VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG („AVV“) GEMÄß ART. 28 EU-DSGVO

1. Gegenstand und Dauer der AVV

1.1 Der Gegenstand dieser AVV (nachstehend auch „Vereinbarung") ergibt sich aus dem Vertrag über die Erbringung von SaaS-Service und Consulting Services zwischen dem Kunden und BELLIN auf den hier verwiesen wird („Vertrag").

1.2 Diese AVV gilt während der Dauer des Vertrages zwischen den Parteien. Unabhängig von der vorstehenden Regelung der Vertragslaufzeit gelten die Verpflichtungen zum Datengeheimnis, die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Ende des Vertrages hinaus.

2. Konkretisierung der AVV

2.1 Die Verarbeitung personenbezogener Daten durch BELLIN für den Kunden als Teil der vertragsgegenständlichen Leistungen (nachstehend auch als „Dienstleistungen") sind in Umfang, Art und Zweck auf diejenigen personenbezogenen Daten beschränkt, die vom Kunden oder im Auftrag des Kunden bei der Nutzung der Dienstleistungen einzig zur vollständigen Bereitstellung der Dienstleistungen gemäß dem Vertrag eingegeben wurden.

2.2 Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, im EFTA-Land Schweiz oder in Kanada statt. Jede Verlagerung in ein davon abweichendes Drittland bedarf der vorherigen Zustimmung des Kunden und muss den Anforderungen gemäß Art. 44 ff. EU-DSGVO entsprechen. Für die Schweiz und für Kanada ist ein angemessenes Schutzniveau durch einen Angemessenheitsbeschluss der Kommission in Art. 45 Abs. 3 EU-DSGVO festgestellt. Für das Vereinigte Königreich wird im Fall eines Austritts aus der Europäischen Union eine Vereinbarung auf Basis der EU Standardvertragsklauseln zwischen BELLIN und betroffenen Unterauftragnehmern in Kraft gesetzt, solange es keinen Angemessenheitsbeschluss der EU betreffend des Datenschutzniveaus im Vereinigten Königreich gibt.

2.3 Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen nach Ziff.6 dieser Vereinbarung.

2.4 Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien:

a) Namen und berufliche Kontaktdaten der User (insbesondere Kontobevollmächtigte);
b) Namen und Kontonummern von Kreditoren und Debitoren (insbesondere Kunden und Lieferanten):
c) Namen und Kontonummern von Mitarbeitern.

3. Technisch-organisatorische Maßnahmen (TOM)

3.1 BELLIN hat die Umsetzung der im Vorfeld der Auftragsvergabe und als Anlage zu dieser Vereinbarung dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung sicherzustellen und dem Kunden die Möglichkeit zur Prüfung auf dessen Kosten und nach ausreichend zeitlicher Vorankündigung einzuräumen. Bei Akzeptanz der TOM durch den Kunden werden diese Maßnahmen durch den Kunden, bei der Umsetzung der Arbeiten, als Grundlage des Auftrags vorausgesetzt. Soweit eine Prüfung des Kunden einen Anpassungsbedarf ergibt, kann dieser vom Kunden beauftragt werden.

3.2 Zusammen handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Trennungskontrolle
e) Pseudonymisierung
f) Weitergabekontrolle
g) Eingabekontrolle
h) Verfügbarkeitskontrolle
i) Auftragskontrolle im Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Soweit sie sich nicht aus dem Vertrag ergeben, sind diese gesondert in der Anlage „Allgemeine technische und organisatorische Sicherheitsmaßnahmen gemäß Art. 28 EU-DSGVO“ (kurz TOM) beschrieben.

3.3 BELLIN hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen Einzelheiten siehe Anlage „Allgemeine technische und organisatorische Sicherheitsmaßnahmen (TOM)“. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es BELLIN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

4. Berichtigung, Einschränkung und Löschung von Daten

BELLIN darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken, sofern nicht gesetzlich eine Verpflichtung von BELLIN zur weiteren Speicherung der Daten des Kunden besteht. Soweit eine betroffene Person sich diesbezüglich unmittelbar an BELLIN wendet, wird BELLIN dieses Ersuchen unverzüglich an den Kunden weiterleiten. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung des Kunden unmittelbar durch BELLIN sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten von BELLIN

BELLIN hat zusätzlich zu der Einhaltung der Regelungen dieser AVV gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet BELLIN die Einhaltung folgender Vorgaben:

- Sofern BELLIN gemäß den Bestimmungen der EU-DSGVO und der betreffenden Datenschutzgesetze im Mitgliedsland der EU, in dem BELLIN ihren Sitz hat, einen Datenschutzbeauftragten zu benennen hat, die schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt. Dessen Kontaktdaten werden dem Kunden zum Zweck der direkten Kontaktaufnahme mitgeteilt. Die Kontaktdaten des benannten Datenschutzbeauftragten finden sich in der Anlage (TOM) wieder.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO. BELLIN setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. BELLIN und jede BELLIN unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO [Einzelheiten siehe Anlage „Allgemeine technische und organisatorische Sicherheitsmaßnahmen (TOM)“].
- Der Kunde und BELLIN arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei BELLIN ermittelt.
- Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei BELLIN ausgesetzt ist, hat ihn BELLIN nach besten Kräften zu unterstützen.
- BELLIN kontrolliert regelmäßig die internen Prozesse, sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich, im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Vereinbarung.
- Die BELLIN für Unterstützungsleistungen entstehenden nachzuweisenden Aufwände und Kosten wird der Kunde erstatten.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die BELLIN z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. BELLIN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Kunde stimmt der Beauftragung der nachfolgende Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO:

Firma Unterauftragnehmer	**Anschrift/Land**	**Dienstleistungen**
BELLIN Treasury Services Ltd.	Suite 1022 470 Granville Street Vancouver, BC V6C 1V5 Kanada	■ BELLIN Cloud Services (exkl. “Treasury Connected”) ■ Consulting ■ Implementierung ■ Anwendungssupport
BELLIN Treasury Alliances Ltd.	Aldwych House 71-91 Aldwych London, WC2B 4HN Großbritannien	■ Consulting ■ Implementierung
BELLIN Treasury International GmbH	Tullastr. 19 77955 Ettenheim Deutschland	■ Kundenpflege ■ Kundenstammdaten-verwaltung ■ Kundenservices (Events, Reiseplanung, Marketingaktivitäten) ■ BELLIN Cloud Services für “Treasury Connected”

6.3 Die Auslagerung auf Unterauftragnehmer bei der Verarbeitung von personenbezogenen Daten des Kunden oder der Wechsel der bestehenden Unterauftragnehmer ist unabhängig von Ziffer 6.2 bei Vorliegen sämtlicher nachfolgender Voraussetzungen zulässig, soweit:

a) BELLIN eine solche Auslagerung auf Unterauftragnehmer dem Kunden eine angemessene Zeit vorab zumindest in Textform anzeigt,

b) der Kunde nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung aus wichtigem BELLIN nachzuweisenden Grund Einspruch erhebt (soweit der Kunden nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt das Einspruchsrecht des Kunden bezüglich der entsprechenden Beauftragung).

c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

d) BELLIN die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher stellt, wenn der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR oder der

Schweiz erbringt. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 6 Satz 2 eingesetzt werden sollen.

Zusätzlich sind bei einer weiteren Auslagerung durch den Unterauftragnehmer die nachstehenden Voraussetzungen zu erfüllen:

e) BELLIN muss einer weiteren Auslagerung durch die Unterauftragnehmer mindestens in Textform ausdrücklich zustimmen, und

f) Sämtliche vertraglichen Regelungen in der Vertragskette müssen auch den weiteren Unterauftragnehmern auferlegt werden.

Die Weitergabe von personenbezogenen Daten des Kunden an den Unterauftragnehmer durch BELLIN gemäß dieser Ziffer 6.3 und das erstmalige Tätigwerden durch den Unterauftragnehmer sind erst mit Vorliegen der vorstehenden Voraussetzungen für eine Unterbeauftragung gestattet.

7. Kontrollrechte des Kunden

7.1 Der Kunde hat das Recht, im Benehmen mit BELLIN Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer nach Maßgabe der nachstehenden Regelungen durchführen zu lassen, um sich von der Einhaltung dieser Vereinbarung durch BELLIN in dessen Geschäftsbetrieb zu überzeugen. Überprüfungen sind rechtzeitig anzumelden sind,.

7.2 BELLIN stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten BELLINs nach Art. 28 EU-DSGVO überzeugen kann. BELLIN verpflichtet sich, dem Kunden auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Anlage (TOM) nachzuweisen. BELLIN ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte von BELLIN sind oder wenn BELLIN durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden von BELLIN, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten BELLIN, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten

7.3 Nach Wahl von BELLIN kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag auch durch folgende Maßnahmen erfolgen:

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4 Beauftragt der Kunde einen Dritten mit der Durchführung der Überprüfung, hat der Kunde den Dritten schriftlich eben-so zu verpflichten, wie auch Kunde aufgrund von dieser Ziffer 7 dieses Vertrags gegenüber BELLIN verpflichtet ist. Zudem hat der Kunde den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen von BELLIN hat der Kunde ihr die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Kunde darf keinen Wettbewerber von BELLIN mit der Kontrolle beauftragen.

7.5 Für die Ermöglichung von durch den Kunden durchgeführten oder beauftragten Kontrollen kann BELLIN eine angemessene Vergütung geltend machen.

8. Mitteilung bei Verstößen durch BELLIN

8.1 BELLIN unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung, sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden.

c) die Verpflichtung, den Kunden im Rahmen seiner Informationspflicht gegenüber den Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.

d) die Unterstützung des Kunden für dessen Datenschutz-Folgenabschätzung.

e) die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten BELLINs zurückzuführen sind, kann BELLIN eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Kunden

9.1 Der Kunde ist berechtigt, im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung, Empfehlungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen, die er durch direkte Hinweise konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind anschließend zumindest in Textform zu vereinbaren.

9.2 Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Kunden.

9.3 Mündliche Hinweise wird der Kunde vor einer Umsetzung zumindest per E-Mail (in Textform) bestätigen. BELLIN hat den Kunden unverzüglich zu informieren, wenn BELLIN der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. BELLIN ist berechtigt, die Durchführung der entsprechenden Vereinbarung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden bestätigt oder geändert wird.

9.4 Falls sich Verpflichtungen in dieser Vereinbarung ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende, neue Festlegung erfolgt

10. Löschung von Daten und Rückgabe von Datenträgern

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher oder behördlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher, nach Aufforderung durch den Kunden, spätestens mit Beendigung der Leistungsvereinbarung, hat BELLIN sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände,

die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden auszuhändigen oder nach vorheriger Zustimmung, datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch BELLIN entsprechend der jeweiligen Aufbewahrungsfristen über das Ende des Vertrages hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Kunden übergeben.

11. Haftung

11.1 Für die Haftung von BELLIN nach dieser Vereinbarung gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Vertrag. Soweit Dritte Ansprüche gegen BELLIN geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Kunden gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Kunde BELLIN von diesen Ansprüchen auf erstes Anfordern frei.

11.2 Der Kunde verpflichtet sich, BELLIN auch von allen etwaigen Geldbußen, die gegen BELLIN verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Kunde Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

12. Beendigung der AVV

Diese AVV endet mit der Beendigung des Vertrages zwischen dem Kunden und BELLIN.

ANLAGE
ALLGEMEINE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM) GEMÄß ART. 28 EU-SDSGVO

Diese Anlage stellt die technischen und organisatorischen Maßnahmen von BELLIN dar.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Zutrittskontrolle

  Es besteht ein allgemeines Zutrittskontrollsystem durch Ausweisleser, Überwachungseinrichtungen und kontrollierte Schlüsselvergabe.

  Für die von BELLIN genutzten Räumlichkeiten gilt: Einbruchmeldeanlage inkl. 24/7 Alarmaufschaltung auf Wachdienst

  - Magnet- und Schließkontakte an allen Außen- und segmentteilenden Innentüren, sowie für die Zugänge besonders schützenswerter Räumen wie Serverräume.
  - Schlüsselloser Zutritt mit Magnetkarten mit personenbezogenen Berechtigungen
  - Biometrische Zugangssperren
  - Manuelles Schließsystem
  - Schließsystem mit Codesperre
  - Umfassende Protokolle für die Verwendung der Zugangskarten
  - Videoüberwachung der Gebäude und der Eingänge
  - Absicherung der Gebäudeschächte
  - Türen mit Knauf Außenseite
  - Klingelanlage mit Kamera
  - Schlüsselregelung / Liste
  - Empfang /Rezeption / Pförtner
  - Besucherbuch / Protokoll der Besucher
  - Mitarbeiter- / Besucherausweise
  - Besucher in Begleitung durch Mitarbeiter
  - Sorgfalt bei der Auswahl des Wachpersonals
  - Sorgfalt bei der Auswahl Reinigungsdienste

  Für das eingesetzte Data Center gilt zusätzlich:

  Der Zutritt zu dem Data Center ist gesichert durch aktuelle Sicherheitseinrichtungen, es erfolgt eine Protokollierung der Zutritte. Die Gruppe der Zutrittsberechtigten ist limitiert. Eine allgemeine Feuer-, Einbruchs- und Wasserbruchsicherung ist eingerichtet.

  - Sicherheitsschleusen, Key Cards
  - Visuelle Kontrolle durch Rechenzentrums-Personal
  - CCTV Videoüberwachung, Sicherheitsalarm
  - 24x7x365: Personal in Gebäude, technischer Support

- Zugangskontrolle
  Das Eindringen Unbefugter in die DV-Systeme wird verhindert. Es werden starke Passwörter mit regelmäßiger Änderung und eine Anwenderverwaltung nebst Benutzeridentifikation und Authentifizierung angewendet.
  - Login mit Benutzername und Passwort
  - Login ,mit biometrischen Daten
  - Anti-Viren-Software Server
  - Anti-Viren-Software Clients
  - Firewall
  - Intrusion Detection Systeme
  - Remote Zugriffe erfolgen nur über verschlüsselte Leitungen (VPN).
  - Verschlüsselung von Datenträgern
  - Verschlüsselung von Notebooks / Tablets
  - Verwalten von Benutzerberechtigungen
  - Zentrale Passwortvergabe
  - Richtlinie "Sicheres Passwort"
  - Richtlinie "Löschen / Vernichten"
  - Richtlinie "Clean desk"
  - Allg. Richtlinie Datenschutz und / oder Sicherheit
  - Mobile Device Policy
  - Anleitung "Manuelle Desktopsperre"
  - Restriktive Zugangskontrollen zu Serverräumen
- Zugriffskontrolle
  - Vertrauliche oder streng vertrauliche Papierdokumente werden durch Verschließen gesichert und datenschutzgerecht entsorgt (Schredder).
  - Genau definierte Mitarbeiter mit Zugriffsberechtigungen auf die Server
  - Physische Löschung von Datenträgern
  - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten; Aufzeichnung von Zugriffen auf Server mit kritischen Daten mit Softwaresteuerung
  - Minimale Anzahl an Administratoren
  - Verwaltung Benutzerrechte durch Administratoren
  - Tresor
  - Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert. Es kommen bedarfsorientierte Berechtigungskonzepte zur Anwendung. Die Zugriffsrechte werden überwacht und protokolliert. Die Anwender sind für die Anwendung und zum Datenschutz geschult. Eingeschränkte und dokumentierte Zugriffskontrolle.
  - Regelmäßige Ausbildung und Pflichtschulung aller Mitarbeiter zum Umgang mit sensiblen Daten und zur Datensicherheit

- Trennungskontrolle
  Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Eine Mischung mit anderen Kundendaten ist ausgeschlossen.
  - Trennung zwischen Betrieb der Server und Entwicklung der Anwendungen
  - Organisatorische Trennung der Prozesse und eingesetzten Anwendungen nach
    - Entwicklung
    - Betrieb
    - Support
  - Physikalische Trennung (Systeme / Datenbanken / Datenträger)
  - Mandatenfähigkeit relevanter Anwendungen: Daten der Kunden werden in unterschiedlichen Datenbanken gehalten. Die Erfassung und Aufbereitung der Daten erfolgt in kundenindividuellen Anwendungen.
  - Steuerung über Berechtigungskonzept
  - Festlegung von Datenbankrechten
  - Datensätze sind mit Zweckattributen versehen
- Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO). Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass bei einer Pseudonymisierung die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können. Im Falle einer Pseudonymisierung werden die Zuordnungsdaten in getrennten und abgesicherten Systemen gesondert aufbewahrt. Es besteht eine interne Anweisung, dass personenbezogene Daten im Fall einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren sind.

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Weitergabekontrolle
  - E-Mail Verschlüsselung
  - Einsatz von VPN
  - Protokollierung der Zugriffe und Abrufe
  - Bereitstellung über verschlüsselte Verbindungen wie sftp, https
  - Weitergabe in anonymisierter oder pseudonymisierter Form
  - Die elektronische Übertragung bzw. Datentransport und Weitergabe von personenbezogenen Daten erfolgt durch moderne Verschlüsselung. Weitergabe erfolgt nur in vorher festgelegten Kanälen nach den technischen Vorgaben der Banken, an die die Daten zu übermitteln sind.
  - Die Daten werden ausschließlich im Rahmen gesetzlicher und steuerlicher Regelungen aufbewahrt
  - Ein Versand über unsichere Kanäle (z. B. per E-Mail) wird nur auf ausdrückliche Anweisung des Kunden vorgenommen.
- Eingabekontrolle
  - Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist durch Audit Trail auf der Ebene von individuellen Benutzernamen (nicht Benutzergruppen) gewährleistet. Die Erfassung der Daten erfolgt ausschließlich durch den Kunden. Die Rolle von BELLIN ist die Übermittlung.
  - Die Lesbarkeit der Daten wird durch die Anwendung gesteuert.
    Die Bearbeitung außerhalb der Anwendung ist durch den Kunden gesteuert und nur in klar definierten Ausnahmefällen möglich. Veränderungen dieser Art bedürfen der schriftlichen Beauftragung des Kunden.
  - Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöscher Serverraum
  - Serverraumüberwachung Temperatur und Feuchtigkeit
  - Serverraum klimatisiert
  - USV
  - Schutzsteckdosenleisten Serverraum
  - RAID System / Festplattenspiegelung
  - Videoüberwachung Serverraum
  - Alarmmeldung bei unberechtigtem Zutritt zu Serverraum
  - Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Ein Notfallplan ist vorhanden, einschließlich Backup Prozessen und dezentraler Datenhaltung. Es gibt definierte Verfügbarkeitszeiträume.
  - Die Server sind redundant in zwei verschiedenen Data Centern innerhalb einer Stadt vorhanden, die über eine Glasfaserstrecke als VLAN verbunden sind
  - Backups sind vereinbarungsgemäß regelmäßig vorhanden; Backup & Recovery Konzept (ausformuliert)
  - Kontrolle des Sicherungsvorgangs
  - Regelmäßige Tests zur Datenwiederherstellung und -protokollierung der Ergebnisse
  - Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
  - Keine sanitären Anschlüsse im oder oberhalb des Serverraums
  - Getrennte Partitionen für Betriebssysteme und Daten
  - Server an redundanten Standorten
  - Es wird ein aktives Monitoring über 24/7 der eingesetzten Rechner- und Speichermedien vorgenommen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

- Datenschutz-Management
  - Software Lösung im Einsatz
  - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung
  - Sicherheitszertifizierung nach ISO 27001
  - Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
  - Externer Datenschutzbeauftragter
  - Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
  - Regelmäßige Sensibilisierung der Mitarbeiter, mind. jährlich
  - Interner Informationssicherheitsbeauftragter
  - Datenschutz-Folgeabschätzung (DSFA) wird bei Bedarf durchgeführt
  - Die Organisation kommt den Informationspflichten nach Art. 13 und 14 EU-DSGVO nach
  - Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- Incident-Response-Management
  - Einsatz von Firewall und regelmäßige Aktualisierung
  - Einsatz von Spamfilter und regelmäßige Aktualisierung
  - Einsatz von Virenscanner und regelmäßige Aktualisierung
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
  - Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
  - Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
  - Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)
  - Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
  - Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen
- Auftragskontrolle
  - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Kunden
  - Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
  - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
  - Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
  - Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
  - Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
  - Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

- Regelung zum Einsatz weiterer Unterauftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Datenschutzbeauftragter

Als Datenschutzbeauftragter der BELLIN GmbH is benannt:

- Herr Sascha Kuhrau, a.s.k. Datenschutz e.K.
  - Schulstr. 16a, 91245 Simmelsdorf
  - info@ask-datenschutz.de
  - Festnetz: (0049) 9155-263 99 70