



UNTERNEHMENSGRUNDSÄTZE

Datenschutzgrundsätze

Verantwortung in Projekten und Geschäftsbeziehungen

Die EMOS Software GmbH achtet die Privatsphäre und den Schutz personenbezogener Daten. Diese Grundsätze beschreiben den Rahmen, an dem wir den Umgang mit personenbezogenen Daten in unseren Geschäftsbeziehungen und IT-Leistungen ausrichten.

In diesem Dokument

Zwecke Zuständigkeiten und Gestaltung	2
Schutzmaßnahmen Rechte und Überprüfung	3

Herausgeber

EMOS Software GmbH
Lateinschulgasse 15 · 94469 Deggendorf
emos@emos.de · +49 89 54558 119

Geschäftsführer Benjamin Artinger
Amtsgericht Deggendorf · HRB 2776

1 Rechtmäßigkeit und klare Zwecke

Personenbezogene Daten dürfen nur auf einer zulässigen Grundlage und für festgelegte, nachvollziehbare Zwecke verarbeitet werden. Umfang, Speicherdauer und Zugänglichkeit sind auf das für den jeweiligen Zweck erforderliche Maß zu begrenzen. Daten sind im erforderlichen Umfang richtig und aktuell zu halten.

Vertraulichkeit gilt auch innerhalb des Unternehmens. Beschäftigte und weitere berechtigte Personen dürfen Daten nur im Rahmen ihrer Aufgaben und Befugnisse nutzen. Eine eigenmächtige Weitergabe oder Nutzung für persönliche Zwecke ist unzulässig.

2 Zuständigkeiten in Kundenprojekten

Vor Beginn einer Verarbeitung sind die datenschutzrechtlichen Rollen und Verantwortlichkeiten zu klären. Ob EMOS als Verantwortlicher, Auftragsverarbeiter oder in einer anderen Rolle handelt, richtet sich nach der tatsächlichen Ausgestaltung der Leistung. Nicht jede IT-Dienstleistung stellt automatisch eine Auftragsverarbeitung dar.

Soweit eine Auftragsverarbeitung vorliegt, sind die erforderlichen Vereinbarungen vor Beginn abzuschließen. Daten dürfen dann nur im Rahmen dokumentierter zulässiger Weisungen verarbeitet werden. Abweichungen und unklare Weisungen sind vor ihrer Umsetzung zu klären. Weitergehende vertragliche Vorgaben des Kunden bleiben zu beachten.

3 Datenschutz durch Gestaltung

Datenschutzanforderungen sollen bereits bei Planung und Auswahl von Anwendungen berücksichtigt werden. Datenarme Voreinstellungen, begrenzte Zugriffsrechte und geeignete Trennung von Informationen unterstützen diesen Ansatz. Wo geeignet, sind anonymisierte oder pseudonymisierte Daten zu verwenden.

Für Entwicklung und Tests sind möglichst synthetische oder wirksam anonymisierte Daten einzusetzen. Ist die Verwendung personenbezogener Daten erforderlich, müssen Rechtsgrundlage, Berechtigungen und Schutzmaßnahmen geklärt sein. Pseudonymisierte Daten bleiben personenbezogene Daten, wenn eine Zuordnung weiterhin möglich ist.

4 Schutz und Einbindung von Dienstleistern

Technische und organisatorische Maßnahmen müssen zum Risiko der Verarbeitung passen. Dazu gehören je nach Schutzbedarf Berechtigungsmanagement, sichere Authentifizierung, geeignete Verschlüsselung, Aktualisierung von Systemen sowie Datensicherung und Wiederherstellung.

Weitere Dienstleister dürfen personenbezogene Daten nur im zulässigen und vereinbarten Rahmen erhalten. Erforderliche Verträge und Genehmigungen sind vorab sicherzustellen. Für Übermittlungen in Länder außerhalb des Europäischen Wirtschaftsraums müssen die jeweils geltenden Voraussetzungen erfüllt sein.

5 Verantwortungsvolle Nutzung von KI

Personenbezogene Daten dürfen nicht ohne rechtliche Grundlage und erforderliche Freigabe in externe KI-Anwendungen eingegeben werden. Bei der Auswahl eines Dienstes sind insbesondere Zwecke, Speicherverhalten, Zugriffsmöglichkeiten und eine mögliche Nutzung für das Modelltraining zu prüfen.

KI-Ausgaben können unrichtige oder nachteilige Aussagen über Menschen enthalten. Ihr Einsatz erfordert eine dem Zweck entsprechende Prüfung. Entscheidungen über Personen und erforderliche menschliche Kontrolle sind unter Beachtung der jeweils anwendbaren Anforderungen auszugestalten.

6 Aufbewahrung und Löschung

Personenbezogene Daten sind zu löschen oder zu anonymisieren, sobald der zulässige Zweck entfällt und keine vorrangigen Aufbewahrungspflichten oder anderen zulässigen Gründe entgegenstehen. Für Kundenprojekte sind Rückgabe und Löschung im Rahmen der jeweiligen Verantwortlichkeiten zu vereinbaren.

Bei Aufbewahrungspflichten ist der Zugriff auf den erforderlichen Personenkreis zu begrenzen. Datenträger und Geräte dürfen erst nach angemessener Datenlöschung oder sicherer Vernichtung weitergegeben beziehungsweise entsorgt werden.

7 Rechte Anliegen und Vorfälle

Betroffene Personen können sich mit Datenschutzanliegen an EMOS Software GmbH, Lateinschulgasse 15, 94469 Deggendorf, oder an emos@emos.de wenden. Anliegen sind zu prüfen und entsprechend den gesetzlichen Voraussetzungen zu bearbeiten. Bei einer Auftragsverarbeitung unterstützt EMOS den verantwortlichen Kunden im vereinbarten und gesetzlich erforderlichen Umfang.

Mögliche Datenschutzverletzungen sind unverzüglich intern zu melden und zu bewerten. Meldungen an Kunden, Aufsichtsbehörden oder betroffene Personen richten sich nach den jeweiligen Rollen und gesetzlichen sowie vertraglichen Anforderungen.

8 Einordnung und Überprüfung

Diese Grundsätze ergänzen unsere Informationssicherheitsleitlinie. Sie ersetzen keine konkreten Datenschutzhinweise nach den gesetzlichen Informationspflichten, insbesondere nicht die Datenschutzerklärung der Website. Die Geschäftsführung überprüft sie mindestens jährlich und bei wesentlichen Änderungen.