

Anlage 2 zum Auftrag gemäss Art. 28 DS-GVO:

Diese Anlage untersteht regelmässigen Anpassungen und Erweiterungen, um die technischen und organisatorischen Massnahmen der Stand der Technik anzupassen. Die Änderungen werden proaktiv vom Auftragnehmer dem Auftraggeber kommuniziert. Die jeweils aktuelle Version kann hier heruntergeladen werden: <https://www.maxbrain.com/AV/de/TOM.pdf>

Technische und organisatorische Massnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- Rechte an Mitarbeiter des Auftragsnehmers werden nach dem Prinzip: „least-privileged-access“ vergeben.
- Sämtliche Web-Konsolen der eingesetzten Software sind ausschliesslich über VPN erreichbar. Nur befugte Mitarbeiter erhalten einen VPN Zugang.
- Jeder Service der MaxBrain Plattform läuft unter einem dedizierten user, der über minimale Rechte verfügt. Selbst bei einem Hacker Angriff kann also der Angreifer nicht auf weitere Systemressourcen oder Daten zugreifen.
- Sämtliche Server der MaxBrain Plattform sind nur innerhalb eines privaten Netzwerks aufrufbar. Die Wartung erfolgt über ein Bastion-Host. Sämtlicher Netzwerkverkehr geschieht über einen zentralen load-balancer mit vorgelagerter Firewall.
- Die Firewall erlaubt ausschliesslich web-traffic und blockiert alle Ports und anderen Protokolle, die nicht benötigt werden.
- Sämtlicher Netzwerkverkehr, der das private Netzwerk verlässt, wird verschlüsselt.
- Zugriff auf den Bastion-Host geschieht ausschliesslich mittels einer Zertifikats-Basierten Verschlüsselung. Damit entfällt das Risiko von unsicheren Passwörtern.
- Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmässigen Abständen erneuert.
- Durch regelmässige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Die eingesetzten Technologien werden auf auftretenden CVEs überwacht. Kritische Schwachstellen werden umgehen geschlossen.
- Falls Festplatten im Datencenter nicht mehr benötigt werden, werden sie mehrfach überschrieben, bevor sie dem Betreiber zurückgegeben werden.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum zerstört (geschreddert).
- Die Daten jedes Kunden werden in einer separaten Datenbank gespeichert. Dadurch ist der unbefugte oder auch unbeabsichtigte Zugriff auf Daten anderer Kunden nicht möglich. Ausnahmen: Analytics Datenbank, Identity Datenbank.
- Entwickler von ausserhalb der EU oder der Schweiz kriegen keinen VPN Zugang. Falls in ihrer Rolle vorgesehen, können sie sich per SSH auf die Server einloggen, um die Logs und die Konfiguration der Server zu überprüfen.

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

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

- Passwörter werden wenn möglich immer vom Auftraggeber gesetzt. Falls sie vom Auftragnehmer gesetzt werden müssen, werden sie ausschliesslich über ein Einmallink versendet. Es liegt in der Verantwortung vom Auftraggeber, diese Passwörter so schnell wie möglich zu ändern.
- Die meisten Daten werden vom Auftraggeber oder seinen Kunden selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

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

- Kritische Services der Plattform werden redundant betrieben.
- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Monitoring aller relevanter Server inklusive ihrer Systemressourcen.
- Alle kritischen Services werden überwacht und bei Ausfall ein Alert ausgelöst.
- Die Plattform wird regelmässig von extern aufgerufen, um Ausfälle zu entdecken. Bei Problemen wird der Auftragnehmer per SMS benachrichtigt.
- Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):
 - o Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) nach ISO-27001 vereint.
- Im Rahmen des von ISO 27001 vorgegebenen Kontinuierlicher Verbesserungsprozess (KVP) und der jährlichen Re-zertifizierung ist die Überprüfung, Bewertung, Evaluierung und Anpassung gegeben.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Die Mitarbeiter des Auftragnehmers werden in regelmässigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Die MaxBrain AG hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.