Anlage 3 zum Vertrag gemäß Art. 28 DSGVO:
Technische und organisatorische Maßnahmen nach Art. 32. DSGVO

I. Verfahren zur Vertraulichkeit – Art. 32 Abs. 1 lit. b.
Die erforderliche Vertraulichkeit im o.g. Sinn, zu den durch unser Unternehmen verantwortlich be- und verarbeiteten pb-Daten, wird gewährleistet durch:

A. Zutrittskontrolle (Gebäude /Räume) zur Verhinderung **unbefugten Zutritts** mit dem Ziel: … nicht zur pb-Datenverarbeitung befugten Personen Zutritt zu unserer DV-Infrastruktur zu verwehren.

- **Hauptverwaltung – Naumannstr. 64, 10829 Berlin**
  - Alarmgesicherte Türen und Fenster
  - Videoüberwachung
  - Alarmanlage
  - Sicherheitsschloss
- **Rechenzentrum – Nonnendammallee 15, 13599 Berlin**
  - Elektronisches Zutrittskontrollsystem (Zugang mit PIN) mit Protokollierung
  - Hochsicherheitszaun um das Rechenzentrum
  - Schranke und Tor am Eingang zum Rechenzentrum
  - Personenvereinzelungsanlage
  - 24/7 Wachschutz am Rechenzentrum
  - Videoüberwachung an den Ein- und Ausgängen, Türen, Fluren und Serverräumen
  - Richtlinien zur Begleitung von Gästen / Wartungspersonal im Gebäude
  - Unterteilung des Rechenzentrums in unterschiedliche Sicherheitszonen mit individuellen Zutrittsberechtigungen über personalisierte ID-Karte
  - Dokumentierte Schlüssel- und ID-Kartenvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für sein(e) Colocation Rack(s))
- **Rechenzentrum – Gradestrasse 64, 12347 Berlin**
  - Elektronisches Zutrittskontrollsystem (Zugang mit PIN und biometrischen Merkmalen) mit Protokollierung
  - Zaun um das Rechenzentrum
  - Richtlinie zur Begleitung von Gästen und Wartungsprotokoll im Gebäude
  - Videoüberwachung an den Ein- und Ausgängen
  - Unterteilung des Rechenzentrums in unterschiedliche Sicherheitszonen mit individuellen Zutrittsberechtigungen über personalisierte ID-Karte
  - Dokumentierte Schlüssel- und ID-Kartenvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für sein(e) Colocation Rack(s))

B. Zugangskontrolle zur DV-Infrastruktur zur Verhinderung der **unbefugten Benutzung** mit dem Ziel: … nicht zur pb-Datenverarbeitung befugten Personen die Nutzung unserer DV-Infrastruktur zu verwehren.

- **Allgemein**

  Der Auftragnehmer vermietet die DV-Infrastruktur an den Auftraggeber. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Durch den Auftragnehmer findet keine Verarbeitung von personenbezogenen Daten statt und es ist ihm auch nicht möglich dies beim

Auftraggeber zu kontrollieren. Der Auftraggeber entscheidet allein und ausschließlich darüber, welche pb-Daten in welcher Weise verarbeitetet werden.

- **Managed-Systeme und Services**

  Bei Managed-Systemen und Services erhalten nur für dieses System / Applikation berechtigte Administratoren einen Zugang. Jeder Administrator hat hierfür einen individuellen VPN-Zugang. Jeder Zugriff eines Administrator wird protokolliert. Es bestehen Regeln zum Schutz und regelmäßigen Austauschs der Zugangsdaten.

- **Unmanaged-Systeme und Services**

  Bei Unmanaged-Systeme und Services obliegt es dem Auftraggeber entsprechende Maßnahmen zu ergreifen, die dazu geeignet sind, unbefugten die Nutzung der Datenverarbeitungssysteme zu verwehren.

- **Colocation**

  Der Auftragnehmer stellt hierbei nur die Zutrittskontrolle zum Rechenzentrum, wie in Abs. A genannt sicher. Weitere Maßnahmen zur Sicherung obliegen **ausschließlich** dem Auftraggeber.

C. **Zugriffskontrolle** zur Verhinderung von **unbefugten Datenzugriff** durch DV-Systembenutzer mit dem Ziel: … zu gewährleisten, dass die berechtigten DV-Systembenutzer, durch Zugriffsrechte gesteuert, nur die für sie bestimmten pb-Daten verarbeiten können; und somit pb-Daten bei deren Be- und Verarbeitung (bei der Anwendung und nach der Speicherung) nicht durch Unbefugte gelesen, kopiert, verändert oder entfernt werden können.

- **Interne Verwaltungssysteme des Auftragsnehmers**

  Ein unberechtigter Zugriff wird durch regelmäßige Sicherheitsupdates, nach dem jeweiligen Stand der Technik durch den Auftragnehmer verhindert.

  Ausschließlich berechtigte Mitarbeiter erhalten Zugriff und jeder Zugriff eines Mitarbeiters wird protokolliert.

- **Managed-Systeme und Services**

  Ein unberechtigter Zugriff wird durch regelmäßige Sicherheitsupdates der vom Auftraggeber installierten Software, nach dem jeweiligen Stand der Technik durch den Auftragnehmer verhindert.

  Ausschließlich berechtigte Mitarbeiter erhalten Zugriff und jeder Zugriff eines Mitarbeiters wird protokolliert.

  Für die Sicherheit der vom Auftraggeber installierten Dienste und Software ist allein der Auftraggeber verantwortlich.

- **Unmanaged-Systeme und Services**

  Die Verantwortung der Zugriffskontrolle obliegt allein dem Auftraggeber.

- **Colocation**

  Die Verantwortung der Zugriffskontrolle obliegt allein dem Auftraggeber.

D. **Datenträgerkontrolle** zur Gewährleistung **der sicheren Benutzung** von Datenträgern mit dem Ziel: … technisch nicht mehr sichere und/oder nicht mehr zu verwendende Datenträger mit pb-

Daten entweder gebrauchsfähig wiederherzustellen oder vollständig zu vernichten.

- Wenn Datenträger nach Beendigung eines Vertragsverhältnisses wiederverwendet werden sollen, wird durch ein definiertes Verfahren mit mehrfachem Überschreiben sichergestellt, dass die Daten unwiederbringlich gelöscht werden.

- Nicht mehr verwendbare Datenträger werden vernichtet.

E. Datentrennungskontrolle zur Gewährleistung **der getrennten Verarbeitung** von pb-Daten mit dem Ziel: … zu gewährleisten, dass pb-Daten, welche zu unterschiedlichen Zwecken erhoben werden und/oder erhoben wurden, getrennt verarbeiten werden.

- **Interne Verwaltungssysteme des Auftragsnehmers**

  Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. Dies gilt auch für die Datensicherung.

- **Managed-Systeme und Services**

  Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. Dies gilt auch für die Datensicherung.

- **Unmanaged-Systeme und Services**

  Die Datentrennungskontrolle obliegt allein dem Auftraggeber. Bei virtualisierten Servern findet eine logische Trennung der Gastsysteme statt. Ab Betriebssystemebene des Gast Systems obliegt die Datentrennungskontolle wieder allein dem Auftraggeber.

- **Colocation**

  Die Datentrennungskontrolle obliegt allein dem Auftraggeber.

II. Verfahren zur Integrität – Art. 32 Abs. 1 lit. b.

Die erforderliche Integrität im o.g. Sinn, zu den durch unser Unternehmen verantwortlich be- und verarbeiteten pb-Daten, wird gewährleistet durch:

A. Übertragungs – und Transportkontrolle zur Gewährleistung **der sicheren Weitergabe** von pb-Daten mit dem Ziel: … zu gewährleisten, dass pb-Daten bei einer elektronischen oder manuell logistischen Übertragung während eines solchen Transports als auch bei der Speicherung auf jegliche Art von lokalen und/oder mobilen Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Des Weiteren ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung der pb-Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- **Allgemein**

  Eine theoretische und technische Zugriffsmöglichkeit auf alle übertragenen Daten zuzugreifen besteht im Rahmen der Verwaltung der Netzwerkhardware wie z.B. von Routern und Switches. Ein Zugriff auf diese Systeme ist nur für geschultes Personal möglich, dass für eine Sicherstellung des Netzwerkbetriebs autorisiert wurde. Die Selektierung von pb-Daten ist hierbei nicht möglich. Es obliegt dem Auftraggeber eine dem technischen Standard entsprechende Verschlüsselung einzusetzen, um dafür Sorge zu tragen, dass die übertragenen Daten nicht lesbar sind.

- **Interne Verwaltungssysteme des Auftragsnehmers**

  Werden pb-Daten aus Interne Verwaltungssysteme übertragen, sorgt der Auftragnehmer für eine dem technischen Standard entsprechende Verschlüsselung

des Übertragungsweges.

- **Managed-Systeme und Services**

  Der Zugriff auf Managed-Systeme und Services wird durch ein vom Auftragnehmer definiertes Berechtigungskonzept geregelt. Ein Zugriff erfolgt ausschließlich durch nach Art. 32 Abs.4 DSGVO unterwiesenes und verpflichtetes Personal. Jeder Zugriff durch das Personal des Auftragnehmers wird protokolliert.
  Werden pb-Daten vom Auftragnehmer übertragen, sorgt der Auftragnehmer für eine dem technischen Standard entsprechende Verschlüsselung des Übertragungsweges.

- **Unmanaged-Systeme und Services**

  Der Auftragnehmer hat bei unmanaged-Systeme und Services keinen Zugriff auf die durch den Auftraggeber verarbeiteten pb-Daten. Werden im Falle einer gesonderten Beauftragung durch den Auftraggeber Daten vom Auftragnehmer übertragen, sorgt der Auftragnehmer für eine dem technischen Standard entsprechende Verschlüsselung des Übertragungsweges.

B. Eingabekontrolle zur Gewährleistung **der nachträglichen Überprüfung** von Eingaben in DV-Systeme zu pb-Daten mit dem Ziel: … zu gewährleisten, dass überprüft und festgestellt werden kann, ob und von wem pb-Daten in DV-Systeme eingegeben, verändert, gespeichert oder entfernt wurden.

- **Interne Verwaltungssysteme des Auftragsnehmers**

  Die Daten werden vom Auftraggeber im Kundenportal selbst eingegeben bzw. erfasst. Eine Eingabe und Erfassung kann auch durch den Auftragnehmer durch Beauftragung des Auftraggebers erfolgen.

  Zugriffe und Änderungen der pb-Daten werden protokolliert.

  Managed-Systeme und Services

  Die Daten werden vom Auftraggeber im Kundenportal selbst eingegeben bzw. erfasst. Eine Eingabe und Erfassung kann auch durch den Auftragnehmer durch Beauftragung des Auftraggebers erfolgen.

  Zugriffe und Änderungen der pb-Daten werden protokolliert.

- **Unmanaged-Systeme und Services**

  Die Eingabekontrolle obliegt allein dem Auftraggeber.

- **Colocation**

  Die Eingabekontrolle obliegt allein dem Auftraggeber.

III. Verfahren zur Verfüg- und Belastbarkeit – Art. 32 Abs. 1 lit. b.

Die erforderliche Verfüg- und Belastbarkeit der einbezogenen DV-Infrastruktur im o.g. Sinn, zu den durch unser Unternehmen verantwortlich be- und verarbeiteten pb-Daten, wird gewährleistet durch:

A. Verfüg- und Belastbarkeitskontrolle zur Gewährleistung der **unbeeinflussten Bearbeitung** von pb-Daten mit dem Ziel: … zu gewährleisten, dass pb-Daten gegen eventuelle Zerstörung und/oder Verlust geschützt sind und im Schadensfall eine schnellstmögliche Wiederherstellung realisiert werden kann.

- **Allgemein**

  Die Stromversorgung der unter A. genannten Rechenzentren erfolgt über mindestens eine n+1 USV-Anlage sowie einer Netzersatzanlage die den Betrieb der Rechenzentren im Fall eines längeren Stromausfalls sicherstellt.

  Eine n+1 Klimaanlage.

  Alle Serverracks werden mit zwei separate Stromzuführungen versorgt.

  Überwachung der Temperatur der unter A. genannten Rechenzentren.

  Flächendeckendes Brandfrühwarnsystem in den unter A. genannten Rechenzentren mit direkter Aufschaltung zur örtlichen Feuerwehr. Sowie einer geeigneten Feuerbekämpfungseinrichtung.

- **Interne Verwaltungssysteme des Auftragsnehmers**

  Die Festplatten-Systeme der IT-Infrastruktur werden Grundsätzlich in einem Raid-Verbund konfiguriert, der eine redundante Speicherung der Daten gewährleistet.

  Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten und Konfigurationen wird durchgeführt und regelmäßig kontrolliert**.**

  Die internen Verwaltungssysteme des Auftragsnehmers werden 24/7 überwacht und gemäß des vereinbarten Service Level Agreements im Falle eines Ausfalls entsprechend entstört.

  Sachgerechter Einsatz von dem technischen Standort entsprechender Sicherheitssoftware (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

- **Managed-Systeme und Services**

  Die Festplatten-Systeme der IT-Infrastruktur werden grundsätzlich in einem Raid-Verbund konfiguriert, der eine redundante Speicherung der Daten gewährleistet.

  Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten und Konfigurationen wird durchgeführt und regelmäßig kontrolliert**.**

  Die vom Auftragnehmer installierten auftragsrelevanten Dienste werden 24/7 überwacht und gemäß des vereinbarten Service Level Agreements im Falle einer Störung entsprechend entstört.

  Sachgerechter Einsatz dem technischen Standard entsprechende Sicherheitssoftware (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

- **Unmanaged-Systeme und Services**

  Die Verfüg- und Belastbarkeitskontrolle obliegt allein dem Auftraggeber, hiervon ausgenommen sind die unter Allgemein genannten Dienste.

- **Colocation**

  Die Verfüg- und Belastbarkeitskontrolle obliegt allein dem Auftraggeber, hiervon ausgenommen sind die unter Allgemein genannten Dienste.

IV. Verfahren zur weisungsgebunden Sicherheit - Art. 32 Abs. 4

A. **Auftragskontrolle** zur Gewährleistung **einer weisungsgebundenen Verarbeitung** von pb-Daten mit dem Ziel: … zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers im Sinne der DSGVO verarbeitet werden können.

- Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß §52 BDSGneu
- Es wurde ein externer Datenschutzbeauftragter bestellt.
- Sofern Subunternehmen mit Aufgaben betraut werden, gelten für diese die gleichen Bestimmungen wir für den Auftragnehmer.

V. Verfahren der Überprüfung, Bewertung und Analyse - Art. 32 Abs. 1 lit. d - Art. 25

A. **Überprüfung, Bewertung und Analyse** zum Datenschutz zum **Wirksamkeitsnachweis** der einbezogenen datenschutzfreundlichen Voreinstellungen sowie der organisatorischen und technischen Maßnahmen mit dem Ziel: … zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, mit einer best- und größtmöglichen Sicherheit mit Bezug zu den Vorgaben der DSGVO und dem BDSGn verarbeitet werden.

- Unsere technischen und organisatorischen Maßnahmen sowie die einbezogene Technikgestaltung und datenschutzfreundliche Voreinstellungen dienen zur Gewährleistung eines sicheren und rechtskonformen Datenschutzes.
- Ein solches Maßnahmenpaket bedarf naturgemäß einer regelmäßigen Überprüfung auf die tatsächliche Wirksamkeit einzelner Komponenten, um deren Effektivität und Effizienz gewährleisten zu können.
- Eine solche Überprüfung geschieht im Rahmen von regelmäßigen Auditierungen im Jahresverlauf durch den bestellten Datenschutzbeauftragten unter dem Einbezug von Mitteln des Qualitätsmanagements entsprechend der DIN EN ISO 9001.
- Weiter sind unsere aufgaben- und prozessbezogenen Aufzeichnungen zum Verzeichnis zu den Verarbeitungstätigkeiten (Art. 30 - DSGVO) im Aufbau ebenfalls an einem qualitätsmanagementbezogenen Auditformat angelehnt, so dass sich bei deren Anwendung jeweils auch Einzelauditierungen mit Wirksamkeitsprüfungscharakter ergeben.
- Insgesamt sind so umfassende und fortlaufende Prüfungen der einbezogenen Maßnahmen auf deren Wirksamkeit zum sicheren Datenschutz gegeben.

Ort: Berlin, 18.05.2018

Bestätigt durch: Herr Dennis. O. Tschech (Geschäftsführer)