Anlage I
Zur Vereinbarung nach Art. 32 DS-GVO
Allgemeine technische und organisatorische Maßnahmen

Der Auftragsverarbeiter setzt folgende technisch und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DS-GVO festgelegt und mit dem Auftraggeber abgestimmt

1. Vertraulichkeit & Integrität gem. Art. 32 Abs. 1lit. B DSGVO

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

- Sorgfalt bei Auswahl der Mitarbeiter
- Zuordnung von Benutzerrechten
- Erstellung von Benutzerprofilen
- differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Passwort vergaben
- Passwort-Richtlinien (Mindestlänge, Komplexität etc.)
- automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Authentifikation mit Benutzernamen und Passwort
- Authentifikation mit Tokens/ Public-Private-Keys/ elektronischen Signaturen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von externen Datenträgern
- Einsatz von Software-Firewalls
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Mehrfaches Überschreiben bei Löschung von Datenträgern vor Wiederverwendung
- Schnittstellenanalyse
- Verschlüsselung der Kommunikationswege

- Übertragung mit elektronischer Signatur
- Transportsicherung
- Festlegung von Datenbankrechten
- Getrennte Keystores für Geheimnisse (z.B. Passwörter)
- Trennung von Produktiv- und Testumgebung
- Physikalische Verteilung von Instanzen
- Container Sicherheitsanalysen
- Konfigurations-Prüftools
- Übertragung mit elektronischer Signatur (z.B. E-Mail)
- Zwei Faktor Authentifizierung (One Time Tokens und Hardware Keys)
- Einsatz von Passwort-Generatoren
- Einsatz von Ende-zu-Ende verschlüsselter Mitarbeiter-Kommunikation (Signal Messenger)

1.1 Zusätzliche Maßnahmen insbesondere für StampLab

- Transportverschlüsselung zwischen Client und Servern (nur TLS 1.2 und TLS 1.3 und HTTP Strict Transport Security)
- AES-256 bit verschlüsselte und SHA256-Integritätsgesicherte Backups
- Passwort-Richtlinien
- Client-Seitiges Hashen von Passwörtern und serverseitiges Zweit-Hashing (mit Salt)
- Tokenbasierte Authentifizierung der StampLab Nutzer nach einmaliger Anmeldung mit Passwort
- Authentifikation mit Benutzernamen und Passwort
- Einsatz von VPN-Technologie bei Übertragung von Daten
- Privat-Public-Key basierter Zugriff auf Serversysteme
- Funktionstrennung von Produktiv- und Testsystem
- AES-GCM verschlüsselte Speicherung von Profilbildern

2. Verfügbarkeit & Belastbarkeit gem. Art. 32 Abs. 1lit. B DSGVO

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Automatische Backup Routine (täglich,mit automatischen Löschzyklen) mit Backup-Ziel außerhalb des genutzten Rechenzentrums (Verfügbarkeit des Backup Speichers liegt

bei 99.999999999%). Die Backups werden vor der Übertragung vollverschlüsselt und Integritätsgesichert (AES-256 bit)
- Es werden aktuelle und quelloffene Server-Betriebssysteme verwendet (Ubuntu 20.04 LTS) die regelmäßig aktualisiert werden
- Sorgsame Auswahl an quelloffener und bewährter Software
- Die Server-Infrastruktur ist ein als hoch verfügbar zu klassifizierendes Kubernetes-Cluster (mit mindestens 3 Control-Planes), dieses ermöglicht eine schnelle Skalierung bei Last und einfache wege zur Wiederherstellung bei Verlust der Verfügbarkeit
- Einsatz von Monitoringsystemen die bei Fehlfunktionen Alarmierungen an Mitarbeiter aussenden
- Einsatz von Fehlererkennung in Anwendungen und automatische Benachrichtigung von Mitarbeitern
- Einsatz von Code Push um (kritische) Korrekturen auch an StampLab Clients auszuspielen
- Softwarebasiertes Load-Balancing zur Lastenkontrolle
- Funktionstrennung von Produktiv- und Testsystem
- Physikalische Verteilung von Instanzen auf verschiedene Rechner
- Regelmäßige Aktualisierung der eingesetzten Software Komponenten und Abhängigkeiten
- Test und Release Konzept

3. Weitere Maßnahmen

- Dokumentation zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter
- Leitlinie zur Informationssicherheit
- Datenschutzkonzept
- Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter
- Datenschutz-Folgenabschätzung wird bei Bedarf duchgeführt
- Die Organisation kommt den Informationspflichten nach DSGVO nach
- Automatisierte Prozesse für Auskunfts- und Löschungsanfragen seitens Betroffener für StampLab Daten

3.1 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Privacy by design wird in Entwicklung berücksichtigt
- Die Organisation erhebt nicht mehr personenbezogene Daten, als für den jeweiligen Zweck erforderlich
- Die Organisation versucht datenschutzfreundliche Voreinstellungen in Anwendungen zu setzen

4. Technische und Organisatorische Maßnahmen des Rechenzentrumsbetreibers (RZB)

Die Bereitstellung der Serverhardware und der Internetanbindung dieser erfolgt durch die IP-Projects GmbH & Co. KG, Am Vogelherd 14, 97295 Waldbrunn

Die Leistungen beschränken sich in diesem Falle auf die Bereitstellung (z.B. kein Auftrag für Backup-Erstellung oder Administration). Es erfolgen keine Leistungen die eine Verarbeitung von personenbezogenen Daten darstellen. Die Verarbeitung von personenbezogenen Daten ist nicht Kern der Rechtsbeziehung und es liegt **keine** Auftragsverarbeitung vor.

Es werden nur Daten der l3montree UG (haftungsbeschränkt) selber durch die IP-Projects GmbH & Co. KG verarbeitet (wie Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungsdaten). Die IP-Projects GmbH & Co. KG hat die Accelerated IT Services GmbH, Kruppstraße 105, 60388 Frankfurt am Main mit der Teilleistung der Colocation (geteiltes ISO/IEC 27001:2013, PCI DSS und vom TÜV Rheinland als „Geprüftes Rechenzentrum der Stufe 3“ zertifiziert Rechenzentrum) beauftragt.

Die Folgenden Unterpunkte der Ziffer 4 sind Maßnahmen der IP-Projects GmbH & Co. KG.

4.1 Zweckbindung und Trennbarkeit

Der RZB gibt an folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische softwareseitige Mandantentrennung

- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern und Signaturen
- pseudonymisierte Daten: Trennung der Zuordnungsdatei und der Aufbewahrung in einem getrennten und abgesicherten IT-System
- Interne Mandantenfähigkeit des Systems
- Funktionstrennung von Produktiv- und Testsystem

4.2 Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des RZB:

- Alarmanlage
- Kameraüberwachung und Aufzeichnung mit Infrarotsystem
- Automatisches Zugangskontrollsystem mit biometrischen Zugangsdaten über Fingerabdruckleser
- Protokollierung sämtlicher Zu- und Ausgänge
- Unterteilung der Flächen in 3 zutrittsgeschützte Räume
- Zugang erfolgt ausschließlich durch Schleusen
- es ist 24x7 Personal vor Ort anwesend
- abgetrennte und gesicherte Räume für Batterien, USV und Stromversorgung
- Automatisches Zugangskontrollsystem mit Chipkarten
- Zuordnung von Benutzerrechten und Einrichtung eines Benutzerstammsatzes pro Nutzer
- Erstellung von Benutzerprofilen
- differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Passwort vergaben
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Authentifikation mit Benutzernamen und Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie bei Übertragung von Daten
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher

- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detektion-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

4.3 Verfügbarkeit, Wiederherstellung und Belastbarkeit der Systeme

Folgende Maßnahmen des RZB gewährleisten, dass die eingesetzten Serversysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- redundante unterbrechungsfreie Stromversorgung (USV) mit bis zu 2.1000kVA Leistung, GreenPower USV Systeme von Socomec
- zwei getrennte Stromfeeds durch 2 Unterverteilungen in jedem Rack
- 10kw Stromaufnahme je Rack und mehr möglich
- Notstromversorgung durch 1000kVA Dieselaggregate
- direkter Nachbar des Umspannwerkes

- 3-Stufiger Überspannungsschutz – Grobschutz in Hauptverteilung, Mittel- / Feinschutz in Unterverteilungen, optionaler weiterer Schutz durch kundeneigene Stromanschlußleisten
- VESDA System zur Früherkennung von Rauchentwicklung
- CO2-Feuerlöscher in allen Bereichen sofort griffbereit
- VDS-Alarmanlagen
- direkte Alarmierung des technischen Personals vor Ort sowie externer Mitarbeiter
- Klimatisierung der Serverräume mit einer Mischung aus direkter und indirekter Freikühlung
- Kaltwasserversorgung durch energiesparende Aggregate von Emerson Networks
- Luftaustausch durch Geräte jüngster Generation von Weiss Klimatechnik
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans
- Einsatz von CWDM Technik für hohe Skalierung der Bandbreiten
- Routing durch moderne Juniper Router
- Coreswitching durch moderne Cisco Switches
- Uplinks wahlweise in 100Mbit, 1GBit oder 10GBit
- Redundante Netzversorgung durch zahlreiche Carrier wie Tiscali International oder die deutsche Telekom
- Peeringverbindungen an diversen Exchangepunkten wie DECiX, AMSiX, KleyReX, ViX und NIX

4.4 Weitere Datenschutzmaßnahmen

- interne Verhaltensregeln
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept