Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung

Wahlleitung/Administration: Es findet keine Pseudonymisierung der gespeicherten Daten (Name, EMail Adresse) statt.

Kandidat*innen: Nach Abschluß einer Wahl kann die Wahlleitung alle persönlichen Daten der Kandidat*innen löschen bzw. anonymisieren. Beschreibungen und Bild werden dabei gelöscht, Name wird pseudonymisiert. Diese Funktion ist vom Wahlvorstand ohne personelle Unterstützung Seitens abstimmen.online möglich.

Wähler*innen: Die Wähler*innen werden als Pseudonyme angelegt. Von Wähler*innen werden keine persönliche Daten erhoben oder gespeichert. Die Logdateien die IP Adressen beinhalten werden nach 3 Tagen gelöscht.

Eine Ausnahme sind Online-Veranstaltungen - hierbei werden Namen und EMail Adressen der Teilnehmer für die Dauer der Veranstaltung gespeichert. Allerdings ist es auch hier nicht möglich von Wähler auf die Stimme schliessen.

2. Verschlüsselung

Daten werden auf dem Übertragungsweg vom Benutzer zum Anbieter verschlüsselt. Dabei wird TLS 1.2 verwendet und die Auswahl der verfügbaren Cipher Suites ist auf nachgewiesen starke Algorithmen-Kombinationen beschränkt.
Die Speicherung aller Daten erfolgt auf verschlüsselten Datenträgern bzw. verschlüsselten SQL Datenbanken. Als Algorithmus kommt hierfür AES-128 oder AES-256 zum Einsatz

wobei die Data Encryption Keys mit einem Master Encryption Key verschlüsselt sind der in einem Schlüsselmanagement verwaltet und regelmäßig alle 90 Tage rotiert wird.
Die Verschlüsselung umfasst auch die Backups der SQL bzw. Verzeichnisdaten und die Snapshots der Virtuellen Maschinen.

3. Gewährleistung der Vertraulichkeit

Neben den unter 1. und 2. aufgeführten technischen Maßnahmen existieren weitere die den Zugriff auf Daten reglementieren.
Alle in den SQL Datenbanken gespeicherten Daten eines Kunden (Schule, Verein etc.) sind jeweils logisch diesem zugeordnet. Alle Abfragen die persönliche Daten betreffen nehmen immer den jeweiligen Kunden mit in Betracht d.h. Abfragen stellen sicher, daß tatsächlich nur Daten des jeweiligen Kunden für genau diese Kunden sichtbar sind.
Die Datenbank ist so aufgebaut, daß Abfragen zu statistischen Zwecken (z.B. Anzahl Wähler*innen) möglich sind ohne persönliche Daten zu berühren.

Anmeldungen der Wahlvorstände sind optional mit Multifaktor-Authentifizierung (MFA) möglich. Ist die MFA für einen Wahlvorstand aktiviert, kann diese vom Wahlvorstand selbst nicht mehr deaktiviert werden.

Öffentliche (also ohne Anmeldung) sichtbare Daten sind rein statistischer Natur, beinhalten also keinerlei persönliche Daten. Eine Ausnahme sind Ergebnisse für eine bestimmte Wahl für die der jeweilige Wahlvorstand eine Bekanntgabe des Ergebnisses inkl. der Namen der Kandidat*innen veranlasst hat.

Praktisch uneingeschränkten Zugriff auf alle gespeicherten Daten hat zum jetzigen Zeitpunkt eine Person (Ingo Schubert).
Alle Zugriffe auf Systeme erfolgt mit MFA. Dies umfasst die abstimmen.online Administrationsoberfläche und die virtuellen Maschienen.

4. Gewährleistung der Integrität

Neben den unter 2. und 3. aufgeführten Maßnahmen werden zur Sicherstellung der Integrität alle Änderungen in den Datenbanken transaktionsbasiert durchgeführt d.h. kann eine Änderung aus technischen Gründen nicht ordnungsgemäß durchgeführt werde, bleiben die Daten in der Datenbank konsistent.
Regelmäßige Sicherungen der SQL Datenbanken und des Benutzerverzeichnisses stellen sicher, daß selbst im Falle eine Kompromittierung eine Wiederherstellung möglich ist wobei ggf. ein Datenverlust nicht ausgeschlossen werden kann.

5. Gewährleistung der Verfügbarkeit

Neben den unter 4. aufgeführten Maßnahmen (regelmäßige Sicherungen) existiert eine Überwachung der kritischen Systeme.
Ausfälle werden protokolliert und gemeldet. Die Überwachung findet außerhalb des Cloud Providers statt und Benachrichtigungen werden per E-Mail und Kurznachricht an den Administrator gesendet.

Weiterhin werden alle Ressourcen permanent überwacht und ihre momentane Auslastung (CPU, RAM, Speicherplatz) protokolliert und bei Überschreitungen von Grenzwerten eine Benachrichtigung an den Administrator gesendet.

Das abstimmen.online System besteht aus zwei getrennten Systemen: Datenbank und Front-end. Beide können unabhängig voneinander auf mehreren Instanzen laufen.
Zum jetzigen Zeitpunkt laufe sowohl die Datenbank als auch das Front-End auf jeweils mindestens einer virtuellen Maschine.

Bei Bedarf kann eine zweite Front-End VM gestartet werden. Da die Front-Ends hinter einem Load Balancer (der selbst ebenfalls hoch-verfügbar ist) platziert sind, ist dadurch ein Ausfall (z.B. durch Neustart des Betriebssystems oder auch nur des Applikationsservers) einer der Front-End VMs möglich ohne die Gesamtverfügbarkeit zu beeinträchtigten.
Dadurch ist z.B. das Einspielen von Patches möglich ohne einen Ausfall zu verursachen.

Beim Neustart eines Systems ist dieses innerhalb kurzer Zeit (<5 Minuten) wieder verfügbar.

Der Cloud Provider selbst hat unabhängig von allen genannten technischen Maßnahmen von abstimmen.online eigene technischen Vorrichtungen um die Verfügbarkeit der Systeme zu gewährleisten. So ist z.B. ein Ausfall des oder der physischen Server auf dem abstimmen.online läuft im Normalfall ohne Auswirkung auf die Verfügbarkeit des Systems da transparent auf alternative Hardwareressourcen gewechselt wird.

6. Gewährleistung der Belastbarkeit der Systeme

Neben dem unter 5. aufgeführten Maßnahmen (Monitoring, Alerting) basiert abstimmen.online auf einer Architektur, die es ermöglicht die Belastbarkeit des Systems zu erhöhen.

Kurzfristige Erhöhungen sind durch das starten der zweiten Front-End VM möglich. Dies kann manuell erfolgen, wird aber auch automatisch vom System veranlasst sollte die momentane Auslastung des Systems über einem festgelegten Schwellwert liegen oder eine größere Veranstaltung in den folgenden 30 Minuten starten. Die zusätzlich gestartete Front-End VM wird grundsätzlich um 1:00 Uhr nachts wieder abgeschaltet. Ein evtl. automatisches Starten der zweiten Front-End VM wird allerdings nicht unterbunden.

Weiterhin kann die Leistung der Datenbank durch die Zuweisung zusätzlicher virtueller CPU Kerne und ggf. RAM erhöht werden. Der verwendete Cloud Provider macht solch eine Erhöhung möglich wobei ein Neustart der Datenbank notwendig ist und damit eine kurzfristiger Ausfall zum jetzigen Zeitpunkt nicht vermieden werden kann.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Backups der relevanten Daten sind verschlüsselt in getrennten Systemen gespeichert und können vom Administrator wiederhergestellt werden. Im Falle der SQL Daten mit nativen Mechanismen des Cloud Providers und im Falle der Anmeldedaten der Wahlvorstände eine manuelle Wiederherstellung des Benutzerverzeichnisses.

Eine Wiederherstellung wird erst durchgeführt nachdem sichergestellt wurde, daß andere technischen Maßnahmen erfolglos waren.

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Einmal pro Jahr wird eine komplette Wiederherstellung der Produktivsysteme auf separate Systeme durchgeführt. Dabei wird überprüft ob danach ein funktionierendes Gesamtsystem vorliegt.

Haldenwang, 10.12.2021