1. Präambel

In diesem Dokument beschreiben wir die wesentlichen technischen und organisatorischen Sicherheitsmaßnahmen, die wir zum Datenschutz ergreifen. Dieses Dokument ist für alle, die für Ausführung und Kontrolle gem. Art. 32 Abs. 1 lit. b DS-GVO und Art. 25 Abs. 1 DS-GVO seitens des Auftraggebers bestimmt wurden.

2. Begriffsdefinitionen

APP
Hierunter verstehen wird die als SaaS bereitgestellte Applikation.

CLOUD
Hierunter verstehen wir die systemtechnische Umgebung für die **APP**. Diese besteht aus einem bei **STRATO** gehosteten virtuellem Server. Technische und organisatorische Maßnahmen von **STRATO** zum Datenschutz sind detailliert in Punkt 3. Beschrieben.

KD Kabel Deutschland

AN Der Auftragnehmer

AG Der Auftraggeber

RAS
Remote Access Raum. Lokaler Administrationsraum beim AN, Zutritt schlüssel- und codegesichert. Zugang nur für zutrittsberechtigte Mitarbeiter. Videoüberwachung aktiv.

SAFE
Datentresor beim AN. Brand-Wasserschutz gem. EN 1047-1 S90. Schlüssel- und Codegesichert.

SADMIN
Administrator Software Solutions Simple

SPK
Schließfach Sparkasse. Zugriff durch namentlich benannte Personen in Zugriffsliste der Sparkasse sowie Schlüssel.

STRATO
PaaS Anbieter (Bereitstellung der Serverplattform)

3. Platform as a Service Anbieter

Der AG hat seine Zustimmung erteilt, dass der AN folgenden Unterauftragnehmer beauftragt.

Name/Firma/ Postadresse/ Land:	STRATO AG Pascalstraße 10 10587 Berlin
In Anspruch genommene Leistungen:	Der **AN** nimmt von **STRATO** Infrastruktur- und Plattformdienstleistungen in Anspruch, z. B. Rechenkapazität und Speicherplatz, um dem **AG** die Nutzung der **APP** als „Software as a Service"-Leistung zur Verfügung stellen zu können. Der **AN** nimmt unter anderem die folgenden Dienste von **STRATO** in Anspruch: Virtual Server Windows, Managed Backup, SSL-Zertifikat.
Vertragliche Grundlagen/ Weitere Informationen:	Die Nutzung der Strato-Dienste erfolgt durch den **AN** im Rahmen der allgemeinen Nutzungsbedingungen und Sicherheitsmaßnahmen von STRATO (abrufbar unter https://www.strato.de/sicherheit/)
Auftragsverarbeitungsvertrag:	Der **AN** hat mit **STRATO** am 09.05.2018 einen Vertrag nach Art. 28 Abs. 3 DSGVO abgeschlossen.
Ort der Server:	Die bei **STRATO** gespeicherten Auftragsdaten werden ausschließlich auf Servern in Deutschland gespeichert.

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

4.1. Zutrittskontrolle

Ein systemtechnischer Zugriff auf die **CLOUD** ist nur durch den **AN** im **RAS** möglich.
Der Zugriff kann nur von einer festen IP erfolgen, die von **KD** vergeben wurde.
Die Implementation erfolgt softwaretechnisch über entsprechende Firewall Regeln.
Der Zugriff erfolgt ausschließlich über Protokolle mit Verschlüsselung (secure rdp, secure ftp)

4.2. Zugangskontrolle

Sämtliche DV-Anlagen, die zur Auftragserfüllung notwendig sind, sind passwortgeschützt. Die Systeme werden per Firewall sowie Benutzername und Passwort vor unberechtigten Zugriffen geschützt. Arbeitsplätze/Notebooks, die zur Systempflege und Systembetreuung eingesetzt werden haben benutzereigene Konten

Das Sicherheitsniveau der Passwörter ist durch eine interne Richtlinie geregelt. Der **AG** hat keinen systemtechnischen Zugang zur **CLOUD**, sondern nur gemäß den Vereinbarungen Zugriff auf die **APP**.

Der **AN** hat der **APP** eine eindeutige Domäne zugewiesen. Nur innerhalb dieser Domäne registrierte Personen können auf die **APP** zugreifen.

Die **APP** hat systemtechnisch folgende Zugriffsberechtigungen

SADMIN	Manager, volle Berechtigungen Benannte Person auf Seiten **AN**
ADMIN	Editor, Registrierung neuer Benutzer, Lesen/Ändern aller Dokumente Gruppe
HR	Editor, Lesen/Ändern/Löschen aller Dokumente Gruppe, durch ADMIN erweiterbar
FIBU	Editor, Lesen/Ändern/Löschen aller Dokumente Gruppe, durch ADMIN erweiterbar
ALL	Autor, Lesen/Ändern/Löschen eigener Dokumente Gruppe, durch ADMIN erweiterbar

Die systemtechnischen Zugriffsberechtigungen werden softwareseitig durch die **APP** eingeschränkt, z.B. ist die Änderung von Dokumenten nur in einem bestimmten Status möglich und wird entsprechend protokolliert. Dasselbe gilt für die Löschung von Daten, diese werden grundsätzlich vor dem Löschen in einen Systempapierkorb übertragen.

Ein direkter Zugriff auf die Rechteverwaltung der **APP** ist nur seitens des **AN** möglich.

Die Zuteilung der Gruppe **ADMIN** ist nur seitens des **AN** möglich, der **AG** erteilt hierzu dem **AN** einen entsprechenden Aufnahmeantrag. Die Gruppen **HR** und **FIBU** können von allen Mitgliedern der Gruppe **ADMIN** modifiziert werden.

Wenn eine neue Person an der **APP** teilnehmen soll, kann ein Mitglied der Gruppe **ADMIN** dieser eine Einladung senden. Die Einladungsgültigkeit beträgt werksseitig 24h und kann durch ein Mitglied der Gruppe **ADMIN** verkürzt oder verlängert werden.

Die Einladung enthält einen Link zur **APP** und ein Passwort welches nach der ersten Anmeldung geändert werden muss. Die Passwortqualität muss den Sicherheitsanforderungen nach ISO 27001 genügen.

Die Verbindung wird über eine gesicherte https Verschlüsselung mit einem entsprechenden gültigen Zertifikat bereitgestellt.

Nach maximal 5 vergeblichen Anmeldeversuchen wird ein Benutzerkonto gesperrt und muss manuell durch ein Mitglied der Gruppe **ADMIN** entsperrt werden.

Mit dem Ausscheiden eines Anwenders erfolgt automatisch eine Deaktivierung seines Zugangs.

4.3. Zugriffskontrolle

Die **APP** ist seitens des AG nur über SSL-gesicherte Verbindungen erreichbar.

Die **APP** ist mit einem differenzierten Zugriffskonzept ausgestattet. Es wird unterschieden in Autorisierung über Rollen, Gruppen und namentlich erfassten Personen.

Jeder für die **APP** berechtigte Anwender ist primär der Berechtigungsgruppe **ALL** zugeordnet, diese erlaubt es, die **APP** zu öffnen, Dokumente zu erstellen und selbst erstellte Dokumente zu lesen, in bestimmten Zuständen auch zu ändern. Über die Konfiguration kann der **ADMIN** Löschrechte erteilen. Weitergehende Rechte sind für Standardanwender nicht gegeben.

Ausnahmen gelten für Personalvorgesetzte, Stellvertreter und Stabsstellen. Diese werden vom **AG** in einer separaten Organisationsdatenbank erfasst und erhalten Leserechte auf alle Ihnen zugeordnete Personen.

Für die Gruppen **HR** und **FIBU** gelten ebenfalls Sonderregelungen. Diese haben erweiterte Rechte an Dokumenten und sind für spezielle Aufgaben wie z.B. die Personalabwicklung (Kontingentierung, Resturlaub, Jahresübertrag, etc.) zuständig. Die Zuteilung von Personen an diese Gruppe obliegt dem **AG**.

Im Rahmen des Workflows werden temporäre Autorenrechte an designierte Personen (z.B. Entscheider bei einem Urlaubsantrag) vergeben, die nach der Ausführung des Arbeitsschrittes wieder entzogen werden.

Falls in der **APP** Löschungen durchgeführt werden, überträgt die **APP** diese vor dem Entfernen in eine separate Datenbank, auf die nur der **AN** Zugriff hat. Das Löschdatum sowie der ausführende Anwender werden protokolliert. Die gelöschten Daten werden für einen durch den **AG** einstellbaren Zeitraum vorgehalten und dann protokolliert vernichtet.

Änderungen an Dokumenten in der **APP** werden über eine Verlaufshistorie gekennzeichnet, die über die gesamte Lebensdauer des Dokumentes mitgeführt wird. Die Protokollierung erfolgt für Aktionen sowie Dokumentinhaltsänderungen sowie die ändernde Person.

4.4. Trennungskontrolle

Pro Mandant (=Domäne) gibt es eine virtuelle Domäne. Diese beinhaltet alle Objekte dieses Mandanten wie Personen, Registrierungen, Abwesenheiten, etc.)

Die **APP** wird in einer eigenen virtuellen Domäne in der **CLOUD** betrieben. Der Zugriff auf die **APP** erfolgt immer personenbezogen durch Eingabe eines Benutzernamens.

Dieser Benutzername wird bei Registrierung automatisch mit dem eindeutigen Domänennamen verknüpft, welcher dem **AG** durch den **AN** bei Auftragserteilung zugeordnet wurde.

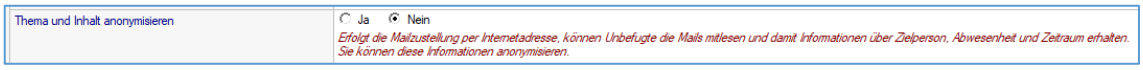
Pro **APP** ist maximal eine Domäne möglich, ein domänenübergreifender Zugriff ist nicht möglich.

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

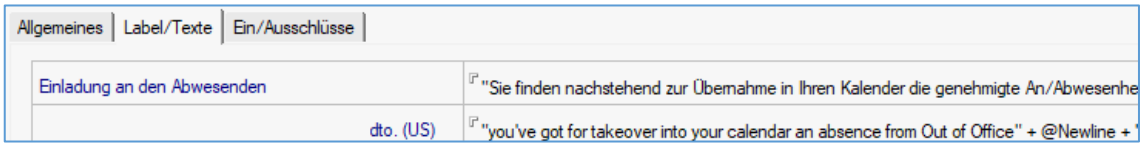
5.1. Weitergabekontrolle

Die APP versendet im Rahmen des Prozesses Mails, die Hinweise auf zu erledigende Aufgaben beinhalten. Dieser Mailversand erfolgt unverschlüsselt und beinhaltet in der Regel keine relevanten personenbezogenen Inhalte.

Der **AG** kann diesen Mailversand vollständig anonymisieren.



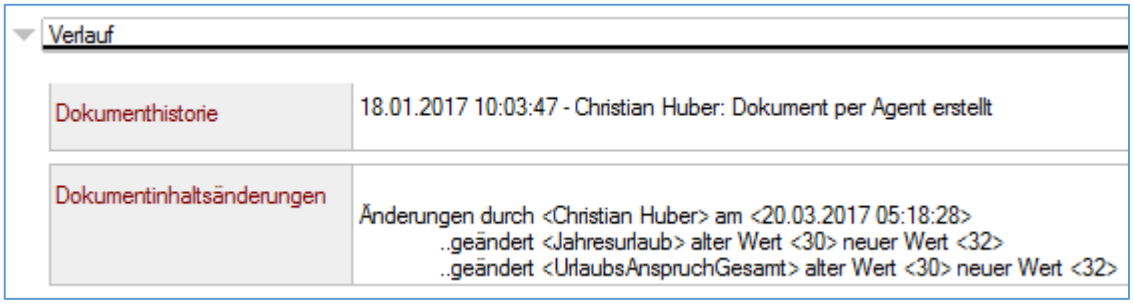
Die **APP** kann im Rahmen der Kalendersynchronisation zu Drittanbietern (z.B. Outlook, Lotus Notes) Einladungen mit Zeit- und Abwesenheitsinformationen versenden. Der Versand erfolgt unverschlüsselt. Der **AG** kann die Synchronisation ein/ausschalten und Texte vollständig anonymisieren.



Der AN implementiert im Rahmen der Bereitstellung der APP zur Datensicherung eine lokale Replik der APP im RAS, die Daten werden über eine 256-Bit verschlüsselte Leitung transportiert und beim AN in einem fest installiertem Tresor der Widerstandsklasse S90 aufbewahrt. Die lokale Speicherung erfolgt verschlüsselt, eine Entschlüsselung kann nur durch den **SADMIN** erfolgen.

5.2. Eingabekontrolle

Änderungen an Dokumenten in der APP werden über eine Verlaufshistorie gekennzeichnet, die über die gesamte Lebensdauer des Dokumentes mitgeführt wird. Die Protokollierung erfolgt für Aktionen sowie Dokumentinhaltsänderungen sowie die ändernde Person.



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

6.1. Verfügbarkeitskontrolle

Der **AN** verwaltet vor Ort nur Clientsysteme, die Verfügbarkeit der Serversysteme ist in der separat mit **STRATO** abgeschlossenen Vereinbarung zur Auftragsdatenverarbeitung zu entnehmen.

Der **AN** unterscheidet hier zwischen der Verfügbarkeit der Daten (z.B. versehentliches Löschen von einzelnen Dokumenten) sowie der Verfügbarkeit der **APP** (z.B. Nichtablaufen auf Grund eines Betriebssystemfehlers).

Die **CLOUD** wird vor jedem Update im Vollmodus gesichert. Jede 2.te Sicherung wird überschrieben. Es erfolgt keine Sicherung von Daten der **APP**, diese ist separat geregelt (s.u.).

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

Eine systemtechnische Wiederherstellung wird nach Meldung durch den **AG** innerhalb 24h an Werktagen durchgeführt.

Bezogen auf die **APP** unterscheidet der **AN** hier 3 Varianten

Standard
Die **APP** wird einmal täglich in den **RAS** repliziert (verschlüsselte Datenübertragung, verschlüsselte lokale Speicherung beim **AN**). Für einen Zeitraum von 30 Tagen erfolgt eine Aufbewahrung im **SAFE**, danach werden die Daten automatisch überschrieben.

Pro
Datenreplikation analog Standard. Zusätzlich Speicherung von Monats- und Jahressicherungen. Offline Lagerung einer verschlüsselten Kopie in der **SPK**.

Premium
Analog Pro. Zusätzlich Bereitstellung eines Clusterservers, auf den die Daten in Echtzeit repliziert werden. Wiederanlaufzeit bei vollständigem Ausfall der **APP** innerhalb 2h nach Meldung an Werktagen zwischen 09:00 und 16:00.

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

7.1. Datenschutzfreundliche Voreinstellungen

Gemäß dem Stand der Technik werden Datenschutzmaßnahmen bereits bei konzeptioneller Entwicklung von Produkten sowie Projekten und Verfahren gem. den Vorgaben des Art.25 DSGVO Abs. 2 durchgeführt.

7.2. Incident-Response-Management

Bei Verletzungen des Schutzes personenbezogener Daten ist eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion sichergestellt (Prüfung, Dokumentation, Meldung). Formulare, Anleitung und eingerichtete Umsetzungsverfahren mit benannten zuständigen Personen.

7.3. Auftragskontrolle

Die Verarbeitung von personenbezogenen Daten erfolgt nur durch die **APP** gemäß den Vorgaben seitens des **AG**. Falls weitergehende Verarbeitung durch den **AN** gewünscht ist (z.B. Auswertungen) ist dies explizit durch den **AG** schriftlich zu beauftragen.

Die Mitarbeiter des **AN** sind auf das Datengeheimnis / Verschwiegenheit / Vertraulichkeit verpflichtet.

Alle Mitarbeiter des **AG** sind mit dem Datenverarbeitungszweck vertraut, auf Vertraulichkeit und Verschwiegenheit gem. Art. 28 Abs. 3 lit. b DSGVO verpflichtet, auf mögliche Haftungsfolgen hingewiesen und über die datenschutzrechtlichen Anforderungen belehrt sowie diesbezüglich instruiert sowie auf deren Einhaltung überwacht.

Ein IT-Sicherheitskonzept ist sowohl beim **AN** wie auch beim **AG** vorhanden und wird regelmäßig an geänderte Umgebungsparameter angepasst.

Unterauftragsverhältnisse werden schriftlich beauftragt.