

# **DATENSCHUTZERKLÄRUNG**

Stand 29. Oktober 2017

Die Soul4Business.Cloud LTD Österreich („Soul4Business“) legt größten Wert darauf, die ihr anvertrauten Daten („Kundendaten“) nur nach den größten Sorgfaltsmaßstäben und sogar über die gesetzlichen Pflichten hinausgehend zu verarbeiten. Soul4Business verarbeitet die ihr anvertrauten Daten daher ausschließlich entsprechend den nachgenannten Grundsätzen um größtmögliche faktische wie auch rechtliche Sicherheit zu gewährleisten.

## **I. SOUL4BUSINESS ALS DIENSTLEISTER**

Soul4Business verarbeitet Daten im Rahmen der Erbringung der angebotenen Dienstleistungen je nach abgeschlossenem Produkt und Service Level Agreement (SLA) ausschließlich im Auftrag und auf (schriftliche) Weisung des Kunden (abgesehen von Punkt II.). Soul4Business wird Kundendaten (abgesehen von Punkt II.) weder zu eigenen noch zu anderen Zwecken als den vom Kunden vorgegebenen verarbeiten. Ohne die Zustimmung des Kunden wird Soul4Business Kundendaten in keinem Fall an Dritte übermitteln. Der Kunde ist daher verantwortlich für die Datenverarbeitung und bleibt in jedem Fall „Herr über seine Daten“, Soul4Business ist in diesem Zusammenhang Dienstleister.

Die gegenseitigen gesetzlichen und vertraglichen Rechte und Pflichten zwischen Soul4Business und dem Kunden hinsichtlich der Auftragsverarbeitung werden in einem gesonderten Zusatz zum Hauptvertrag, dem SLA, den diesen zugrundeliegenden AGB von Soul4Business bzw. dem Dienstleistervertrag geregelt.

### **1. Verarbeitung in Europa**

Soul4Business setzt als Backend Server (Server auf denen der Content bzw. die Daten der Kunden physisch gehostet werden) nur eigene Server ein, die ausschließ-

lich in Österreich situiert sind. Als Edge-Server (Server die zur Auslieferung des Contents bzw. der Daten der Kunden dienen) kommen zum Teil gemietete Virtual Private Server (VPS) zur Anwendung. Auf allen Servern sind Content bzw. gehostete Daten der Kunden ausschließlich in verschlüsselter Form gespeichert und können selbst von Soul4Business nicht direkt ausgelesen werden. Die Edge-Server sind ausschließlich innerhalb des Europäischen Wirtschaftsraumes (EWR) situiert. Dies stellt die Geltung des strengen europäischen Datenschutzrechtes sicher. Soul4Business wird seine Kunden informieren, wenn weitere Serverstandorte hinzukommen oder bestehende geändert werden. Sofern anwendbar, wird Soul4Business auch über allfällige Widerspruchsrechte hinsichtlich der Verarbeitung an anderen Orten informieren.

## **2. Soul4Business und Datenverarbeitung im Rahmen ihrer Produkte**

Bei sämtlichen Produkten von Soul4Business erfolgt die Verarbeitung der Daten auf den Servern von Soul4Business verschlüsselt, sodass selbst Soul4Business keine Möglichkeit hat, vom Inhalt der Daten Kenntnis zu erlangen.

Soul4Business setzt selbstverständlich nur technische Lösungen ein, sowohl hardware- als auch softwareseitig, die dem aktuellen Stand der Technik entsprechen. Um eine größtmögliche Sicherheit zu garantieren, wird Soul4Business diese Lösungen an die laufenden Entwicklungen anpassen. Die konkret beschriebenen Lösungen (Verschlüsselungstechniken, physische Sicherheitsmaßnahmen, etc.) können sich daher im Laufe der Zeit zwar ändern, werden jedoch den in dieser Datenschutzerklärung beschriebenen Sicherheitsstandard insgesamt nicht verringern.

Der Zugang zu den Serverdiensten von Soul4Business erfolgt derzeit ausschließlich über TLS v1.1, v1.2 oder SSH Protokoll 2 verschlüsselte Verbindungen. Dies bezieht sich gleichermaßen auf Verbindungen via Webbrowser (Zugang zum Customer-Care Bereich mit der Möglichkeit zum Up- bzw. Download von Daten durch den Kunden, bzw. der Möglichkeit des Kunden, Einstellungsänderungen an seinen, von Soul4Business zur Verfügung gestellten Produkten vorzunehmen) als auch auf Verbindungen die durch das sFTP Protokoll (Sicherer Dateitransfer via SSH Protokoll 2) hergestellt werden.

Serverseitig sind alle Dateisysteme bzw. Partitionen vollverschlüsselt. Als Cipher (Algorithmus) kommt derzeit AES mit einem 512 Bit langen Schlüssel zur Anwendung, als Hashfunktion kommt derzeit sha512 zum Einsatz.

- **Content Delivery Network**

Mittels CDN Caching wird die Auslieferung Ihrer Webseiten, Anwendungen, Video-dateien und anderer Webinhalte beschleunigt. Soul4Business stellt diese Technologie und den Speicherplatz zur Verfügung ohne selbst Einfluss auf oder Kenntnis von Inhalte(n) zu haben.

Nach dem Upload der Daten bzw. des Contents durch den Kunden auf den zentralen Upload Server von Soul4Business (ebenfalls Backend Server in Österreich), wird der Content umgehend auf die von Soul4Business betriebenen Backend Server gespiegelt. Dies erfolgt vollautomatisiert und verschlüsselt. Die Backend Server von Soul4Business nehmen, durch eine Firewall gesichert, ausschließlich Verbindungen vom zentralen Upload Server (derzeit SSH Protokoll 2 Verbindung) und von den Edge Servern (derzeit Standard HTTP Verbindungen) entgegen. Ein direkter Zugriff auf die Backend Server durch den Kunden oder durch Dritte ist nicht möglich.

Die Auslieferung des Contents via Webbrowser an den anfragenden Client erfolgt ausschließlich verschlüsselt via HTTPS (derzeit Protokolle TLS v1.1 und v1.2). Des Weiteren werden durch Soul4Business im Zuge der Auslieferung des Contents alle sicherheitsrelevanten Header serverseitig gesetzt um ein Maximum an Sicherheit zu gewährleisten (derzeit Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-XSS-Protection, Referrer-Policy, X-Content-Type-Options sowie Public-Key-Pins).

Die verwendeten Cipher für die webbasierenden TLS Verbindungen wurden von uns auf maximale Sicherheit bei gleichzeitiger möglichst breiten Browserkompatibilität optimiert. Dieser Prozess unterliegt aufgrund der technischen Entwicklung ständigen Anpassungen. Die aktuell verwendeten Cipher werden auf Anfrage gerne bekanntgegeben.

## ▪ **Hosted E-Mail Security und Hosted Web Security**

Die tatsächliche Datenverarbeitung beschränkt sich auf die Durchleitung der E-Mails bzw. des Internetverkehrs. Die Überprüfung erfolgt ohne Einfluss oder Kenntnis von den Inhalten der durchgeleiteten Datenströme durch Soul4Business.

### Hosted E-Mail Security:

Beim Einlangen einer E-Mail an unserem SMTP Cluster (derzeit 14 SMTP Nodes im EWR sowie 4 Backup Systeme in Österreich bzw. dem EWR), durchläuft jede E-Mail das nachfolgend genannten Prüfverfahren und wird auf Spam, Malware, Viren etc. sowie auf unerwünschte Dateianhänge geprüft. Bei einem Spam-Score von 5.0 bis 9.5 wird die E-Mail durch Setzen eines E-Mail Headers als Spam markiert. Bei einem Spam-Score über 9.5 wird die E-Mail abgelehnt, das bedeutet, dass diese E-Mail nicht an den Kunden weitergeleitet wird. Der Absender der E-Mail erhält eine Benachrichtigung über die Ablehnung seiner E-Mail samt einer kurzen Begründung der Ablehnung. Die genannten Level können durch den Kunden im Customer Care Bereich selbst verwaltet werden.

I. Überprüfung des PTR-Eintrages (Reverse DNS Eintrag) der Domain des Absenders in sogenannten DNS Blacklists (Namen). Sollte der PTR-Eintrag des Absenders (Domain) sich in einer Blacklist befinden, wird diese umgehend von Soul4Business abgelehnt.

II. Im zweiten Schritt erfolgt die SPF- und DKIM-Prüfung. Diese Einträge sind zwar nicht zwingend erforderlich, aber üblich, darum erhöhen wir im Falle des Fehlens dieser Einträge, den Spam-Score einer E-Mail. Existieren die Einträge, so werden sie auf Korrektheit geprüft.

Bei der SPF (Sender-Frame-Policy) handelt es sich im Wesentlichen um einen DNS TXT Eintrag in den für die Absenderdomain zuständigen DNS-Servern. In diesem Eintrag wird vom Eigentümer bzw. Administrator der Absenderdomain festgelegt, welche Server (IP-Adresse oder DNS-Name) berechtigt sind, E-Mails für die Absenderdomain zu versenden. Schlägt die SPF-Prüfung fehl, bedeutet das, dass der Server (IP-Adresse oder DNS-Name), der die ankommende E-Mail versendet hat, nicht berechtigt ist E-Mails für diese Absenderdomain zu versenden. Diese E-Mails werden umgehend abgelehnt, da es sich bei derartigen Nachrichten erfahrungsgemäß um Spam handelt.

Fehlende DKIM-Einträge (DomainKeys-Identified-Mail), sogenannte Signaturen, führen ebenfalls zu einer Erhöhung des Spam-Score. Fehlerhafte DKIM-Einträge hingegen führen zu einer Ablehnung der E-Mail. Ein fehlerhafter DKIM-Eintrag bedeutet, dass die in den Kopfdaten (E-Mail Header) hinterlegte DKIM-Signatur nicht mit dem im DNS gespeicherten Public-Key der DKIM-Signatur übereinstimmt oder sich der HASH-Wert gewisser Attribute der E-Mail-Kopfdaten nachträglich, d.h. nach dem eigentlichen Versand bzw. der Signatur der E-Mail, geändert hat. Diese Attribute sind Absender-E-Mail-Adresse, Empfänger, Betreff, Datum und Nachrichtentext. Bei der Signatur wird ein HASH-Wert, eine sogenannte Checksumme der E-Mail, erstellt, die der empfangende E-Mail-Server überprüfen kann. Hat sich diese Checksumme zwischen dem Versand und dem Empfang geändert, wurde die E-Mail nachträglich manipuliert und werden derartige Nachrichten umgehend abgelehnt.

III. Hat eine eingehende E-Mail die Prüfung gemäß den Punkten I und II bestanden, folgt die Prüfung auf Viren, Trojaner, Malware, Spam und unerwünschte Dateierweiterungen (.bat, .exe, .vbs, .com, .ade, .adp, .cpl, .wsc, .html, .inf). Soul4Business verwendet zur Antivirenprüfung derzeit drei verschiedene kommerzielle Virens Scanner-Module: Kaspersky, F-Secure sowie ClamAV. Zur Spam- und Phishingprüfung wird derzeit Spamassassin eingesetzt, die weltweit führende Software in diesem Bereich.

IV. Übersteht die E-Mail auch diese Überprüfung positiv, wird sie umgehend an den Mailserver des Kunden weitergeleitet, von wo die abschließende Verteilung in die richtige Mailbox stattfindet.

#### Hosted Web Security:

Hosted Web Security verhindert Bedrohungen, bevor sie das eigene Netzwerk erreichen. Dies erhöht nicht nur die Sicherheit, sondern spart auch Rechenzeit, Arbeitszeit und Nerven.

Hosted Web Security ist ein Proxy Server (derzeit Software Squid in Kombination mit HAVP) über den sämtliche Webanfragen der Benutzer des Kunden laufen. Dabei wird der gesamte Datenstrom in Echtzeit gescannt und die Übertragung gefährlicher Inhalte wie Viren, Trojaner und gefährliche JavaScripts verhindert. Für Kunden besteht auch die frei konfigurierbare Möglichkeit, Webseiten explizit zu blocken (z.B. pornografische Inhalte) oder den Zugriff auf soziale Medien wie Facebook,

YouTube oder Instagram nur zeitgesteuert (z.B. In der Mittagspause) zu ermöglichen.

Ebenfalls besteht auf Veranlassung des Kunden die Möglichkeit, spezielle vom Kunden gewählte Anwendungen, die eine Internetverbindung benötigen, zu priorisieren um ein beständiges Maß an Bandbreite zu reservieren (QoS).

#### ▪ **Hosted E-Mail Archiving**

Das E-Mail-Archiv eröffnet die Möglichkeit, sämtliche E-Mail-Kommunikation transparent und ausschließlich für den Kunden zugänglich, sicher zu archivieren. Soul4Business stellt diese Technologie und den Speicherplatz zur Verfügung, ohne selbst Einfluss auf oder Kenntnis von Inhalte(n) zu haben.

Der Zugang zum jeweiligen E-Mail-Archiv ist auf den Kunden, bzw. auf eine Person oder einen Personenkreis beschränkt, der Soul4Business vom Kunden bekanntgegeben wird.

Für die Zugriffskontrolle wird eine Zwei-Faktor-Authentifizierung eingesetzt. Das Passwort in Klartext ist ausschließlich dem Kunden bekannt und wird in der Kundendatenbank von Soul4Business nur verschlüsselt gespeichert. Soul4Business kann daher Passwörter nicht wiederherstellen. Nach erfolgreichem Login mittels Username und Password, sendet Soul4Business automatisiert eine SMS mit einem Einmal-PIN, der nur fünf Minuten lang gültig ist, an die hinterlegte Mobilrufnummer. Sollte der PIN drei Mal in Folge falsch eingegeben werden, oder drei Mal in Folge ein PIN durch einen Login-Versuch angefordert werden, ohne dass dazwischen ein erfolgreicher Login erfolgt, wird der entsprechende Kundenzugang automatisiert gesperrt. Eine Entsperrung kann nur durch Soul4Business, nach vorangegangener Prüfung und im Auftrag des Kunden, erfolgen. Die Verfügbarkeit des Service, d.h. der Betrieb des E-Mail-Archives selbst, wird durch diese Zugangssperre nicht beeinflusst.

Der Speicherplatz auf dem das Kunden-E-Mail-Archiv physisch liegt, ist entsprechend oben genannten Kriterien vollverschlüsselt. Ausgenommen davon ist die sogenannte „Keyphrase“, die aus dem vom Kunden gewählten Passwort generiert wird. Dadurch wird gewährleistet, dass auch Soul4Business keine Möglichkeit hat,

auf das E-Mail-Archiv des Kunden zuzugreifen.

- **Cloud**

Die dedizierten Cloud-Hosting-Server nutzen die ownCloud Software, um Zugriff auf Geschäftsdateien, persönliche Dokumente, Fotos, Medien, Kontakte, Kalender und Backups von jedem Ort aus über einen Desktop Sync Client, Web Browser Login oder Smartphone / Tablet App zu ermöglichen. Soul4Business stellt diese Technologie und den Speicherplatz zur Verfügung ohne selbst Einfluss auf oder Kenntnis von Inhalte(n) zu haben.

Zusätzlich zur Festplatten- bzw. Partitionsvollverschlüsselung wie oben beschrieben, sind sämtliche Daten von Kunden in den Cloud-Services durch die Verschlüsselungsfunktion von ownCloud automatisch nochmals verschlüsselt.

Die Soul4Business Cloud Services verwenden die Zugangsdaten des Kunden als Kennwort für den einzigartigen privaten Schlüssel. Nachdem das Kennwort ausschließlich als HASH auf den Servern von Soul4Business gespeichert wird, haben weder Soul4Business noch Dritte die Möglichkeit Kundendaten auszulesen. Ausgenommen davon sind naturgemäß Daten oder Ordner, die vom Kunden für Dritte freigegeben wurden. Eine Freigabe (das Teilen) bezieht sich aber niemals auf alle Daten, sondern immer nur auf kundenseitig ausgewählte Dateien, Ordner, Kontakte und Kalender bzw. Kalendereinträge. Eine Freigabe kann ausschließlich durch den Eigentümer der Daten erfolgen. Eine Freigabe durch Soul4Business ist unmöglich.

- Sicherheitsmaßnahmen

Sämtliche Systeme (Server) von Soul4Business sind durch eine Firewall geschützt, die den Zugriff auf die von Soul4Business angebotenen Dienste regelt. Zudem unterliegen bestimmte Serverdienste, wie die Remote-Administration der Systeme (SSH) zusätzlich der Einschränkung auf bestimmte, durch Soul4Business autorisierte IP-Adressen unter Verwendung des SSH2-Public-Key-Authentifizierungsverfahren.

Kundenseitig besteht die Möglichkeit zum Upload von Daten via sFTP (Verschlüsselung durch SSH Protokoll 2) oder über die Weboberfläche des Customer Care Bereiches. (Verschlüsselung durch TLS v1.1, TLS v1.2). Zu keinem Zeitpunkt erlaubt Soul4Business Kunden, Drittanbietern oder Subunternehmern den

Remote Zugriff auf die von Soul4Business betriebenen Systeme.

- Verfügbarkeit und Belastbarkeit

Soul4Business stellt den Zugang und die Abrufbarkeit der Daten sicher. Dafür sorgt die Verteilung der Daten auf mehrere Server sowie die mehrfach redundante Internetanbindung (durch verschiedene Provider), die räumliche Trennung der redundanten Einheiten und die redundant ausgelegte Stromversorgung.

Weiters wurden Maßnahmen entsprechend dem aktuellen Stand der Technik getroffen, um einen versehentlichen Verlust der Internetverbindung oder der Daten zu verhindern sowie zum größtmöglichen Schutz vor böswilligen Handlungen (z.B. (Distributed) Denial of Service (DDos) Angriffe).

Kunden sind vor Datenverlusten aufgrund von Infrastrukturproblemen, Stromausfällen oder ähnlichem durch örtlich getrennte Back-Ups, redundante Speicherung und Back-Up-Verbindungen maximal geschützt.

Datenbackups erfolgen stündlich inkrementell sowie als Fullbackup einmal täglich. Dies bezieht sich sowohl auf die gehosteten Daten bzw. E-Mails der Kunden als auf sämtliche Datenbanken. Der Datenbankcluster ist physisch von den Backend Servern getrennt.

Sämtliche Komponenten des von Soul4Business betriebenen Netzwerkes sind zumindest zweifach redundant ausgeführt.

- Integrität

Authentifizierungsmaßnahmen wie die Zwei-Faktor-Authentifizierung sorgen für Schutz vor Veränderungen der Daten während der Verarbeitung, Speicherung oder Übermittlung.

Ein Eindringen in das System wird durch Firewalls, SSH2-Public-Keys zur Remote Administration (Schlüssellänge 4096 Bit RSA) sowie die Einschränkung auf von Soul4Business autorisierten IP-Adressen verhindert.

Sämtliche von Soul4Business betriebenen Systeme (Server) sind stets mit Festplatten-Raid-Systemen, redundanten Internet-Uplinks und einer redundanten

Stromversorgung ausgestattet. Jede von Soul4Business betriebene Komponente ist zumindest zweifach redundant ausgelegt. Ersatzteile für jede Komponente stehen ständig zur Verfügung.

- Vertraulichkeit

Daten sind während der Speicherung und der Übertragung wie oben beschrieben transportverschlüsselt.

Soul4Business garantiert, dass ausschließlich qualifizierte, autorisierte und auf den Datenschutz und zur Vertraulichkeit verpflichtete Mitarbeiter mit der Datenverarbeitung betraut sind. Mitarbeiter erhalten nur soweit Zugriff wie zur Zweckerreichung notwendig. Die Aufgabenverteilung bei der Datenverwendung ist zwischen den Organisationseinheiten und den Mitarbeitern ausdrücklich festgelegt und erfolgt jegliche Datenverarbeitung nur aufgrund gültiger Aufträge. Die Zugriffsberechtigung auf Daten und Programme ist durch Username und Passwort, SSH2-Public-Keys, digitale Zertifikate sowie IP-Adressen-Einschränkungen sichergestellt.

- Transparenz

Auf Anfrage wird Soul4Business dem Kunden eine detaillierte Dokumentation und genaue Beschreibung der getroffenen Maßnahmen zur Verfügung stellen, damit dieser seiner Nachweispflicht betreffend die Auswahl des Auftragsverarbeiters sowie seinen Kontrollpflichten nachkommen kann. Dies umfasst detaillierte Dokumentationen über die getroffenen aktiven Sicherungsmaßnahmen sowie über reaktive Maßnahmen wie Backup und Disaster Recovery Maßnahmen sowie Eskalationsszenarien.

- Datentrennung

Soul4Business stellt durch softwaretechnisch getrennte Speicherplätze, CHRoot-Umgebungen und dezidierte Datenbanken für jeden Kunden sicher, dass Daten eines Kunden nicht mit Daten anderer Kunden vermischt werden.

- Protokollierung

Sämtliche Serverdienste werden von Soul4Business rund um die Uhr überwacht und im Falle eines Ausfalls, wird umgehend eine Eskalationskette via E-Mail sowie SMS-Benachrichtigung in Gang gesetzt. Alle von Soul4Business betriebenen

Dienste speichern Logfiles. Diese werden von uns auf Unregelmäßigkeiten überwacht und entsprechend den gesetzlichen Vorgaben archiviert.

- Zutrittskontrolle und andere physische Sicherheitsmaßnahmen

Der physische Zugang zu den Serversystemen ist nur autorisiertem und speziell geschultem Personal von Soul4Business möglich. Der physische Zutritt zu den von Soul4Business betriebenen Systemen wird durch Videoüberwachungsanlagen und den Wachschutz unserer Hosting-Partner rund um die Uhr protokolliert und überwacht. Zutrittsberechtigungen werden durch einen biometrischen Fingerabdruckscanner überprüft.

### **3. Rechte Betroffener und Benachrichtigungen**

Soul4Business unterstützt den Kunden nach Kräften seinen Verpflichtungen (Auskunft, Löschung, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit) gegenüber den von der Datenverarbeitung durch den Kunden Betroffenen nachzukommen und wird dem Kunden sämtliche mögliche Unterstützung in Verfahren vor dessen Aufsichtsbehörde zukommen lassen.

Im unwahrscheinlichen Fall einer Verletzung des Schutzes seiner Daten wird Soul4Business den Kunden unverzüglich davon benachrichtigen.

### **4. Ende der Verarbeitung**

Nach Beendigung der Auftragsverarbeitung hat der Kunde die Möglichkeit seine Soul4Business überlassenen Daten in der selben einfachen und sicheren Weise zurück zu übertragen, in der er sie überlassen hat.

### **5. Subauftragsverarbeiter**

Soul4Business bedient sich Subauftragsverarbeiter für den Betrieb der Server. Für die eigenen contentrelevanten Backend Server ist das derzeit die der Rechenzentrumsbetreiber [next layer GmbH](#). Die Edge Server (VPS-Server) werden derzeit bei [WORLD4YOU Internet Services GmbH](#) (Österreich), [Host Europe GmbH](#) (Europaweit) und [1&1 Internet SE](#) (Europaweit) gemietet. Die zukünftige Heranziehung oder die Änderung bestehender Auftragsverarbeiter wird dem Kunden unter der

Möglichkeit des Widerspruchs oder der Vertragsanpassung bzw. -auflösung rechtzeitig mitgeteilt.

Soul4Business kommt seiner gesetzlichen Auswahlverpflichtung sowie seiner Kontrollpflicht durch regelmäßige Kontrollen der Subauftragsverarbeiter nach. Jedem Subauftragsverarbeiter wurden die selben Pflichten auferlegt, denen auch Soul4Business gegenüber dem Kunden unterliegt und hat dies vertraglich sichergestellt.

## **II. SOUL4BUSINESS ALS AUFTRAGGEBER**

Zum Zweck der Vertragserfüllung mit dem Kunden, entsprechend dem abgeschlossenen Produkt und Service Level Agreement (SLA), speichert und verarbeitet Soul4Business folgende Daten seiner Kunden im eigenen Namen; nämlich Name/Firma, Firmenbuchnummer, Umsatzsteuer-Identifikationsnummer (UID), Anschrift, Kontaktdaten, Ansprechpartner, Informationen zu Rechnungslegung und Bezahlung, Kopie eines amtlichen Lichtbildausweises des Zeichnungsberechtigten sowie Geburtsdatum des Zeichnungsberechtigten.

Aus Sicherheitsgründen sowie um eigenen datenschutzrechtlichen Pflichten nachzukommen (insbesondere hinsichtlich Datensicherheit und Dokumentation bzw. Protokollierung) speichert und verarbeitet Soul4Business weiters Zugriffs- und Verkehrsdaten seiner Kunden im eigenen Namen; nämlich IP-Adresse, Zugriffszeitpunkte, Upload-/Downloadzeitpunkte, Upload-/Downloadvolumen, Speicherauslastung, Geräteart (PC, Tablet, Smartphone), Standort, Betriebssystem, Refferer sowie den verwendeten Browser.

Soul4Business übermittelt diese Daten, außer sofern gesetzlich dazu verpflichtet oder zur Vertragserfüllung notwendig, keinesfalls an Dritte oder verarbeitet diese Daten zu anderen Zwecken als den oben genannten (wie z.B. zu Werbezwecken).

## **III. NUTZUNG DER WEBSITE**

Der allgemeine Webauftritt von Soul4Business verwendet Cookies zur Speicherung der Spracheinstellungen. Das Soul4Business Customer Care Center (Kundenzugang) verwendet Cookies zur Authentifizierung und Protokollierung unrechtmäßiger

Vorgänge; so dienen diese Cookies der zusätzlichen Identifizierung und der Vorbeugung unrechtmäßiger Anmeldungen oder Änderung der Zugangsdaten. In jedem Fall werden nur eigene 1st Party Cookies eingesetzt und die Daten nicht für andere Zwecke eingesetzt oder an Dritte weitergegeben.

#### **IV. ALLGEMEINES**

Soul4Business wird die gemäß Punkt II. verarbeiteten Daten nur so lange speichern, wie für die Erfüllung des Vertragszweckes notwendig oder wenn gesetzlich bestimmte längere Aufbewahrungsfristen bestehen.

Kunden haben das Recht auf Auskunft der über Sie verarbeiteten Daten sowie im berechtigten Fall das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie ein Widerspruchsrecht. Zuständige Aufsichtsbehörde, insbesondere zur Ausübung des Beschwerderechts, ist die Österreichische Datenschutzbehörde.

Soul4Business wird derzeit nach ISO27001 und ISO27018 zertifiziert. Mit dem Abschluss der Zertifizierung ist in Kürze zu rechnen.