Annex 4

CRM SOLUTIONS GMBH – HAMBURG

Technische und organisatorische Maßnahmen

nach Art. 32 Abs. 1 lit. b DS-GVO

Änderungen bleiben vorbehalten
Version 1.05 / 12.2020

gültig ab dem: 07.05.2018

CRM Solutions GmbH
Kattrepel 2 (Montanhof)
20095 Hamburg

Telefon: +49 40 68 98 99 9 - 80
info@crm-solutions-gmbh.de
www.crm-solutions-gmbh.de

Geschäftsführer:
André Büggel, Viktor Polischuk
Amtsgericht Hamburg HRB 98788

Commerzbank HH
BLZ 200 400 00, Kto. 363 060 500
IBAN DE 86200400000363060500
BIC COBADEFFXXX

Inhalt

§ 1 Verantwortliche Stelle

§ 2 Unternehmen

CRM Solutions GmbH
Kattrepel 2 (Montanhof)
20095 Hamburg

Tel.: +49 40 68 98 99 9-80

E-Mail: support@crm-solutions-gmbh.de
Internet: www.crm-solutions-gmbh.de

§ 3 Gesetzlicher Vertreter (Geschäftsführung)

Herr André Büggel
Tel.: 040 / 68 98 99 9-80
E-Mail: andre.bueggel@crm-solutions-gmbh.de

Herr Viktor Polischuk
Tel.: 040 / 68 98 99 9-80
E-Mail: viktor.polischuk@crm-solutions-gmbh.de

§ 4 Datenschutzbeauftragter des Auftragsverarbeiters

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH
Datenschutzbeauftragter: Herr Dipl.-Inform. Olaf Tenti
Telefon: 02331/356832-0
E-Mail: datenschutz@gdi-mbh.eu

1 Technische und organisatorische Maßnahmen

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

1.1.1 Zutrittskontrolle

Das Bürogebäude befindet sich innerhalb eines Betriebsgeländes. Eine Bewachung des Geländes ist sowohl innerhalb als auch außerhalb der Betriebszeiten durch Wachpersonal gewährleistet. Die Hauseingangstür verfügt über ein automatisiertes Schließsystem, welches außerhalb der Öffnungszeiten (Mo-Fr 07:00 Uhr bis 17:00 Uhr) mit einem RFID-Chip geöffnet werden kann. Für Besucher kann die Eingangstür per Fernzugriff und Festnetznummer über die Zentraleinheit geöffnet werden.

Der Geschäftsbereich befindet sich im Obergeschoss des Gebäudes und ist nur über eine zentrale Zugangstür erreichbar. Die Zugangstür ist grundsätzlich verschlossen.

Besucher nutzen die Klingel an der Büroeingangstür. Die Türöffnung erfolgt manuell durch Mitarbeiter. Ein unbefugter oder unbemerkter Zugang zum Geschäftsbereich ist damit ausgeschlossen. Besucher betreten die Büroräume nur in Begleitung eines Mitarbeiters.

Alle Mitarbeiter wurden im Rahmen einer Datenschutzunterweisung darauf hingewiesen, dass sie verpflichtet sind, personenbezogene und vertrauliche Daten vor unberechtigten Zugriffen zu schützen und betriebsfremde Personen nicht unbeaufsichtigt zu lassen.

Server, TK-Anlagen sowie Netzverteiler sind innerhalb des Geschäftsbereichs abgegrenzt. Der Unternehmensserver befindet sich in einem ISO 27001 zertifiziertem Rechenzentrum mit Zutrittskontrollsystem, Videoüberwachung, Brandmeldeanlage, einem automatischem Trigon-Brandlöschsystem, USV-unterbrechungsfreier Stromversorgung, Notstromversorgung durch Dieselaggregat sowie einem redundanten Kühlsystem.

Es finden sich keine Schlüssel oder RFID-Chips bei betriebsfremden Personen. Alle Schlüssel- und Chipinhaber werden in einer Liste geführt. Die Schlüsselinhaber haben beim Schlüsselerhalt eine schriftliche Belehrung zur Aufbewahrung erhalten, d.h. keine Kennzeichnung der Schlüssel und unmittelbare Mitteilung an die Geschäftsleitung bei Schlüssel- oder Chipverlust.

Schlüsselkopien können nur unter Vorlage des Sicherheitszertifikats beim Hersteller erzeugt werden. Das Zertifikat befindet sich beim Vermieter.

Im Gebäude sind Rauchmelder installiert, die einen Innenalarm auslösen.

1.1.2 Zugangskontrolle

Anmeldungen erfolgen ausschließlich über das Domainkonto. Alle integrierten Systeme haben eine individuelle und geheime Anmeldung mit Namen und verschiedenen Passwörtern. Die Passwörter sind geheim und werden an keiner Stelle im Klartext gespeichert.

Alle Passwörter bestehen aus Kombinationen von mindestens 10 Zeichen, Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen und werden regelmäßig geändert (90 Tage). Die Passwortkonvention des Terminalservers wird vom Betriebssystem bzw. von den Anwendungen eingefordert. Die Mitarbeiter sind über die Notwendigkeit der Passwortkonvention unterrichtet und angewiesen, diese umzusetzen.

Jeder Nutzer hat die Möglichkeit sein Passwort in den einzelnen Systembereichen und Anwendungen selbst zu ändern.

Auf allen Arbeitsplätzen ist ein passwortgeschützter Bildschirmschoner aktiviert, der sich nach Ablauf von 10 Minuten automatisch einschaltet. Alle Mitarbeiter sind zudem angewiesen, eine manuelle Bildschirmsperre bei Verlassen des Arbeitsplatzes vorzunehmen. Damit wird unbefugte Nutzung bei Abwesenheit des Mitarbeiters verhindert.

Der Internetzugang erfolgt über ein Modem und Router. Die Konfiguration der lokalen Firewall ist nur einem autorisierten Personenkreis möglich.

Die Aktualisierung der Sicherheitspatches erfolgt regelmäßig und automatisch, kann bei Bedarf auch manuell erfolgen.

Homeoffice-/Telearbeitsplätze verfügen über eine Einwahlmöglichkeit in das Firmennetzwerk. Die Einwahl erfolgt über eine gesicherte VPN-Verbindung.

Alle Mitarbeiter haben eine Verpflichtungserklärung auf die Vertraulichkeit nach Art. 5 Abs. 1 lit. f i.V.m. Art. 32 Abs. 4 DS-GVO sowie auf die Wahrung von Geschäftsgeheimnissen gem. § 23 GeschGehG unterzeichnet, in der alle Regeln im Umgang mit schutzwürdigen und personenbezogenen Daten festgehalten sind.

Nicht flüchtige Speicher (Flash oder Festplatten) in den Geräten werden vor der Entsorgung mechanisch zerstört oder datenschutzkonform formatiert, so dass eine Wiederherstellung der Daten ausgeschlossen ist.

1.1.3 Zugriffskontrolle und Speicherkontrolle

Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Programme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.

Das Kopieren von Daten ist nur im Rahmen der Datensicherung und für die besonders geregelten Fälle der Datenweitergabe erlaubt, z.B. notwendiger Datenaustausch mit Kunden. Der Datenaustausch erfolgt über einen separaten Bereich im Netzwerk des virtuellen Servers. Der Zugang ist passwortverschlüsselt.

Test- und Entwicklungssysteme befinden sich in einem eigenen Datenbereich auf dem virtuellen Server.

Die Administrationsrechte für das interne Firmennetz hat nur ein eingeschränkter Personenkreis. Die Rechte sind über separate Zugriffe geregelt.

Das Netzwerk ist vollständig dokumentiert.

Alle Notebooks, Rechner und externen Speichermedien sind zum Schutz vertraulicher oder personenbezogener Daten vollständig verschlüsselt. Damit wird ein Zugriff Unbefugter auf die Daten verhindert.

Die Wartung des Firmennetzwerkes erfolgt nur auf Freigabe.

1.1.4 Trennungskontrolle

Das Prinzip der Funktionstrennung wird konsequent eingehalten, dabei erfolgt eine strikte Trennung zwischen auftragsbezogenen und internen Verarbeitungen, und zwar organisatorisch und datentechnisch.

Schutzwürde Daten werden nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.

Es ist gewährleistet, dass Daten zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Personal-Kundennummer) erhobene bzw. gespeicherte Daten getrennt verarbeitet werden können.

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

1.2.1 Weitergabekontrolle

Die Vernichtung von Akten und anderem vertraulichem Schriftgut sowie Datenträgern wie CDs und DVDs wird mit einem Schredder der Sicherheitsstufe P-4 nach DIN 66399 durchgeführt. Für Papierdokumente wird die Partikelbreite von 4 mm und die Partikellänge von 35 mm nicht überschritten.

Nicht mehr benötigte Festplatten und Datensicherungsbänder, werden vor der Entsorgung mechanisch durch eine Bohrung zerstört. Diese Regelung trifft für interne, als auch für Kundengeräte zu.

Die auf Basis eines Vertrages und einer Geschäftsbeziehung bestehenden erforderlichen Daten sind über einen separaten, passwortgeschützten Bereich des virtuellen Servers erreichbar. Zugriffsberechtigung erhalten nur der Kunde sowie der für die Auftragsverarbeitung zuständige Support-Mitarbeiter. Daten werden nach Projektende gelöscht. Dokumente werden revisionssicher archiviert und nach Ablauf der gesetzlichen Aufbewahrungsfristen vollständig, datenschutzgerecht und dauerhaft gelöscht.

Der Fernzugriff zu Wartungszwecken auf ein Kundennetz erfolgt auf Weisung des Kunden und je nach Zweck per:

Fernzugriff auf Server
Der Fernzugriff ins Kundennetzwerk erfolgt über eine gesicherte VPN-, Remote-Desktop- oder TeamViewer-Verbindung (TeamViewer Host) oder eine administrative Benutzerberechtigung. Der Zugriff erfolgt ausschließlich weisungsgebunden auf Basis eines bestehenden Service- oder Wartungsvertrages und bedarf keiner zusätzlichen Autorisierung. Support-Mitarbeiter besitzen nur die Einwahlberechtigung für die von ihm betreuten Kundennetzwerke. Die Zugangsdaten sind individuell und werden von einem eingeschränkten Personenkreis verwaltet.

Fernsteuerung
Eine Fernsteuerung erfolgt nur unter Aufsicht und Zustimmung des Kunden. Für die Fernsteuerung

wird das Programm TeamViewer eingesetzt. Für jede Fernsteuersitzung wird eine neue Sitzungs-ID durch den ferngesteuerten Arbeitsplatz vergeben. Alle Verbindungen mit TeamViewer sind verschlüsselt und damit sicher vor dem Zugriff Dritter geschützt.

1.2.2 Eingabekontrolle

Die eingesetzten CRM-Systeme, die für die Kundenbeziehungen genutzt werden, protokollieren die Änderungen mit Namen und Zeitstempel revisionssicher.

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

1.3.1 Verfügbarkeitskontrolle

Der Unternehmensserver befindet sich in einem ISO 27001 zertifiziertem Rechenzentrum mit Zutrittskontrollsystem, Videoüberwachung, Brandmeldeanlage, automatisches Trigon-Brandlöschsystem, USV-unterbrechungsfreier Stromversorgung, Notstromversorgung durch Dieselaggregat sowie einem redundanten Kühlsystem.

1.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Die zur Auftragsverarbeitung erforderlichen Daten sowie unternehmensinterne Daten werden regelmäßig gesichert. Datensicherungen und Backup-Prozesse werden kontinuierlich auf Wiederherstellbarkeit und Funktion getestet und angepasst.

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

1.4.1 Auftragskontrolle

Eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO findet ausschließlich auf Weisung des Auftraggebers und auf Basis eines Vertrages statt. Weisungsänderungen durch den Auftraggeber erfolgen schriftlich und werden auf Vertrags- und Datenschutzkonformität überprüft. Alle Mitarbeiter werden regelmäßig im Umgang mit personenbezogenen Daten geschult.

1.4.2 Kontrollverfahren

Der Datenschutz und das Datenschutzmanagement (Incident-Responce-Management, Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)) unterliegen einem kontinuierlichen Verbesserungsprozess und werden an die aktuellen und gültigen Datenschutzbestimmungen angepasst. Eingesetzt sind Firewalls, Spamfilter, Virenscanner. Ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen sowie die entsprechend dokumentierte Vorgehensweise ist vorhanden. Verfahrensweisen und Regelungen zum Datenschutz sind zentral dokumentiert (ELO-Archivsystem) mit Zugriffsmöglichkeit für alle Mitarbeiter. Eine Aktualisierung der technischen und organisatorischen Maßnahmen findet fortlaufend statt und wird protokolliert. Zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen wird das interne Verfahrensverzeichnisse jährlich im Rahmen eines Datenschutz-Audit geprüft und fortlaufend aktualisiert (d. h. neue und veränderte

Verfahren an den Datenschutzbeauftragten gemeldet); Sicherheitsmaßnahmen werden regelmäßig kontrolliert. Es ist ein externer Datenschutzbeauftragter (GDI Gesellschaft für Datenschutz und Informationssicherheit mbH) gestellt.