvertretungsberechtigten Vorstand Herrn Jean-Claude Parent

- Auftrags-Datenverarbeiter, nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Vereinbarung der Vertragsparteien bezüglich der Nutzung der S-Verein-Vereinsverwaltungs- sowie der Verein.Cloud Community-App, Web-App und Finanzbuchhaltungs-Softwarelösungen gemäß Lizenznutzungsvertrag und den Allgemeinen Geschäftsbedingungen, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

Im Rahmen der Leistungserbringung ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung der Leistungsvereinbarung.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Zweck der vorgesehenen Verarbeitung von Daten

Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung der Parteien.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien der (Vereins-)Mitglieder des Auftraggebers:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (z.B. Vereinsname, Adresse, vertretungsberechtigte Organe)

- Mitgliedshistorie
- Abrechnungs- und Zahlungsdaten zur Mitgliedschaft sowie Daten zu Zahlungsmöglichkeiten (z.B. Kontodaten, SEPA-Lastschriftmandate)
- Planungs- und Steuerungsdaten
- Bildaufnahmen / Fotos

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitglieder
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Sponsoren
- Fans

(4) Ferner werden aus den bestehenden Daten neue Daten generiert und gespeichert - dies umfasst insbesondere die automatische Erstellung von Rechnungen und Belegen, das Erstellen von Zuwendungsbescheinigungen sowie von Protokollen.

(5) Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung der Leistungsvereinbarung. Eine Kündigung der Leistungsvereinbarung bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

3. TOM-Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 1** dieses Vertrags aufgelisteten TOM-technische und organisatorische Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 1** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

4. Berichtigung, Einschränkung und Löschung von Daten

- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Schlussbestimmungen

- (1) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.
- (2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen der Artt 28 ff. DS-GVO am besten gerecht wird.

Meersburg 29.01.2024

Ort/Datum



.....

.....

Jean-Claude Parent, Vorstand

Anlage 1 - TOM Technisch Organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2 - Unter-Auftragsdatenverarbeiter und Rechenzentren der Tineon AG:

1. Domainfactory GmbH

Neuturmstrasse 5
80331 München/Deutschland
<https://www.df.eu/de/datenschutz/>

2. Hetzner Online GmbH

Industriestr. 25
91710 Gunzenhausen/Deutschland
<https://www.hetzner.com/de/legal/system-policies/>

3. teuto.net Netzdienste GmbH

Niedernstr. 26
33602 Bielefeld/Deutschland
<https://teuto.net/datenschutzhinweise/>

4. BuchhaltungsButler GmbH

Spreestraße 5

15913 Märkische Heide

<https://www.buchhaltungsbutler.de>

5. Billwerk+ Germany GmbH

Mainzer Landstraße 5

60329 Frankfurt am Main

<https://www.billwerk.com>