Sicherheit & Datenschutz bei AYGOnet

Inhalt

1. Einleitung

An Orten, wo es um Beratungen geht, die auch sehr private Inhalte über die Person, Gefühle oder Gesundheit haben, muss Datenschutz ein Kernbaustein sein.

Wir sind uns dieser sensiblen Inhalte und der damit einhergehenden Verantwortung bewusst und wollen daher den bestmöglichen Schutz für eine vertrauenswürdige Beratung bieten. So ist Datenschutz nicht erst seit der DSGVO, sondern schon seit Beginn ein wichtiger Bestandteil von AYGOnet. Mit AYGOnet 2 haben wir das Thema Datenschutz jedoch nochmal auf eine neue Ebene gestellt. Um dies zu ermöglichen, haben wir eine Vielzahl an Maßnahmen ergriffen, die den Datenschutz in AYGOnet und somit den Datenschutz in Ihren Beratungen an erste Stelle stellen.

Im Folgenden möchten wir Ihnen einen Überblick über die getroffenen Maßnahmen geben.

2. Allgemeine Fragen

Es gibt ein paar grundlegende Fragen, die sich aus der Gesamtheit der Maßnahmen beantworten lassen. Diese wollen wir hier zu Beginn einmal beantworten – bzw. unsere Einschätzung dazu geben.

2.1. Sollten wir unsere / unseren Datenschutzbeauftragte*n in die Wahl eines solchen Tools mit einbeziehen?

Ja – wir empfehlen dringend die verantwortliche Person mit entsprechender Expertise einzubeziehen. Am Ende ist es jene Person, die hier eine für Ihre Beratungsstelle zutreffende Einschätzung liefern kann. Unser Fokus liegt zudem auf den Regularien der DSGVO. Sollten für Sie weitere Regularien wie beispielweise das KDG relevant sein, kann Ihr / Ihre Datenschutzbeauftragte*r dies auf Basis dessen einordnen. Hierbei kann dieses Dokument helfen. Wir stehen Ihnen und Ihrer / Ihrem Datenschutzbeauftragten aber auch gerne persönlich für Fragen zur Verfügung.

2.2. Kann AYGOnet bei Ermittlungen (bspw. bei suizidaler Androhung) unterstützen?

Im Falle von Ermittlungen steht Ihnen das komplette AYGOnet Team zur Verfügung und unterstützt sowohl die Beratungsstellen als auch die Behörden nach allen Möglichkeiten.

Wie Sie dem folgenden Dokument entnehmen können, sammelt AYGOnet jedoch keinerlei Daten. Auch Logs (die personenbezogenen Daten wie IP-Adressen) werden nicht erstellt. Somit ist uns eine Identifikation betroffener in der Regel nicht möglich. Die meisten Daten, die eine Identifikation ermöglichen liegen den Berater*innen durch die Beratung vor. Einzig die E-Mail-Adresse der Klient*innen – soweit angegeben, liegt der Beratungsstelle nicht vor und könnte ausschließlich durch die AYGOnet GmbH eingesehen werden.

Bei Rückfragen zu den Möglichkeiten, warum eine Identifizierung durch uns nicht möglich ist und bei weiteren Fragen zu diesem Thema, sprechen Sie unser Team gerne an.

3.Verschlüsselungen

Die Verschlüsselung der Daten ist wohl oder minder einer der wichtigsten Punkte um die Kommunikation privat zu halten.

So haben wir folgende Verschlüsselungsverfahren implementiert.

- Transportverschlüsselung (TLS)
- Public-Private-Key Verfahren
- Verschlüsselte PHP-Sessions

Neben der obligatorischen TSL (weitläufig bekannt unter SSL) Verschlüsselung, wird die Kommunikation zwischen den Gesprächsbeteiligten in einem Public-Private-Key Verfahren verschlüsselt.

Bei der Registrierung eines neuen Accounts, wird immer ein persönlicher Key erstellt. Eine versendete Nachricht wird also immer mit dem Private-Key des versendenden Accounts verschlüsselt. Die / der Empfänger*in, kann dies dann mit dem Public-Key wieder entschlüsseln.

3.1. Public-Private-Key Verfahren / Passwörter

Bei diesem Verfahren gibt es vier zentrale Anwendungsfälle. Die Registrierung, den Login, das Passwort Reset und das Erneuern eines Keys.

Das Key Verfahren läuft zudem sehr eng mit dem Umgang der Passwörter, weshalb auch diese hier thematisiert wird.

3.1.1. Registrierung

- Eine Person registriert sich – das neu gesetzte Passwort wird (ergänzt um einen zufälligen Salt) bCrypt gehasht.
- Ein neues Schlüsselpaar wird erzeugt und mit dem zuvor erzeugten Passwort-Hash AES-256-CBC-verschlüsselt.
- Anschließend wird das 1-mal gehashte Passwort dann nochmal bCrypt-gehasht und in der Datenbank abgelegt.

Passwörter werden übrigens immer durch die/den Nutzer*in vergeben. Auch bei Berater*innen Accounts, werden keine Passwörter durch die / den Administrator*in vergeben.

3.1.2. Login

- Beim Login wird das eingegebene Passwort mit einem neuem Salt bCrypt-gehasht. Ist der Login erfolgreich, wird das neu-gehashte Passwort in der DB abgelegt.

Im unwahrscheinlichen Fall eines unerlaubten Datenbankzugriffs, können also nicht mal die gehashten Passwörter weiterverwendet werden – da sich diese regelmäßig – bei jedem Login ändern.

3.1.3. Passwort Reset

Ist eine Mailadresse hinterlegt, kann die/der Nutzer*in ein neues Kennwort anfordern. An die hinterlegte Mailadresse wird dann ein Link zum Generieren eines neuen Passwortes versendet. Dieser Link ist wie alle Systemlinks 10 Minuten gültig.

Bei einem Passwort Reset wird darüber hinaus ein neues Schlüsselpaar erzeugt und später freigegebene Inhalte neu verschlüsselt. Vorerst sind alte Gesprächsverläufe aber nicht lesbar, da diese noch mit dem alten Schlüsselpaar verschlüsselt sind.

Alle Account Rollen (ausgenommen Klient*innen) müssen anschließend von einer übergeordneten Rolle (siehe Punkt 6) freigeschaltet werden um anschließend eine Wiederherstellung / Entschlüsselung zu starten.

Abhängig von der Rolle des Accounts erfolgen dann unterschiedliche Schritte. Mehr dazu unter Punkt 5.2.2.

3.1.4. Schlüsselpaar erneuern

Möchte man also aus Sicherheitsgründen den eigenen Key erneuern, kann dies durch die Passwortvergessen-Funktion erfolgen.

3.1.5. Beratungsstellenschlüssel

Im Beratungsverlauf kommt es immer wieder zu Situationen, in denen eine Beratung noch einseitig ist (Beratungsbeginn / Erstanfrage), bzw. Dritte in ein Gespräch geholt werden (Supervisor Anfrage). In dieser Phase erfolgte also noch kein Schlüsselaustausch zwischen den Gesprächspartner*innen und es müssen z.B. im Fall der Erstanfrage mehrere Personen auf diese zugreifen können. Auch in diesem Zustand sollen die Anfragen dasselbe Schutzniveau behalten. Zu diesem Zweck gibt es für jede Beratungsstelle ein Beratungsstellenschlüsselpaar. Die Nachrichten sind also zwischen Klient*in und Beratungsstelle verschlüsselt. Mit Übernahme einer Beratung durch eine / einen Berater*in wird diese Verschlüsselung jedoch zwischen den beiden Gesprächspartner*innen hergestellt und eine Verschlüsselung mit dem Beratungsstellenschlüssel erfolgt nicht mehr.

Der Beratungsstellen-Private-Key steht allen Berater*innen zur Verfügung um diese empfangenen Nachrichten zu entschlüsseln. Dieser Schlüssel wird jedoch für jeden Account einzeln mit dem eigenen Private-Key verschlüsselt abgelegt. So hat jeder Account seinen eigenen Private-Key der Beratungsstelle, welcher nur von diesem genutzt werden kann.

3.1.6. Versendete Dateien

Im Beratungsverlauf haben Berater*innen und je nach Beratungsstelleneinstellung, auch die Klient*innen, die Möglichkeit Dateien an ihre Nachrichten anzuhängen. Diese werden in den Beratungsstellen eigenen Ordner abgelegt und sind nur über einen direkten Link aufrufbar. Zudem werden alle so versendeten Inhalte synchron verschlüsselt.

Beim Versand einer Datei wird ein zufälliges Passwort erzeugt, mit welchem die Datei verschlüsselt wird. Dieses wird der Nachricht mitgegeben und die Nachricht wir, wie gewohnt, mit dem Private-Key verschlüsselt.

Wichtig: das betrifft nur über die Mailberatung bzw. interne Kommunikation versendete Dateien. Nicht aber z.B. Profilbilder. Hierzu mehr unter 3.4.

3.2. Verschlüsselte PHP-Sessions

Da die Keys nicht lokal, sondern innerhalb der Datenbank auf dem Server liegen, werden diese beim Login serverseitig entschlüsselt und aus Sicherheitsgründen nicht lokal übertragen. Damit die während der Nutzung entschlüsselten Daten jedoch weiter geschützt bleiben, findet die Entschlüsselung innerhalb einer verschlüsselten PHP-Session statt.

Aus dieser Session werden die Inhalte dann TLS verschlüsselt an die Nutzer*innen übertragen.

3.3. Ende-zu-Ende Verschlüsselung?

An dieser Stelle stellt sich natürlich die Frage, ob wir hier von einer reinen Ende-zu-Ende Verschlüsselung sprechen können. Kurz gesagt, können wir das (derzeit) für die **Mailberatung** nicht.

Auch wenn unsere Inhalte wie beschrieben durchgehend verschlüsselt sind, entspricht dies keiner reinen Ende-zu-Ende-Verschlüsselung.

Grund hierfür ist, dass für eine reine Ende-zu-Ende Verschlüsselung keine Entschlüsselung zwischen den Gesprächspartner*innen erfolgen darf. Das wiederum erwartet die Entschlüsselung direkt bei dem/der Nutzer*in (im Browser/ der Anwendung). Dies ist wiederum nur möglich, wenn der Key lokal abgelegt und beim Login eingegeben werden kann.

Bei dem Pendant in der PGP verschlüsselten Mail erfolgt dies beispielweise durch die Einbindung des Zertifikats in den Mail-Client.

Ohne dass der Schlüssel also durch die/den Nutzer*in oder eine lokale Anwendung eingespielt / verwaltet wird, kann also keine dauerhafte Ende-zu-Ende Verschlüsselung erfolgen.

Das von uns eingesetzte Verfahren, stellt jedoch zu keiner Zeit unverschlüsselte Inhalte bereit. Der Austausch zwischen den Gesprächspartner*innen erfolgt also stets mit mindestens einer Verschlüsselungsschicht (z.B. TLS oder die verschlüsselte PHP-Session).

Für die Zukunft, soll es auch möglich sein, Beratungsstellen-Kommunikationen optional mit einer Ende-zu-Ende Verschlüsselung im Bereich der Mailberatung zu betreiben. Dies setzt jedoch das lokale Ablegen des eigenen Schlüssels voraus. Die Sicherheit der Ende-zu-Ende Verschlüsselung richtet sich dann natürlich nach dem Umgang mit den Schlüsseln. Ein solches Verfahren wird dann aber zu gegebener Zeit angekündigt.

Video- und Chatberatung. Diese beiden Beratungsformen können aber schon von Beginn an mit einer durchgehenden Ende-zu-Ende Verschlüsselung angeboten werden. In diesem Fall findet der Austausch eines temporären Schlüsselpaars statt. Der Schlüssel wird also für ein Chat- oder Videogespräch erstellt, zwischen den Gesprächspartner*innen ausgetauscht und verfällt bei Beendigung des Gesprächs wieder.

3.4. Was ist NICHT verschlüsselt?

Es gibt Daten, die unverschlüsselt in der Datenbank stehen. Zumeist handelt es sich um Systeminformationen / -einstellungen. Doch auch die Metadaten der Gesprächsverläufe sowie einzelne systemrelevante Nutzungsdaten. Eine Liste finden Sie hier:

- Accountname, Rolle, Mailadresse
- Alle Beratungsstellen-Settings
- Mail Metadaten wie Uhrzeit, Teilnehmer*innen
- Kategorien
- Profilbilder und Logos

4.Sicherheit der Daten

4.1. Server- und Datenbanksicherheit

4.1.1. Datentrennung

Die Datentrennung innerhalb der AYGOnet Anwendung erfolgt auf mehreren Ebenen. So ist das System in zwei Ebenen aufgeteilt: Ressorts und Beratungsstellen.

Ein Ressort enthält 20-50 unterschiedliche Beratungsstellen. Die Beratungsstellen eines Ressorts teilen sich eine Docker-Stack.

Jede Beratungsstelle hingegen verfügt über eine eigene Datenbank, auf die nur aus dem jeweiligen Docker-Stack zugegriffen werden kann. Zudem wird jeder Beratungsstelle ein eigener Upload-Ordner bereitgestellt.

4.1.2. Datensparsamkeit

Wir sammeln keine Daten, die nicht für den Betrieb notwendig sind. Für den Betrieb notwendig sind beispielweise die unter Punkt 4.2 thematisierten Inhalte, wie Logs und Login-Informationen.

4.2. Daten die wir sammeln und Daten die uns mitgeteilt werden

4.2.1. Daten der Nutzer*innen und Beratungsdaten

Für die Registrierung durch Ratsuchende wird lediglich ein Accountname und ein Passwort zwingend benötigt. Berater*innen und Administrator*innen benötigen darüber hinaus noch eine eigene Mailadresse. Alle weiteren Vorgaben und Anforderungen an die Registrierung werden durch die Beratungsstelle selbst getroffen. So ist beispielweise die zwingende Angabe einer Mailadresse für Klient*innen durch die Beratungsstelle aktivierbar.

4.2.2. Tracking

Innerhalb der AYGOnet Anwendung erfolgt kein Tracking.

4.2.3. Loging: Integrität & Sicherheit

Derzeit gibt es lediglich Logs, die zum Betrieb und für die Sicherheit der Anwendung notwendig sind. Welche Logs erstellt werden und wie lange diesen Bestand haben, wird nachfolgend erklärt.

- Error Log
  Dieser enthält angaben zu Fehlverhalten der Anwendung und wird nur bei solchen geschrieben. Er enthält den Zeitpunkt des Aufrufs, die IP-Adresse und Informationen zu verwendetem Browser und Betriebssystem. Die Logs werden 10-14 Tage aufbewahrt. Diese Logs dienen der Sicherheit und der Stabilität des Systems sowie der Fehleranalyse.

- Software Log
  Innerhalb der Anwendung werden zukünftig zudem systemrelevante Ereignisse geloggt. Dort sollen Inhalte wie Log In und Out Zeitpunkte, sowie das Löschen, Erstellen und Ändern von Accounts geloggt werden. Darüber hinaus auch Informationen zu Änderungen an der Beratungsstelle, welche einen signifikaten Einfluss auf diese haben. Zu solchen Änderungen würde z.B. die Löschung einer Abteilung oder der gesammten Beratungsstelle gehören. Das Loggen dieser Inhalte dient der Integrität und der Eingabekontrolle vor allem bei administrativen Rollen zu protokollieren.

Die Software-Logs sollen immer für einen Monat erstellt und nach drei Monaten wieder gelöscht. Abgesehen von den Accountnamen, der Aktion und der Uhrzeit, sind jedoch keine Daten enthalten.

4.3. Passwörter, 2FA und Systemlinks

Der Zugang zum System ist besonders zu schützen, da dieser die Einsicht in die persönlichen Beratungsinhalte bzw. die der Klient*innen gewährt.

So ergreifen wir mehrere optionale und nicht optionale Maßnahmen zum Schutz des Zugangs.

4.3.1. Mindestanforderung an die Passwörter

Die durch die Anwendung geltenden Mindestanforderungen an ein Passwort sind:

- Mindestens 12 Zeichen
- Bestehend aus Groß-, und Kleinbuchstaben
- Enthält mindestens eine Zahl
- Enthält mindestens ein Zeichen, welches weder klein, groß noch eine Zahl ist

4.3.2. Zwei-Faktor-Authentifizierung

Eine Zwei-Faktor-Authentifizierung kann die Sicherheit des Zugangs weiter verstärken. Die in AYGOnet implementierte Zwei-Faktor-Authentifizierung erfolgt über eine E-Mail.

Nach dem Login mit den Zugangsdaten wird eine E-Mail an die/den Nutzer*in gesendet. Diese enthält einen Code, welcher in der nach dem Login erscheinenden Maske eingegeben werden muss.

Die Zwei-Faktor-Authentifizierung ist für alle administrativen Rollen standardmäßig aktiviert. Ressortadministratior*innen können dies auch nicht deaktivieren.

Den administrativen Rollen der Beratungsstelle ist eine Deaktivierung jedoch möglich.

Für Berater*innen und Klient*innen ist die Zwei-Faktor-Authentifizierung zwar standardmäßig deaktiviert, kann jedoch aktiviert werden. Dies setzt lediglich eine hinterlegte E-Mail-Adresse voraus.

4.3.3. Session TimeOut

Jede Session wird nach einer Inaktivität von einer Stunde automatisch beendet. Anschließend ist ein neuer Login erforderlich.

4.3.4. Gültigkeit der Systemlinks

Alle Systemlinks, die das (Zurück-) Setzen eines Passworts oder die Authentifizierung ermöglichen, haben eine Gültigkeitsdauer von 10 Minuten. Anschließend, muss ein neuer Link ausgestellt werden.

4.3.5. Zusätzliche Sicherheitsmaßnahmen bei der AYGOnet GmbH und Ihren Dienstleistern

Über die Systemanforderungen von AYGOnet hinaus haben wir uns als Unternehmen und unseren Dienstleistern weitere Sicherheitsmaßnahmen auferlegt, um die Sicherheit zu erhöhen. Alle anderen Regeln bleiben unangetastet.

- Die Passwortlänge beträgt mindestens 16 Zeichen
- Alle Zugänge müssen mit unterschiedlichen Passwörtern versehen werden
- Eigene Zugänge dürfen nur einem selbst zugänglich gemacht werden
- Zugänge zu den Servern erfolgen ausschließlich über personalisierte SSH-Keys und freigegebene IP-Adressen

5. Datenverfügbarkeit & Löschung

5.1. Backup / Verfügbarkeitskontrolle

Der gesamte Datenbestand aller Server wird täglich festplattengestützt an zwei geographisch getrennten Orten gesichert. D.h. es existiert ein Backup aller Daten aller Server am Standort und ein entferntes Backup auf einem via VPN angebundenen Server. Dabei wird eine Sicherung 6 Tage die Woche durchgeführt und am siebten Tag ein Wochenbackup abgelegt. Es existieren also 6 Tage zurück tägliche Sicherungsstände und 4 Wochen zurück die jeweiligen Wochenbackups. Eine weitere Archivierung wird nicht vorgenommen.

5.2. Datenlöschung

Die Löschung von Accounts und Daten erfolgt in der Regel unmittelbar.

5.2.1. Beratungsstellen

Bei der Löschung einer Beratungsstelle durch die Ressortadministration werden unmittelbar alle Zugänge, Einstellungen und die damit verbundene Datenbank gelöscht. Mögliche Datei-Ordner mit hochgeladenen Dokumenten, Profilbildern und Ähnlichem werden mit einem Zeitstempel versehen umbenannt. Durch dieses Verfahren, ist ein Zugriff von Außen nicht mehr möglich. Alle 48 Stunden läuft dann ein Cronjob, welcher diese Daten komplett löscht. Die Löschung einer Beratungsstelle durch die AYGOnet GmbH erfolgt ausschließlich nach schriftlicher Weisung durch die Auftraggeber*innen.

5.2.2. Accounts

Die Löschung eines Accounts erfolgt ebenfalls umgehend. Die mit dem Account verknüpften Daten / Dokumente werden, wie unter 5.2.1 beschrieben, behandelt und durch einen Cronjob nach 48 Stunden gelöscht. Die Löschung eines Beraterinnen / Berater Accounts setzt die Verschiebung der verknüpften Beratungsstränge an andere Beraterinnen / Berater voraus. Die Löschung der Klientinnen / Klienten hingegen kann jederzeit durch die Klientinnen / Klienten selbst durchgeführt

werden. In diesem Fall werden alle Beratungsverläufe umgehend gelöscht. Bestehen bleiben in allen Fällen jedoch die Accountnamen und die Protokolle / Logbücher, welche durch die Beraterinnen / Berater erstellt wurden. Abhängig von der Beratungsstelle ist die Aufbewahrung dieses Protokolls verpflichtend. Ist dies nicht der Fall erhält die Beraterin / der Berater die Möglichkeit dieses komplett zu löschen. Die Accountnamen werden aufbewahrt um den anschließenden Missbrauch zu unterbinden, wodurch sich Dritte für ehemalige Klientinnen / Klienten ausgeben könnten.

In allen Szenarien, können Daten (wie oben beschrieben) bis zu 4 Wochen auf einem BackUp Medium weiter bestehen. Die vollständige Löschung erfolgt somit spätestens nach 4 Wochen.

Die Löschung inaktiver Accounts erfolgt ebenfalls in festgelegten Zyklen. Nach welchem Zeitraum ein inaktiver Account gelöscht wird, bestimmt die Beratungsstelle.

5.3. Wiederherstellbarkeit

Eine Wiederherstellung von einmal gelöschten Inhalten ist durch die endgültige Löschung nicht mehr möglich. BackUps werden nur im Falle einer technischen Störung verwendet, nicht jedoch um gelöschte Inhalte wiederherzustellen.

Die Wiederherstellung der Daten nach Passwortverlust ist nur unter bestimmten Voraussetzungen möglich.

Da der Private Schlüssel, mit welchem die eigenen Beratungsverläufe verschlüsselt sind, durch das eigene Passwort verschlüsselt ist, kann dieser auch nur mit diesem entschlüsselt werden. Im Falle eines Passwortverlustes wäre somit eine Entschlüsselung mangels Zugriffes auf die Schlüssel nicht mehr möglich. Um dieses Szenario zu vermeiden erhalten Berater*innen und Administrator*innen die Möglichkeit einen Wiederherstellungscode zu speichern. Dieser sollte beim ersten Login und bei jedem Passwort Reset neu erstellt und an einem sicheren Ort verwahrt werden.

Mit der Eingabe dieses Codes, erhält man Zugriff auf das bisherige Schlüsselpaar und die bisherigen Nachrichten. Diese Nachrichten werden dann wiederum mit dem neuen Schlüsselpaar verschlüsselt.

Die Entschlüsselung auf Seiten der Klient*innen erfolgt hingegen etwas anders. Diese können nach dem Login auf alle Daten aber nicht auf die Beratungsverläufe zugreifen. Mit dem neuen Schlüssel (welcher durch den Passwort Reset erstellt wurde) können Sie nun aber wieder mit den Berater*innen in Kontakt treten. Berater*innen haben dann die Möglichkeit die Inhalte für die Klient*innen wieder neu freizugeben. So kann eine / ein Klient*in sich zuvor erklären und so (nach Entscheidung der / des Berater*in) wieder auf die alten Inhalte zugreifen.

6. Wer darf was?

Die Sicherheit einer Anwendung besteht natürlich nicht nur aus den zentralen und wichtigen Bausteinen der technischen Umsetzung, Hardware und Verschlüsselung, sondern auch aus einem durchdachten Rollenkonzept.

6.1. Rollenkonzept

Das Rollenkonzept der AYGOnet Anwendung, soll dazu dienen, dass jede Rolle nur die Rechte erhält, die sie zur Erfüllung der Aufgaben benötigt. Zudem wird hierdurch eine Trennung der administrativen und der beratenden Tätigkeiten erreicht.

Hierarchisch sieht dies wie folgt aus:

Ressortadministration
> Beratungsstellenadministration
> Abteilungsadministration
> Berater*in
> Klient*in

6.1.1. Ressortadministration

An dieser Stelle werden alle Beratungsstellen eines Ressorts verwaltet. Es werden Beratungsstellen angelegt und bearbeitet. Zudem erhält diese Rolle einen Einblick in die mit der Beratungsstelle verknüpften Benutzer*innen aller Rollen.

Durch die Rolle der Ressortadministration können ausschließlich Accounts zur Beratungsstellenadministration angelegt werden. Der Erste dieser Accounts wird initial mit der Beratungsstelle angelegt. Alle weiteren Accounts dieser Rolle müssen immer durch die/den „Haupt-Administrator*in“ (s.u.) freigegeben werden. So kann verhindert werden, dass unbemerkt weitere Accounts mit administrativen Rechten für eine Beratungsstelle angelegt werden.

Änderungen an Accounts, egal welcher Rolle, sind keiner / keinem Ressortadministrator*in möglich.

Die Accounts der Ressortadministration bilden die höchste Ebene der Rechtsstruktur und unterliegen nur den Serveradministrator*innen, welche jedoch keine Rolle der Anwendung darstellen.

6.1.2. Beratungsstellen- / Abteilungs-Administration

Die Administration einer Beratungsstelle sowie einer Abteilung laufen sehr parallel. Unterschiede liegen lediglich in der Reichweite der möglichen Änderungen. Dabei ist die Reichweite der Abteilungs-Administration auf jene Abteilung begrenzt.

Die Rolle der Beratungsstellen-Administration kann neben den Einstellungen der Beratungsstelle auch die der Abteilungen anpassen, Abteilungen anlegen und neue Abteilungsadministrator*innen, sowie neue Berater*innen anlegen.

Das Setzen des Passworts erfolgt, wie bereits beschrieben, nicht über diese Rolle, sondern ausschließlich über die / den Nutzer*in.

Einmal angelegt, kann die Rolle der Beratungsstellen-Administration zwar Eigenschaften, E-Mail Adresse und Kontaktdaten, nicht aber das Passwort der Berater*innen ändern.

Eine Änderung der Klient*innen Daten durch Administrator*innen ist zudem nicht möglich.

Über die Verwaltung der Beratungsstelle und der Accounts hinaus, dient diese Rolle auch dazu, Accounts der Berater-Rolle nach dem Passwort Reset oder nach einer Sperrung durch zu viele fehlerhafte Logins wieder frei zu schalten.

Wichtig ist zudem, dass die Administratoren Rolle keine Beratungen durchführen. Dafür ist sie jedoch Teil der internen Kommunikation.

Bei Änderungen (durch Administrator*innen) von Userdaten, Löschen von Accounts und ähnlichem, werden stets alle beteiligten Administrator*innen via E-Mail informiert. So können keine unbemerkten Änderungen erfolgen.

Die Nutzung der Rolle wird mit personenspezifischen (nicht geteilten) Zugängen empfohlen.

Hervorgehoben sei an dieser Stelle noch die Sonderposition der / des ältesten bestehenden Beratungsstellen-Administrator*in – der / des Hauptadministrator*in. Dieser Account erhält (gekennzeichnet durch eine Krone in der Liste der Administrator*innen einer Beratungsstelle) die zusätzliche Funktion / Rolle der Freigabe und dem Erstellen neuer administrativen Accounts.

So kann verhindert werden, dass durch andere administrative Accounts oder die Ressortadministration unbemerkt weitere Beratungsstellen-Administrator*innen angelegt werden.

6.1.3. Berater*innen

Accounts der Berater-Rolle haben stehts nur Zugriff auf die eigenen Daten und die zugeordneten Klient*innen. Die Änderung der Daten Dritter ist für diese Rolle nicht möglich.

Diese Rolle ist die Erste und neben der folgenden Rolle der Klient*innen die Einzige mit Zugriff auf die Beratungsmodule. Verwaltung und Beratung werden also getrennt.

6.1.4. Klient*innen

Klient*innen können lediglich ihre eigenen Daten bearbeiten. Sie haben darüber hinaus keine weiteren Rechte.

6.1.5. Zustimmungen: Supervisor, Freigaben

Innerhalb einer Beratung gibt es die Möglichkeit eine / einen Supervisor*in anzufragen.
Eine / ein Supervisor*in ist eine normale / ein normaler Berater*in mit der Zusatzfunktion der Supervision. Die Hinzunahme einer / eines Supervisor*in erfolgt auf Anfragen der / des Berater*in jedoch ausschließlich mit der Zustimmung der beteiligten Klient*innen. Weder der Zugriff noch die Verschlüsselung der Beratungsverläufe erfolgt bevor die / der Klient*in eine Freigabe erteilt haben. Wird die Zustimmung nicht erteilt, erfolgt keine Freigabe für die Supervision. Das Beenden einer Supervision erfolgt anschließend über die / den Supervisor*in. Das Hinzukommen oder Verlassen einer dritten Person in einen Gesprächsverlauf (ob als Supervisor*in oder innerhalb einer Gruppenberatung), wird im Sinne der Transparenz visuell dargestellt.

6.2. Worauf kann die AYGOnet GmbH zugreifen?

Wie unter Punkt 3.5 beschrieben gibt es lediglich eine Handvoll unverschlüsselter Daten innerhalb der AYGOnet Anwendung. Auf diese beschränkt sich auch der Zugriff der AYGOnet GmbH. Zusammenfassen lassen sich diese Daten unter dem Kontext der Metadaten, die bei der Zustellung der Nachrichten anfallen (keine Nachrichteninhalte) sowie alle Einstellungen der Beratungsstellen und Accountdaten (Name und E-Mail Adressen). Weder Mitarbeiter*innen der AYGOnet GmbH noch die der Dienstleister können sich ohne Zustimmung der Beratungsstellen einen ensprechenden Zugang erstellen.

6.3. Schnittstellen / Dritte

Innerhalb von AYGOnet werden weder Schnittstellen zu Dritten noch Inhalte Dritter eingebunden. Neben den unten (Punkt 10.1) genannten Dienstleistern, haben Dritte auch keinen Zugriff auf die Anwendung.

7.Dokumente und Bestimmungen

7.1. Betroffenenrechte

Die Betroffenenrechte nach DSGVO (Art. 15 – 21) haben wir soweit dies möglich ist, direkt in die Prozesse der Anwendung eingebaut. Der Umgang mit z.B. Recht auf Berichtigung, Löschung etc. sind diesem Dokument zu entnehmen. Darüberhinaus liegt ein maaßgeblicher Teil der Umsetzung innerhalb der Beratungsstellen. Bei der Erfüllung der Betroffenenrechte unterstützen wir alle Kund*innen nach allen Möglichkeiten.

7.2. Datenschutz, Nutzung und Impressum

Die Bestimmungen zum Datenschutz, der Nutzung und das Impressum unterliegen der Verantwortung der Kund*innen. Um den Einstieg zu erleichtern, stellen wir jedoch einen Rahmen für die eigenen Datenschutzbestimmungen bereit. Es ist jedoch darauf zu achten, das dies nur als

Rahmen zu verstehen ist. Da die Einstellungen je Beratungsstelle variiren können und wir keinen Einblick in den Umgang mit den Daten innerhalb einer Beratungsstelle haben, können wir keine vollwertige Datenschutzbestimmung für die Nutzung bereitstellen. Zur Erstellung sollten die in diesem Dokument bereitgestellten Informationen jedoch dienlich sein.

7.3. Verfügbarkeit und SLAs

Die Verfügbarkeit der AYGOnet Beratungsstellen (soweit das Hosting durch uns erfolgt) beträgt 99% / Jahr.
Sollte es jedoch mal zu Störungen im System kommen, gibt es drei Wege, über welche wir Sie informiert halten. Mehr dazu und wann welcher Weg genutzt wird, finden sie im folgenden Abschnitt.
Durch uns festgestellte Einschränkungen werden unmittelbar kommuniziert.

Sollten von Ihnen Fehlermeldungen oder weitere Anfragen zur Unterstützung bei der Nutzung gestellt werden, kann dies sowohl telefonisch als auch via Mail erfolgen.
So erhalten Sie (falls nicht anderweitig vereinbart) spätestens nach 36 Stunden nach Ihrer Anfrage eine erste Rückmeldung von uns. Ausgenommen sind hier Wochenenden und Feiertage.
Die telefonische Erreichbarkeit beschränkt sich auf die regulären Arbeitszeiten. Sollten wir telefonisch einmal nicht erreichbar sein, rufen wir in der Regel zurück. Die Anfrage sollte in diesem Fall jedoch am bessten nochmal via Mail gestellt werden. Die entsprechenden Kontaktdaten sind unten zu finden.

Die allgemeine Bereitstellung der Anwendung erfolgt für mindestens 9-12 Monate.

7.4. Störungs, Änderungs, Sicherheitslücken oder weitere Meldungen

Abhängig vom Meldungsgrund, verwenden wir unterschiedliche Wege zur Information.

- Statusseite:

  Wir bieten eine Status Seiteite www.aygonet.de/status an. Auf dieser können aktuelle und bekannte Statusmeldungen gefunden werden. Zudem werden wir diese um entsprechende Informationen und Hintergründe ergänzen. Diese Form wird sowohl für geplante als auch für ungeplante Ereignisse genutzt.

- E-Mail

  Einen direkten Kontakt via E-Mail suchen wir beispielweise bei Sicherheitslücken, welche eine Dokumentation des Vorgangs bedürfen.

- Beratungsstellen PopUp / Admin Mail

  Geplante Wartungszeiten oder andere planbare Ereignisse, kündigen wir frühzeitig an. Hierbei erfolgt eine Meldung an alle Administrator*innen. Eine Meldung an Klient*innen einer Beratungsstelle, muss dann jedoch durch die Beratungsstellenadministration erfolgen.

7.5. Technisch und organisatorische Maßnahmen

Unsere technischen und organisatorischen Maßnahmen erhalten Sie gerne auf Anfrage

7.6. AV Vertrag

Den AV Vertrag stellen wir als AYGOnet GmbH zur Verfügung. Bei Annahme eines Angebots, stellen wir diesen aus und starten einen digitalen Prozess zur Gegenzeichnung. Einen entsprechenden Entwurf, erhalten Sie auf Anfrage.

8. Zertifizierungen & Prüfung durch Dritte

8.1. Zertifizierungen

- ISO 27001 Zertifizierung des Rechenzentrums
- Zertifizierung nach dem Standard GDD-cert.EU der Datenschutzbeauftragten
- Zertifizierung Datenschutzbeauftragter (TÜV) durch PersCert TÜV unseres Datenschutzkoordinatoren

8.2. Pentests

Durchführendes Unternehmen	**Prüfart und geprüfte Inhalte**	**Datum**
TÜV TRUST IT GmbH	Graybox Pentest | Module: Core, Mail, Intern	Q3 2022

8.3. Datenschutzprüfung

Durchführendes Unternehmen	**Geprüfte Inhalte**	**Datum**
SCO-CON:SULT GmbH	Module: Core, Mail, Intern	Q3 2022

9. Verantwortliche und Dienstleister

9.1. Dienstleister

- **Databay AG** (Technische Betreuung und Entiwcklung)
  Jens-Otto-Krag-Straße 11, 52146 Würselen/Aachen
  info@databay.de | www.databay.de

- **Die Medialen GmbH** (Vertireb, Support, Verwaltung und Projektmanagement)
  Colmantstraße 39, 53115 Bonn
  info@aygonet.de | www.aygonet.de

- **RelAix Networks GmbH** (Hosting)
  Auf der Hüls 172, 52068 Aachen
  info@relaix.net | www.relaix.net

9.2. Standorte

Alle Unternehmensstandorte, Dienstleistungen und das Hosting (solange dies durch uns gestellt wird) erfolgen innerhalb Deutschlands. Ein geplanter Transfer der Daten in Drittstaaten vor allem in solche, die nicht unter die Regelungen der DSGVO fallen, findet nicht statt. Die genauen Standorte der Dienstleister oder der AYGOnet GmbH finden Sie in den entsprechenden Abschnitten.

9.3. Verantwortliche

AYGOnet GmbH
Herr Bernd Jacob
Colmantstraße 39 | 53115 Bonn
info@aygonet.de | www.aygonet.de

9.4. Datenschutzbeauftragter / -koordinator

9.4.1. Datenschutzbeauftragter

SCO-CON:SULT GmbH

Herr Lukas Biniossek

Hauptstraße 27 | 53604 Bad Honnef

datenschutz@aygonet.de | www.sco-consult.de

9.4.2. Datenschutzkoordinator

Die Medialen GmbH

Herr Lukas Oettinghaus

Colmantstraße 39 | 53115 Bonn

datenschutz@aygonet.de | www.aygonet.de

10. Kontakte

- Vertrieb: info@aygonet.de | +49 228 90822 22
- Support: support@aygonet.de | +49 228 90822 277

[Stand: 09.11.2022]