DATENSCHUTZKONZEPT DER MATE DEVELOPMENT GMBH

Inhalt

1. PRÄAMBEL

MATE Development GmbH, Rankestraße 9, 10789 Berlin, eingetragen beim Amtsgericht Charlottenburg unter HRB 117234 B, vertreten von den Geschäftsführern Florian Kühne, Matthias Heicke und Sven Frauen („Sweap“) bietet über die Internetseite sweap.io Softwareprodukte an Unternehmer in Ausübung ihrer Geschäfte oder selbstständigen beruflichen Aktivitäten im Sinne des § 14 BGB („Kunden“), an.

Die Kunden wünschen diese Produkte für die Zwecke eines besseren Event- und Organisationsmanagements innerhalb ihres jeweiligen Unternehmens als webbasierte SaaS bzw. Cloud-Lösung gemäß der Produktbeschreibung zu nutzen.

2. DATENSCHUTZRECHTLICHE ZIELE UNSERES UNTERNEHMENS

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

3. GELTUNGSBEREICH

Dieses Datenschutzkonzept richtet sich an folgende Personen:

- Die Personen oder Abteilungen, die über den Einsatz/die Bereitstellung eines Anwendungssystems entscheiden (Systemadministrator, kaufmännische Leitung, Geschäftsführung);
- Die Personen oder Abteilungen, die über die Nutzung des Systems für ihre Aufgaben entscheiden;
- Benutzer, d.h. diejenigen, die das zur Verfügung gestellte System für die Erledigung ihrer betrieblichen Aufgaben nutzen (bei Speicherung personenbezogener Daten auf einem Arbeitsplatzrechner entscheidet der einzelne Benutzer ggf. auch über die im System erfolgende Verarbeitung und die dazu verwendeten Programme);
- den Datenschutzbeauftragten, der ihre Umsetzung beratend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung des Datenschutzkonzepts verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden. Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über dieses Konzept informiert werden; das gilt auch für temporär Beschäftigte.

4. DATENSCHUTZBEAUFTRAGTER

MATE Development GmbH hat nach Maßgabe des Artikels 37 DSGVO einen externen Datenschutzbeauftragten ernannt. Die Kontaktdaten unseres Datenschutzbeauftragten sind zu finden unter:

PROLIANCE GmbH / www.datenschutzexperte.de
Datenschutzbeauftragter
Leopoldstr. 21
80802 München
datenschutzbeauftragter@datenschutzexperte.de

Der Datenschutzbeauftragte nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

5. GRUNDSÄTZE BEI DER VERARBEITUNG VON PERSONENBEZOGENEN DATEN

Bei der Verarbeitung von personenbezogenen Daten beachten wir die in Art. 5 DSGVO festgeschriebenen Grundätze. Danach sind personenbezogene Daten **rechtmäßig, transparent und unter Beachtung von Treu und Glauben** zu verarbeiten. Weiterhin dürfen sie nur für **festgelegte, eindeutige sowie legitime Zwecke** erhoben werden. Die Verarbeitung von Daten unterliegt einer **Zweckbindung**, das betrifft auch die Weiterverarbeitung. Nach dem **Prinzip der Datenminimierung** ist die Datenverarbeitung auf das notwendige Maß zu beschränken. Der **Grundsatz der Richtigkeit** erfordert, dass personenbezogene Daten sachlich richtig und aktuell sein müssen. In zeitlicher Hinsicht gibt es eine Speicherbegrenzung für den Zeitraum, für den die entsprechenden personenbezogenen Daten im Hinblick auf den Zweck der Datenverarbeitung benötigt werden.

Darüber hinaus beachten wir auch die **Grundsätze der Integrität und Vertraulichkeit** im Hinblick auf die Datenverarbeitung, was geeignete technische und organisatorische Maßnahmen umfasst, die die verarbeiteten Daten vor Verlust, unrechtmäßiger Verarbeitung, vor Zerstörung oder Schädigung schützen sollen.

6. ERHEBUNG/VERARBEITUNG VON PERSONENBEZOGENEN DATEN

6.1. Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

6.2. Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den

Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

6.3. Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Datenschutzbeauftragte zu kontaktieren.

7. VERPFLICHTUNG UND SCHULUNG DER MITARBEITER

7.1. Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten **zu verpflichten**.

7.2. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars durch den Vorgesetzten oder die Personalabteilung. Mitarbeiter, die ggf. darüber hinaus besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 TKG oder Berufsgeheimnisträger nach § 203 StGB) unterliegen, werden ergänzend schriftlich verpflichtet. Die jeweilige Verpflichtungserklärung ist zu den Personalakten zu nehmen.

7.3. Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist (sog. Need-to-know-Prinzip). Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen eines Berechtigungskonzepts. Siehe hierzu **Anlage „Berechtigungskonzept“.**

7.4. Jeder Mitarbeiter hat zu Beginn seiner Tätigkeit und danach einmal jährlich eine vom Unternehmen bereitgestellte **Schulung zum Datenschutz** und zum Umgang mit personenbezogenen Daten zu absolvieren. Die Teilnahme an der Schulung wird dokumentiert.

8. BESCHAFFUNG VON HARD- UND SOFTWARE

8.1. Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden Person/Abteilung durch die zentrale DV-Beschaffung.

8.2. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

8.3. Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten verwendet werden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z.B. private Notebooks) bedarf der Genehmigung durch die IT-Abteilung im Einzelfall. Die IT-Abteilung führt ein

Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme.

8.4. Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind sowohl der direkte Vorgesetzte als auch die DV-Abteilung unverzüglich zu informieren. Darüber hinaus ist bei Verdacht einer Datenschutzverletzung der Meldeweg einzuhalten (s. Punkt 13).

9. DATENHALTUNG/VERSAND/LÖSCHUNG

9.1. Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch die IT-Abteilung und der Registrierung durch die den Träger einsetzende Abteilung/Benutzer. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

9.2. Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen.

9.3. Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Diese sind in einem Löschkonzept festgehalten.

9.4. Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

10. PASSWORTRICHTLINIE

Um einen bestmöglichen Schutz für Daten in unserem Unternehmen zu gewährleisten und insbesondere den Zugang Unbefugter zu unseren Systemen zu verhindern, haben wir eine unternehmensweit geltende Passwortrichtlinie aufgestellt.

11. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Im Einklang mit Art. 30 DSGVO führen wir ein **Verzeichnis von Verarbeitungstätigkeiten**, in dem alle stattfinden Verarbeitungstätigkeiten unseres Unternehmens aufgeführt sind. Dieses findet sich in **Anlage „Verzeichnis von Verarbeitungstätigkeiten“.**

12. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen wir **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

13. UMGANG MIT DATENSCHUTZVORFÄLLEN

Jeder Mitarbeiter soll bei Datenschutzvorfällen (vermeintliche Datenschutzverletzung) diese seinem jeweiligen Vorgesetzten, dem Datenschutzkoordinator oder dem Datenschutzbeauftragten melden. In Fällen von

- unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder –
- bei Verlust personenbezogener Daten

ist der im Unternehmen vorgesehene Meldeweg zwingend einzuhalten, damit bestehende Meldepflichten von Datenschutzverletzungen erfüllt werden können.

14. EXTERNE DIENSTLEISTER/AUFTRAGSVERARBEITUNG/WARTUNG

14.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) oder mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten erhalten, so ist ein entsprechender den Anforderungen des Art. 28 DSGVO genügenden **Auftragsverarbeitungsvertrag** zu schließen.

14.2 Entsprechendes gilt, falls unser Unternehmen entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

15. UMGANG MIT BETROFFENENANFRAGEN

Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DSGVO oder seinem Berichtigungs- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, so erfolgt die Bearbeitung durch den verantwortlichen Bereich. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt. Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus diesem Datenschutzkonzept ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere

durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

Neben diesem Datenschutzkonzept bestehen ggfs. ergänzende Regelungen (z.B. interne Richtlinie, Vereinbarungen), die insbesondere zu Realisierung der Datensicherungsgebote des Art. 32 DSGVO zu treffenden Maßnahmen betreffen.