Datenschutzkonzept

1. Präambel

Der Schutz der personenbezogenen Daten unserer Kunden und Interessenten unterliegt höchster Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz bei Megatech berücksichtigt, umgesetzt und gelebt wird. Bei uns wird für die Datenverarbeitung nach folgendem Datenschutzkonzept verfahren:

Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

gewährleistet werden.

Die Sicherheitsmaßnahmen werden in dem Datenschutzkonzept in die Bereiche

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Nutzung der Internetdienste und
- Nutzung der Telekommunikationsdienste

gegliedert und geben mithin ein hohes Sicherheitsniveau vor.

2. Datenschutzrechtliche Rahmenbedingungen

Das Erheben und Verarbeiten personenbezogener Daten ist im Bundesdatenschutzgesetz (BDSG) und im neueren Telemediengesetz (TMG) geregelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (so genannter Betroffener).
Generell gilt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn gesetzliche Vorschriften dies ausdrücklich zulassen oder der Betroffene ausdrücklich eingewilligt hat. Die Einwilligung ist nur wirksam, wenn der Nutzer über die Tragweite des Verfahrens informiert wurde, dies heißt, welche Daten zu welchem Zweck in welcher Form gespeichert und verarbeitet werden und die Einwilligung nicht in anderen Erklärungen versteckt worden ist.

3. Inhalt und Zweck des Konzeptes

Grundvoraussetzung für den Datenschutz ist die Datensparsamkeit. Daraus resultiert, dass nicht mehr Daten als benötigt verwendet werden.
Die erhobenen persönlichen Daten dürfen nur zu Ihrem bestimmten Zweck verwendet werden. Die Zustimmung des Betroffenen ist zwingend von Nöten.

4. Beteiligte, speichernde Stellen im Sinne des Datenschutzes

Die beteiligte speichernde Stelle im Sinne des Datenschutzes ist die Megatech Software GmbH. Diese wird durch den Geschäftsführer Jochen vertreten.
Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt daher bei der Geschäftsführung.

5. Verpflichtung zum Datenschutz

Die Megatech Software GmbH, eingeschlossen ihrer Mitarbeiter /-innen verpflichten sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen haben eine entsprechende Datenschutzerklärung zur Geheimhaltungspflicht unterzeichnet.

6. Beschreibung der personenbezogenen Daten und Angaben der jeweiligen Zweckbindung (Nutzungszweck)

6.1 Kundendaten

Bei dem betroffenen Personenkreis handelt es sich um Kunden der Megatech Software GmbH. Bei den Daten handelt um

- Firma
- Ansprechpartner
- Kontaktdaten
- Rechnungsdaten

internen Zuweisungen wie

- Kundennummern
- Freischaltungscodes
- Online-Lizenzen

Die Daten werden zu Zwecken der

- Kundenbetreuung
- Kundengewinnung
- Abwicklung von Rechnungsmodalitäten
- Interne Auswertung
- Marketingzwecke

verwendet.

6.1.1 Rechtsgrundlage

Die Rechtsgrundlage zur Nutzung der Erhobenen Daten bildet das Datenschutzgesetz.

6.2 Lieferantendaten

Lieferanten und Dienstleister werden von uns auf Einhaltung bestehender Datenschutzrichtlinien geprüft.

Bei Lieferanten erhobenen Daten handelt es sich um

- Firma
- Ansprechpartner
- Kontaktdaten

Die Daten werden zu Zwecken der

- Kundengewinnung
- Marketingzwecke

verwendet.

6.3 Mitarbeiterdaten

- Gehaltsberechnung
- Gehaltsabrechnung
- Mitarbeiterbeurteilungen
- QM-System / Organigramm

6.4 Daten von Schülern, Studenten und Dozenten

Bei dem betroffenen Personenkreis handelt es sich um Schüler, Studenten und Dozenten, die eine kostenlose MegaCAD Ausbildungsversion der Megatech Software GmbH als Online-Lizenz in der Schule / (Fach-)Hochschule und zuhause nutzen wollen.
Bei den Daten handelt es sich um

- Name der Schule / (Fach-)Hochschule
- Name des Schülers, Studenten oder Dozenten
- Kontaktdaten des Schülers, Studenten oder Dozenten
- Erklärung, dass die Ausbildungsversion nicht gewerblich genutzt wird.

Zur internen Zuweisung von

- Online-Lizenzen
- internen Auswertung

verwendet.

7. Verfahrensbeschreibung

Für standardisierte Verfahren sind unter anderem

- Die Erhebung
- Der Zweck
- Die Weitergabe
- Die Löschung

In einer Verfahrensbeschreibung (Workflow) festzulegen und auf dem neuesten Stand zu halten. Das Verfahrensverzeichnis wird vom Datenschutzbeauftragten geführt, per Dienstanweisung ist geregelt, dass alle Mitarbeiter und Führungskräfte den Datenschutzbeauftragten bei der Führung des Verfahrensverzeichnisses größtmögliche Unterstützung geben.

8. Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz

Entsprechend den datenschutzrechtlichen Bestimmungen sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

a) nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
b) personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
c) personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
d) jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
e) festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
f) die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

9. Vertraulichkeit

9.1 Vertraulichkeit

9.1.1 Zutrittskontrolle

Der Zugang zu den Räumlichkeiten ist nur autorisierten Personen möglich. Berechtigt sind alle Mitarbeiter/-innen der jeweiligen Niederlassung.

9.1.2 Zugangskontrolle

Der elektronische Zugang zu den Systemen ist durch Firewall-Technologien geschützt. Der Zugang ist nach heutigen technischen Standards mittels VPN-Technologie und SSL-Verschlüsselung gesichert.
Zugangsdaten zur Administration und Wartung der Firewall-Dienste sind Administratoren und verantwortlichen Mitarbeitern bekannt. Die Passwörter werden regelmäßig geändert.

9.1.3 Zugriffskontrolle

Der Datenzugriff ist ausschließlich über unsere Softwarelösungen möglich und nach Mandanten getrennt. Die Mandantendaten sind logisch voneinander getrennt und verfügen jeweils über eine eigenständige Benutzer- und Zugriffsverwaltung für die Vergabe individueller Zugriffsberechtigungen. Auf Basis eines kundenspezifischen Rollenkonzepts werden Zugriffsberechtigungen definiert, damit personenbezogene Daten nach ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

9.1.4 Weitergabekontrolle

Eine elektronische Weitergabe (Übertragung) von Daten erfolgt automatisiert mittels standardisierter Export-Schnittstellen innerhalb der Anwendungsumgebung. Der Zugriff auf Schnittstellen wird anwendungsseitig auf Basis der Berechtigungen gesteuert. Die Zugangskontrolle erfolgt anhand der eingesetzten technischen Komponenten.
Die Verfahren zur Übertragung an weitere Stellen (Dritte) werden anhand einer Schnittstellenspezifikation definiert und sind in der Ausführung durch den Auftraggeber steuerbar, die technischen Eigenschaften und Verfahren dann spezifisch in Abstimmung mit dem Auftraggeber definiert und innerhalb der Dokumentation berücksichtigt. In dieser Abhängigkeit sind ggfs. zusätzliche datenschutzrechtliche Regelungen mit Dritten zu vereinbarem.

9.2 Integrität

9.2.1 Eingabekontrolle

Anwendungsseitig ist gewährleistet, dass berechtigte Benutzer (i.d.R. Administratoren) nachträglich feststellen können, wann und von wem personenbezogene Daten erfasst, verändert oder entfernt worden sind. Die Dokumentation erfolgt zum Kundendatensatz und ist nicht manipulierbar.

9.2.2 Auftragskontrolle

Auf Basis der Datenschutzerklärung zur Auftragsdatenverarbeitung wird gewährleistet, dass die Verarbeitung von personenbezogenen Daten nur entsprechend den Weisungen des Vertragspartners (Nutzers) durchgeführt wird.

9.3 Verfügbarkeit

9.3.1 Verfügbarkeitskontrolle

Die Daten werden von Megatech, entsprechend dem vorliegenden Backup-Konzept gesichert. Eine Kontrolle des Backups erfolgt nicht.

9.4 Authentizität

Die Authentizität der Daten ergibt sich aus den in den verschiedenen Informationssystemen implementierten Verfahren, die eine Authentizität gewährleisten, zusammen mit den Organisationskonzepten:

- Berechtigungskonzept
- Sicherheitskonzept
- und das hier vorliegende Datenschutzkonzept.

9.5 Revisionsfähigkeit

Die Revisionssicherheit der erhobenen Daten wird gewährleistet durch:

- Die Ordnungsmäßigkeit der Datenerhebung und –Verarbeitung.
- Die Sicherheit des Gesamtverfahrens, gewährleistet durch die organisatorischen Maßnahmen sowie die entsprechenden Umsetzungen (Sicherheitskonzept).
- Die Sicherung vor Verlust der Daten durch ein Backup-Konzept sowie dessen Umsetzung.
- Die Gewährleistung, dass eine Nutzung der Daten nur durch Berechtigte erfolgt (Berechtigungskonzept).
- Die Einhaltung der gesetzlich geforderten Aufbewahrungsfristen (Archivordnung).
- Dokumentation der einzelnen Verfahren in entsprechenden Konzepten.

9.6 Transparenz

Dem Transparenzgebot wird durch dieses Datenschutzkonzept genügt, in dem die Methoden der Erhebung und Nutzung der Daten beschrieben wird.