Maßnahmen nach Art. 32 I DS-GVO

Technische Organisatorische Maßnahmen TOMs

der Yoummday GmbH, Infanteriestraße 11a, Haus E2, 80797 München

Stand: 2024

Inhaltsverzeichnis:

Verantwortung des für die Verarbeitung Verantwortlichen gemäß Art. 24 EU DS-GVO.

I. Grundsätze

Als verantwortliche Stelle wurden geeignete technische und organisatorische Maßnahmen getroffen, welche die Einhaltung der Grundsätze der Europäischen Datenschutzgrundverordnung sicherstellen. Hiermit kann sichergestellt werden und der Nachweis erbracht werden, dass die Verarbeitung gemäß den Vorschriften der EU-DSGVO erfolgt.

Die folgenden Maßnahmen dienen der Gewährleistung der Vertraulichkeit der Systeme und dienen der

- Gewährleistung der Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Integrität der Systeme und Dienste
- Gewährleistung der Verfügbarkeit der Systeme und Dienste
- Gewährleistung der Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen und technischen Zwischenfall.
- Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Die zu treffenden technischen und organisatorischen Maßnahmen orientieren sich an:

- Stand der Technik
- den Implementierungskosten
- Art, Umfang, Umstände und Zweck der Verarbeitung
- der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Dabei wird ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleistet. Zur Aufrechterhaltung des Schutzniveaus werden die Maßnahmen regelmäßig überprüft und aktualisiert.

II. IT-Infrastruktur

siehe Dokument: Technisches Setup

III. Leiter IT

Leiter-IT:

Wolfgang Maier, Head of IT
E-Mail: wolfgang.maier@yoummday.com

Stellvertreter:

Florian Neumeier, VP Product & Tech
E-Mail: florian.neumeier@yoummday.com

Datenschutzbeauftragter:

Björn Barthelmes
Karl-Frank-Straße 35
12587 Berlin
E-Mail: datenschutz@yoummday.com

Datenschutzkoordinator:

Jörg Hoffmann
E-Mail: joerg.hoffmann@yoummday.com
Telefon: +49 89 231 66 00-03

IV. Einzelmaßnahmen

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

1.1 Zutrittskontrolle

Schutz der Räume mit Datenverarbeitungsanlagen vor dem Zutritt Unbefugter

Anforderung	Status
Sicherungseinrichtung Grundstück	(+) Das Betriebsgelände, auf dem Rechner untergebracht sind, ist teilweise umzäunt, (+) Toranlage mit Anmeldung
Geländeüberwachung	(+) Videoüberwachung mit Kamerasteuerung, (+) die Videoüberwachung ist mit Hinweisschildern gekennzeichnet
Zutrittskontrollsystem Gebäudesicherung	(+) Schließsystem Sicherheitsschloss (+) Schließsystem digitales Schloss mit codiertem Schlüssel (+) Schließsystem RFID Chip
Zentraler Empfangsbereich	(+) Alle Besucher haben sich beim Empfang anzumelden und sind in die Besucherliste ein- und auszutragen sowie im Haus zu begleiten.
Zutrittskontrollsystem Geschäftsräume	(+) Schließsystem Sicherheitsschloss (+) Schließsystem RFID Chip
Maßnahmen bei Verlust eines Schlüssels/Karte/Chip	(+) Austausch der Schließanlage mit Schlüsseln (+) Neuprogrammierung des Codes
Überwachungssysteme Gebäude	(+) Rauchalarmanlage, (+) Brandalarmanlage
Sicherung der Serverräume	(+) Schließsystem digitales Schloss mit codiertem Schlüssel
Externe Dienstleister	(+) Alle externen Handwerker, Haus- und RZ-Techniker müssen sich zu Beginn ihrer Arbeiten am Empfang anmelden. Dieser informiert den Mitarbeiter, der den Besuch erwartet und veranlasst die Abholung. Ist weder der gewünschte Mitarbeiter noch ein anderer Mitarbeiter, der mit der Aufgabe für den

	externen Handwerker, Haus- oder RZ-Techniker vertraut ist, erreichbar, darf kein Zutritt gewährt werden.
Schlüssel/Schlüsselvergabe	(+) Die Schlüsselvergabe erfolgt durch das zentrale Gebäudemanagement. (+) Jeder ausgegebene Schlüssel wird in ein Schlüsselbuch oder in einem Schlüsselmanagementsystem erfasst.
Besonderer Schutz des Rechenzentrums	(+) Aufteilung des Rechenzentrums nach Schalenprinzip. (+) Zutritt zum Rechenzentrumsräumen durch Schleusen. (+) Videoüberwachung (+) Bewegungsmelder (+) Rauchmelder (+) Temperaturüberwachung (+) Alarmanlage

Rechenzentrum der Yoummday GmbH:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland, Tel.: +49 (0)9831 505-0, Fax: +49 (0)9831 505-3

Die vollständige Adresse des Rechenzentrums lautet wie folgt:

Hetzner Online GmbH, Am Datacenter-Park 1, 08223 Falkenstein/Vogtland.

1.2 Zugangskontrolle

Schutz der Computersysteme gegen den Zugang für Unbefugte

Anforderung	Status
Zugang zu Systemen nur über Zugangsberechtigungen	(+) Der Zugang zu den Systemen erfolgt grundsätzlich über eine Benutzerkennung und ein entsprechend sicheres Kennwort
Benutzer Authentifizierung	(+) User ID und Passwort (+) Passwort Mindestlänge
Kontrolle der Passwortkonventionen	(+) Freigabe nur durch Administrator
Rechteverwaltung	(+) Für die Rechteverwaltung besteht ein Rechtekonzept. (+) Alle Berechtigungen sind nachvollziehbar dokumentiert (+) Die Rechteänderung erfolgt in folgenden Fällen (+) Ausscheiden eines Mitarbeiters,

Bildschirmsperre	(+) Bildschirmsperre bei der Abwesenheit mit Passwortkennung ist eingerichtet.
Firewall	(+) Open Source iptables
WLAN	(+) physikalische Trennung des Gäste-WLANs vom Firmen Netz
Sicherheit von Notebooks	(+) User ID und Passwort
Protokollierung und Kontrolle fehlerhafter Anmeldungen	(+) Fehlerhafte Anmeldungen werden protokolliert und bei Bedarf ausgewertet.
Automatische Sperrung PC (z.B. Kennwort und Pausenschaltung)	(+) Eine automatische Sperrung des PC erfolgt nach 10 Minuten.
Sichere Anbindung für „Remote Zugriff“	Der „Remote Zugriff“ aus dem „Home-Office“ auf Systeme ist mit eigenen PCs und Laptops nur unter folgenden Bedingungen möglichmöglich. (+) User ID und Passwort (+) Daten werden verschlüsselt übertragen

1.3 Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle sind darauf gerichtet, unerlaubte Tätigkeiten (z.B. unbefugtes lesen, kopieren, verändern oder entfernen) in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern.

Es ist ein streng überwachtes Berechtigungskonzept mit persönlichen Benutzerkonten eingerichtet. Der Zugriff auf bestimmte Informationen wird über ein Gruppen- bzw. Rollenkonzept gewährt.

Schutz der Daten gegen den Zugriff Unbefugter

Anforderung	**Status**
schriftliches Administrationskonzept	(+) einheitliche Vorgaben zu IT-Sicherheit (+) Trennung von Verantwortlichkeiten (+) Administratoren sind eigene Mitarbeiter (+) Trennung der Administratorenkonten nach Systemen und Personen

Identifizierung und Authentifizierung der Administratoren	(+) UserID und Passwort
Admin Passwortkonventionen	(+) Zeichenmindestlänge alphanumerischer Zeichensatz, (+ Ausschluss Trivialkennwort, (+) Passworteingabe mit verschlüsseltem Vorgang (+) sichere Passwortdateien
Rollenbasiertes Berechtigungskonzept	(+) Ein rollenbasierendes Nutzerberechtigungskonzept ist gesetzt.
Restriktives Rechtevergabesystem	(+) Die Zugriffsberechtigung erfolgt immer nach dem Prinzip der restriktiven Rechtevergabe
Protokollierung der Systemnutzung	(+) Protokollierung der Systemnutzung erfolgt über LOG-Dateien der entsprechenden Systeme
Zugriff auf Daten nur über Zugriffsberechtigungen	(+) Der Zugriff auf Daten erfolgt über eine Benutzerkennung und ein entsprechend sicheres Kennwort sowie den entsprechend zugewiesenen Zugriffsberechtigungen (Rollen)
Berechtigungen nur nach Genehmigung durch Vorgesetzte	(+) Die Zugriffsberechtigungen (Rollen) werden über einen elektronischen Workflow beantragt und genehmigt
Regelungen zum Entzug von Zugriffsberechtigungen	(+) Der Entzug von Zugriffsberechtigungen (Rollen) erfolgt über einen elektronischen Workflow
Berechtigungsvergabe nur durch autorisierte Personen	(+) Berechtigungsvergaben erfolgen nur anhand eines elektronischen Workflows durch autorisierte Personen
Kontrolle der Berechtigungen	(+) Eine Kontrolle der Berechtigungsvergaben erfolgt regelmäßig
Besondere Berechtigungen	(+) Besondere Zugriffsberechtigungen werden nur im Ausnahmefall durch einen speziell ermächtigten Vorgesetzten vergeben.
Verpflichtungserklärungen für Administratoren	(+) Die Mitarbeiter werden bei Einstellung auf die Einhaltung des Datengeheimnisses, des Datenschutzes, und des Fernmeldegeheimnisses verpflichtet und soweit notwendig auf das Sozialgeheimnis. Eine Sensibilisierung erfolgt bei Einstellung bzw. regelmäßig

Schulungen der Administratoren	(+) Administratoren werden regelmäßig im Umgang mit Informationssicherheit speziell geschult
Kontrollierte Vernichtung von Daten und Ausdrucken	(+) Die kontrollierte Vernichtung von Daten und Ausdrucken erfolgt durch spezialisierte, zertifizierte Dienstleister

1.4 Trennungskontrolle

Trennung der Datenbestände, die zu unterschiedlichen Zwecken verarbeitet werden

Anforderung	Status
Zweckbindung der Systeme	(+) Die Systeme werden gemäß der Unternehmensdatenschutzrichtlinie nach einem strengen Rechtekonzept verwaltet.
Rechtekonzept nach Datenzweck	(+) Das Rechtekonzept wird streng auf die Datentrennung abgestellt.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS.-GVO; Art. 25 Abs. 1 DS-GVO)

Sofern für Daten eine Pseudonymisierung vorgesehen ist, erfolgt die Verarbeitung personenbezogener Daten in der Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und mit entsprechenden technischen- und organisatorischen Maßnahmen unterlegt.

Folgende; Pseudonymisierungsverfahren werden eingesetzt:

- Anonymisierte Kennungen, welche nur mit Hilfe einer separaten Datenbank auflösbar sind.

1.6 Maßnahmen zur Verschlüsselung der Daten

Ziel der Maßnahmen zur Verschlüsselung von personenbezogenen Daten ist, die Inhalte von Datenbanken vor unerlaubter Einsicht und Veränderung zu schützen.

Sämtliche persönliche Daten als auch sonstige vertrauliche Informationen werden grundsätzlich verschlüsselt übertragen. Hierfür wird entweder ein sicheres HTTPS-Portal verwendet oder es werden passwortgeschützte Zip-Dateien elektronisch versendet.

Eine Mailverschlüsselung ist auf Gegenseitigkeit möglich.

Es werden folgende Verschlüsselungstechniken eingesetzt:

- Bei E-Mailverkehr TLS-Verschlüsselung

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

2.1 Weitergabekontrolle

Es wird dafür Sorge getragen, dass unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindert wird.

Anforderung	Status
Organisatorische Festlegungen zur Aufbewahrung von Datenträgern	(+) Unternehmensinternes Regelwerk, für den Umgang mit Datenträgern
Geschützte Räume zur Datenaufbewahrung	(+) Die Lagerung der Datensicherungen erfolgt entweder in einem geschützten Raum (z.B. Datenschutzraum, Rechenzentrum) extern durch einen entsprechenden Dienstleister
Datenschutzgerechte Datenträgerentsorgung	(+) Die physikalische Vernichtung von Datenträgern erfolgt gemäß DIN 66399 min. in Sicherheitsstufe 3)
Identifizierung und Authentifizierung der Beteiligten	(+) Identifizierung und Authentifizierung der Beteiligten erfolgt durch Benutzerkennung, Rufnummern, Identifikation, Passwort Benutzerkennung
Verschlüsselung von E-Mails	(+) Die Übermittlung hochsensibler Daten erfolgt nur verschlüsselt

2.2 Eingabekontrolle

Dokumentation, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (Protokollierung, Dokumentenmanagement)

Nachweis der Dateneingabe oder – veränderung

Anforderung	Status
Zugangsregelungen	(+) Es bestehen Zugangsregelungen und Benutzerberechtigungen, wodurch die Identifizierung aller Benutzer und Datenstationen im System möglich ist

Protokollierung der Einrichtung und des Betriebes des IT-Systems	(+) Dokumentation aller berechtigten Nutzer mit Rechteprofil (+) Dokumentation für die eingerichteten Nutzungsrechte
Systemprotokolle	(+) Die Tätigkeit der Benutzer wird in Systemprotokollen protokolliert. Die Eingabekontrolle in Datenbanksystemen erfolgt im Rahmen der mit den gelieferten Datenbanksystemen gelieferten Standardverfahren, die je nach Datenbanksystem bis zur Erfassung alle Eingaben umfassen kann. Soweit in den Softwaresystemen Buchungsjournale möglich sind, werden diese befüllt
Aufbewahrung von Systemprotokollen	(+) Systemprotokolle werden im Rahmen der gesetzlichen bzw. vertraglichen Vorgaben aufbewahrt.
Logging-Funktionen	(+) Die Tätigkeiten der Benutzer sind über umfangreiche Logging-Funktionen nachvollziehbar
Änderungsprotokollierung	(+) Auf den Servern bzw. in den Programmen werden Änderungen protokolliert
Datenbanken	(+) Die Eingabekontrolle in Datenbanksystemen erfolgt im Rahmen der mit den Datenbanksystemen gelieferten Standardverfahren, die je nach Datenbanksystem bis zur Erfassung aller Eingaben umfassen kann
Tabellenprotokollierung	(+) sofern Softwarertechnische Tabellenprotokollierung und Audit-Informationssystem vorliegen, kann über diese Funktionen eine entsprechende Kontrolle erfolgen

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten.

Anforderung	Status
Regelmäßige Datensicherungen	(+) Die Sicherung der Daten erfolgt in Backup-Systemen und kann durch redundante Systeme erweitert werden. So kann für etwaige Katastrophenszenarien eine kurze Wiederherstellzeit bzw. hohe Gesamtverfügbarkeit gewährleistet werden
Spiegeln von Festplatten, z.B. RAID-Verfahren	(+) Eine Spiegelung der Daten findet regelmäßig statt (RAID Systeme, Spiegelung auf räumlich getrennte Systeme)

Unterbrechungsfreie Stromversorgung (USV)	(+) Die Rechenzentren sind durch getrennte USV Anlagen mit Batteriepufferung gegen Stromausfälle gesichert
Getrennte Aufbewahrung	(+) Eine Spiegelung der Daten findet regelmäßig statt (Spiegelung auf räumlich getrennte Systeme). Getrennte Aufbewahrung von Daten erfolgt
Virenschutz/Firewall	(+) Auf allen Systemen Virenscanner und Firewallsysteme.
Backupsystem	(+) Systembezeichnung: TG2
Notfallplan	(+) Das Unternehmen verfügt über einen Notfallplan und entsprechende Handbücher zur Aufrechterhaltung der Kernprozesse im K-Fall. Erstellung und Pflege eines kundenspezifischen K-Fall Handbuchs erfolgt regelmäßig

3.2 Rasche Wiederherstellbarkeit

Es existieren Notfallpläne/Krisenpläne/Desaster Recovery für die Rechenzentren. Diese sind in dem Backup- bzw. Notfallkonzept dokumentiert. Die Funktionsfähigkeit dieses Konzeptes wird in regelmäßigen Abständen geprüft. Die Notfallpläne werden einem regelmäßigen Prüf- und Verbesserungsprozess unterzogen.

4. Organisationskontrolle

4.1. Organisationskontrolle

Organisatorische Maßnahmen zur Sicherstellung der Verarbeitung personenbezogener/ sensibler Daten

Anforderung	Status
IT-Sicherheitskonzeption	(+) Eine Informationssicherheitsleitlinie ist in der aktuellen Version vorhanden und kann vor Ort eingesehen werden
Kennwortrichtlinie	(+) Die Kennwortrichtlinie ist in der aktuellen Version vorhanden und kann vor Ort eingesehen werden
Datenschutzrichtline	(+) Eine Datenschutzrichtlinie ist vorhanden und kann vor Ort eingesehen werden.
Datenschutzbeauftragter	(+) Ein externer Datenschutzbeauftragter ist gestellt

Verpflichtung der Mitarbeiter nach Art. 29 +32 DS-GVO	(+) Alle Mitarbeiter sind auf das Datengeheimnis und die Einhaltung von Betriebs- und Geschäftsgeheimnissen verpflichtet und sind gemäß DS-GVO, Artikel 29 und 32 (4) angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten
Verpflichtung der Mitarbeiter auf § 88 TKG	(+) Desweiteren wurden sie auf das Telekommunikationsgesetz § 88 verpflichtet
Subunternehmer	(+) Richtlinie Subunternehmer ist vorhanden
Trainings/Schulungen	(+) In jährlich verpflichtenden Trainings müssen alle Mitarbeiter den führenden Mitarbeitern ihr Datenschutzbewusstsein nachweisen. Sie achten auf die verbindliche Umsetzung der Datenschutz- und Informationssicherheitsvorgaben, die im unternehmensweiten Intranet verpflichtet werden.

4.2 Security- und Risikomanagement

Leistungen werden auf der Grundlage eines Informationssicherheitsmanagements abgewickelt. Dieses beinhaltet unter anderem schriftlich dokumentierte Richtlinien, Prozesse und Handbücher zum IT-/ Rechenzentrumsbetrieb. Sie bauen auf gesetzlichen Regelungen sowie auf intern bewährten Regelungen auf.

Die eingesetzten Sicherheitsverfahren werden laufend überprüft.

Es ist ein Risikomanagement implementiert, das sowohl die operativen Risiken aus Ausschreibungen, Verträgen und in Projekten bewirkt. Darüber hinaus existiert ein IT-Sicherheitsrisikomanagement, welches sich mit den prozessualen, dienstleistungs- und standortbezogenen Risiken beschäftigt.

Die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß DS-GVO, Artikel 32, werden im Rahmen der ISO-Zertifizierung regelmäßig überprüft. Darüber hinaus finden bei internen Prozessaudits auch datenschutzrelevante Fragestellungen Berücksichtigung.

4.3 Zertifizierung

yoummday:

ISO 9001:2015 (Qualitätsmanagement)

ISO 27001:2017 (Informationssicherheitsmanagement)

Rechenzentrum:

ISO 27001:2013 (Informationssicherheitsmanagement)

4.4 Incident-Response-Management

Auftretende Security Ereignisse werden einem standardmäßigen Betriebsverfahren und toolgestützten Prozessen bearbeitet, um möglichst zeitnah einen störungsfreien Betrieb wiederzuerlangen. Sicherheitsvorfälle/Security incidents werden zeitnah überwacht und analysiert. Abhängig von der Art des Ereignisses werden an deren Bearbeitung zuständige und notwendige Mitarbeiter der Fachabteilungen und Spezialisten hinzugezogen.

4.5 Datenschutzfreundliche Voreinstellungen

Durch datenschutzfreundliche Voreinstellungen („Privacy by Design and by Default“) wird dem Datenschutz schon zu einem möglichst frühen Zeitpunkt Rechnung getragen, um eine unrechtmäßige Verarbeitung oder den Missbrauch von Daten präventiv zu verhindern. Über angemessene technische Voreinstellungen soll sichergestellt werden, dass grundsätzlich nur die personenbezogenen Daten erhoben und verarbeitet werden, die für den konkreten Zweck auch tatsächlich erforderlich sind (Need to Know-Prinzip).

Um eine möglichst risikoarme Verarbeitung personenbezogener Daten zu erreichen, werden u.a. folgende Schutzmaßnahmen umgesetzt:

- Menge der personenbezogenen Daten minimieren
- Daten so früh wie möglich pseudonymisieren oder verschlüsseln
- Transparenz in Bezug auf die Funktionen und die Verarbeitung Daten herstellen
- Daten so früh wie möglich löschen oder anonymisieren

- Zugriffsmöglichkeiten auf Daten minimieren
- Vorhandene Konfigurationsmöglichkeiten auf die datenschutzfreundlichsten Werte voreinstellen

4.6 Auftragskontrolle

Ziel der Auftragskontrolle ist, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Alle Subdienstleister werden nach definierten Kriterien ausgesucht und auf die Einhaltung der DSGVO verpflichtet. Eine Liste der Subdienstleister ist vorhanden.

Dienstleister, die als Auftragsverarbeiter im Sinne des DS-GVO tätig sind, werden nach datenschutzrechtlichen Kriterien mit größter Sorgfalt ausgewählt. Diese werden gemäß Art. 28 DS-GVO vertraglich an den Auftraggeber gebunden. Die im Rahmen der vertraglichen Bindung festgelegten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten orientieren sich an den in diesem Dokument beschriebenen Standards. Eine Liste der Auftragsverarbeiter ist vorhanden.
Die Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen. Sie sind daher bezüglich der Auftragsdatenverarbeitung sowohl in der Rolle als Auftraggeber als auch in der Rolle als Auftragnehmer mit dem Weisungsrecht des Aufraggebers vertraut. Weisungsbefugte Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt.

Es erfolgt eine Bewertung der IT-Sicherheit des Auftragnehmers vor Auftragsvergabe.

Durch eine eindeutige Vertragsgestaltung mit Abgrenzung der Rechte und Pflichten der Parteien, wird mit formalisierten Verträgen und Auftragsformularen sichergestellt. Es erfolgt eine regelmäßige Prüfung und Kontrolle der Vertragsausführungen. Weisungen werden grundsätzlich schriftlich und mit schriftlicher Bestätigung entgegengenommen.

Es erfolgt 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.

Jeglicher Aktivität liegt ein Auftrag eines Kunden zugrunde. Im Minimum gilt ein bestehendes Vertragswerk. Standard Changes werden, sofern personenbezogene Daten verarbeitet werden, ausschließlich von autorisierten Personen des Kunden entgegengenommen.