AYGOnet
Sicher beraten

Sicherheit & Datenschutz bei AYGOnet

Inhaltsverzeichnis

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.

In AYGOnet verbinden wir einen starken und verlässlichen Schutz der Beratungen mit einer intuitiven und sorgenfreien Handhabung. Damit Sie sich voll und ganz auf Ihre Beratungen konzentrieren können, haben wir eine Vielzahl von Maßnahmen ergriffen.

Im Folgenden möchten wir Ihnen einen Überblick über die getroffenen Maßnahmen zum Datenschutz und der Datensicherheit 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 bei der Wahl einer solchen Anwendung mit einbeziehen?

Ja – wir empfehlen die verantwortliche Person mit entsprechender Expertise dringend miteinzubeziehen. 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 beispielsweise 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 (mit 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.

Den Kern der Verschlüsselung innerhalb von AYGOnet stellt das Public-Private-Key Verfahren. Aufgrund der Architektur der Anwendung, werden unterschiedliche Schlüsselpaare verwendet welche folgend genauer beschrieben werden.

Neben dem Public-Prvate-Key Verfahren, wird natürlich auch die obligatorischen TSL (weitläufig als SSL bekannt) Verschlüsselung eingesetzt.

3.1. Account-, Beratungsstellen- und Kommunikations-Verschlüsselung

Für die verschlüsselten Inhalte der Beratungsstelle, der Nutzerdaten, Evaluationsdaten, der Mail Beratung sowie für die interne Kommunikation, wird auf ein Public-Private-Key Verfahren gesetzt. 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 werden.

Bei der Registrierung eines neuen Accounts, wird immer ein persönlicher und ein öffentlicher Key erstellt. Eine versendete Nachricht, sowie der Titel, der Anhang und die Nachricht eines Termins, werden also

immer mit dem Public-Key des versendenden und empfangenden Accounts verschlüsselt. Die / der Empfänger*in, kann den Inhalt dann mit dem eigenen Private-Key wieder entschlüsseln.

Um den Komfort einer sicheren Verschlüsselung zu gewährleisten und die Nutzer*Innen nicht mit dem Key-Management zu belasten, werden die Keys verschlüsselt in die Datenbank der Beratungsstelle abgelegt. Um dennoch zu gewährleisten, dass Inhalte nie unverschlüsselt abliegen, wird dieser Prozess um Verschlüsselte PHP Sessions ergänzt. Daraus ergeben sich folgende Verschlüsselungsschichten.

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

Eine grafische Darstellung der Verschlüsselungsschichten, kann dem Schaubild unter Punkt 11.1.1 entnommen werden. Ebenfalls darin enthalten, eine Darstellung, zur Verdeutlichung der Verschlüsselung der Data-at-Rest.

3.1.1. 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.

3.1.2. 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.

3.1.3. 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 diese sich regelmäßig – bei jedem Login ändern.

3.1.4. 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 6.1.

3.1.5. Schlüsselpaar erneuern

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

Im Falle des folgend beschriebenen Beratungsstellenschlüssels (vgl. Punkt 3.1.6) kann dies jedoch nur über die AYGOnet GmbH erfolgen. Dies führ aber dazu, dass Inhalte, die bisher mit dem Beratungsstellenschlüssel verschlüsselt wurden, nicht mehr entschlüsselbar sind. Aus diesem Grund sollte dies nur im äußersten Notfall erfolgen.

3.1.6. 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.

Aber auch in Teamberatungsstellen, in welchen alle Berater*Innen alle Verläufe lesen können sollen, gibt es den Bedarf einer Bereitstellung, die über die involvierten Parteien hinausgeht.

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*n Berater*in wird diese Verschlüsselung jedoch zwischen den beiden Gesprächspartner*innen hergestellt und eine Verschlüsselung mit dem Beratungsstellenschlüssel erfolgt nur noch im Fall einer Teamberatungsstelle.

Der Beratungsstellen-Private-Key steht allen Berater*innen zur Verfügung um solche empfangenen Nachrichten zu entschlüsseln. Dieser Schlüssel bzw. das zugehörige Passwort zur Entschlüsselung wird jedoch für jeden einzelnen Account mit dem eigenen Private-Key verschlüsselt abgelegt.

3.1.6.1. Besonderheiten

Wie alle Schlüssel, liegen auch die Beratungsstellenschlüssel verschlüsselt in der Datenbank. Die AYGOnet GmbH hat also keinen Zugriff auf die Schlüssel. Die Verteilung der Zugriffe auf diesen Schlüssel erfolgt stets über den administrativen Zugang einer Beratungsstelle. So wird das Passwort für diesen Key beispielweise im Zuge der Freischaltung von Berater*innen weitergeleitet. Es ist daher wichtig, dass mindestens ein Administrator*in handlungsfähig bleibt. Im Falle eines Passwortverlusts, können diese analog zu den Berater*innen einen QR Code zur Wiederherstellung verwenden. Sollte dieser nicht vorliegen, erfolgt eine Übergabe des Passworts von Berater*in an den/die Administrator*in im Sinne eines 4-Augen-Prinzip durch Nennung eines Freigabecodes auf der einen und Eingabe dessen auf der anderen Seite. Den Genauen Prozess, können Sie den Handbüchern entnehmen.

3.1.7. Dateiablage, Versendete Dateien & Sprachnachrichten

Im Beratungsverlauf haben Berater*innen und je nach Beratungsstelleneinstellung auch die Klient*innen die Möglichkeit, Dateien und Sprachnachrichten 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.

Auch Dateien in der Dateiablage, werden über diesen Weg synchron verschlüsselt abgelegt. Das Passwort wird anschließend mit dem Key der Beratungsstelle verschlüsselt abgelegt. Dieser Key steht allen Berater*innen und Administrator*innen zur Verfügung.

Beim Versand einer Datei oder Sprachnachricht wird ein zufälliges Passwort erzeugt, mit welchem die Datei (bzw. im Fall der Dateiablage das zugehörige Passwort) verschlüsselt wird. Dieses Passwort wird der Nachricht mitgegeben. Nachricht und Dateipasswort werden dann wie gewohnt mit dem Private-Key verschlüsselt.

Empfänger einer Nachricht haben keinen direkten Zugriff auf das Passwort. Beim Aufruf (und Entschlüsselung der Nachricht) wird dies vom System zur Bereitstellung der Datei verwendet.

Anhänge an Terminen werden gleichermaßen verschlüsselt. Ist der Termin öffentlich, wir die Datei mit einem allgemeinen (nicht Personen bezogenen) Key verschlüsselt. So bleiben alle Anhänge immer verschlüsselt, stehen den Ratsuchenden jedoch weiter zur Verfügung.

Wichtig: Dies betrifft nur über die Mailberatung bzw. interne Kommunikation versendete Dateien und Sprachnachrichten. Nicht aber z.B. Profilbilder. Hierzu mehr unter Punkt 3.4.2.

3.2. Protokoll-Verschlüsselung

Die Chats bieten die Möglichkeit, Protokolle zu erstellen. Diese Protokolle werden lokal erzeugt und verschlüsselt abgelegt. Damit die Berater*Innen diese im Nachgang wieder einsehen können, kommt auch hier ein dediziertes Schlüsselpaar zum Einsatz.

Da diese Schlüssel lediglich für die Protokolle verwendet werden, benötigen nur Berater*Innen und Administrator*Innen entsprechende Schlüssel. Ratsuchenden stehen diese Schlüssel nicht zur Verfügung.

Beim Betreten des Chats wird der Public Key des/der Berater*In geladen und zur Verschlüsselung des Protokolls verwendet. Wird das Protokoll im Nachgang aufgerufen, wird neben dem verschlüsselten Protokoll auch der synchron verschlüsselte Private Key des/der Berater*in heruntergeladen. Die Eingabe des Passworts entschlüsselt dann den Private Key und dadurch auch das Protokoll. Die Entschlüsselung des Private Keys und des Protokolls erfolgen nur im Browser. Entschlüsselte Inhalte verlassen so nie den lokalen Browser des Nutzers.

Im Protokoll sind neben den Nachrichten auch alle Metadaten enthalten und verschlüsselt. Das Protokoll selbst gibt lediglich Aufschluss über den Termin und ggf. den Sprechzimmernamen.

Protokolle können nur erstellt werden, wenn die Protokollverschlüsselung zuvor aktiviert wurde.

Mehr zum Protokoll unter Punkt 3.2.

3.2.1. Schlüsselpaar erstellen

Um Protokolle erstellen und anschließend aufrufen zu können, muss ein entsprechendes Schlüsselpaar (RSA-OAEP mit SHA-256) erstellt werden. Dies kann in den Kontoeinstellungen erfolgen. Hierzu muss ein Passwort zur Verschlüsselung des Keys hinterlegt werden. Dieses Passwort folgt den allgemeinen Passwortregeln der Beratungsstelle (vgl. Punkt 4.3.1). Stellen Sie sicher, dass Sie dieses Passwort sicher aufbewahren. Ohne dieses, können alte Protokolle nicht mehr geöffnet werden. Auch ein Passwortwechsel ist nur mit diesem Passwort möglich.

In der Datenbank finden sich dann der mit dem Passwort verschlüsselte Private Key und der unverschlüsselte Public Key. Das Passwort selbst wird zu keiner Zeit gespeichert.

3.2.2. Passwort Reset

Das Passwort der Protokoll-Schlüssel kann jederzeit in den Kontoeinstellungen geändert werden. Dies ist jedoch nur möglich, wenn das alte Passwort bekannt ist. Ist dieses nicht bekannt, bleibt nur die Möglichkeit, das Schlüsselpaar zu erneuern. Zuvor verschlüsselte Protokolle sind dann nicht mehr einsehbar.

3.2.3. Schlüsselpaar erneuern

Im Falle des Protokoll-Schlüssels erfolgt die Erneuerung in den Kontoeinstellungen. Wird ein neuer Schlüssel erstellt, führt dies jedoch dazu, dass alte Protokolle nicht mehr geöffnet werden können. Alte Protokolle werden somit nicht neu verschlüsselt.

3.2.4. Gültigkeitsdauer des Schlüsselpaars

Die Schlüsselpaare sind tendenziell unbeschränkt gültig. Wird das Modul der Chatberatung jedoch deaktiviert, erfolgt die Löschung der Keys mit einer Latenz von 2 Monaten.

3.3. Chat- & Video-Verschlüsselung

Die Verschlüsselung innerhalb eines Chats und eines Videogesprächs erfolgt ebenfalls mittels eines Public-Private-Key Verfahrens. Im Gegensatz zu den vorrangegangenen Schlüsselpaaren, werden die Schlüsselpaare hier lokal und nur temporär jeweils bei Beginn des Gesprächs erzeugt.

Da diese Cluster darüber hinaus losgelöst voneinander und von der Beratungsstelle selbst sind (vgl. Punkt 4.1.1.2) findet auch kein Austausch von schlüsseln oder ähnliches statt.

Eine dauerhafte Speicherung von Inhalten, Chats, Streams außerhalb der Chat-Protokolle erfolgt nicht.

3.3.1. Chat-Verschlüsselung

Unter Einsatz von temporäre Schlüsselpaaren (ECDH mit einer P-256-Kurve), welche lokal für den Zeitraum des Chats erstellt werden, verfügt die Chat Beratung über eine vollwertige Ende-zu-Ende Verschlüsselung.

Da es sich nur um temporäre und keine dauerhaften Schlüssel handelt, die schon beim Re-Load der Seite neu generiert werden, sind einige der zuvor thematisierten Punkte, wie der Passwort Reset, hier obsolet.

Die so generierten Schlüssel verschlüsseln die komplette Kommunikation inklusive aller Anhänge. Lediglich die Meta-Daten, die zur Verarbeitung benötigt werden, verbleiben unverschlüsselt (mehr unter Punkt 3.4.2).

Ein Schlüsselaustausch findet beim Betreten des Chats statt. Nach dem Erstellen des Schlüsselpaars, wird der Public-Key per Websocket an den Chat-Cluster gesendet und von dort via Broadcast an alle Teilnehmer*Innen verteilt. Für später beitretende Teilnehmer*Innen werden die Public Keys im Zwischenspeicher des Chat-Clusters vorgehalten.

3.3.2. Video-Verschlüsselung

Die Video-Beratung kann durch eine Ende-zu-Ende Verschlüsselung geschützt werden. Diese muss beim Betreten eines Raumes jedoch derzeit noch initial gestartet werden.

Die Verschlüsselung erfolgt auf Basis der „WebRTC Insertable Streams“ API (Inklusive dem DTLS-SRTP Protokoll).

Ähnlich wie bei der Chat Beratung, werden beim Betreten des Gesprächs temporäre Schlüssel erstellt und mit den anderen Teilnehmern ausgetauscht.

Bei der Verwendung von Insertable Streams für Ende-zu-Ende-Verschlüsselung werden die Daten in kleine Blöcke aufgeteilt, die einzeln verschlüsselt und in den Datenstrom eingefügt werden. Auf diese Weise können die Daten sicher übertragen werden, da sie nur von autorisierten Parteien entschlüsselt werden können.

3.4. Weitere Informationen zur Verschlüsselung

3.4.1. 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 (derzeit) nur bei der Chat- und Videoberatung (s.u.), nicht aber der Mailberatung, von einer echten Ende-zu-Ende Verschlüsselung sprechen.

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), was jedoch nur möglich ist, wenn der Key lokal generiert oder 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 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 stets mit mindestens einer Verschlüsselungsschicht (z.B. TLS oder die verschlüsselte PHP-Session).

In 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 zu gegebener Zeit angekündigt.

Chat- und Videoberatung. In der Chat- und Videoberatung erfolgt die komplette Kommunikation über eine Ende-zu-Ende-Verschlüsselung. Dies betrifft auch die Chat-Protokolle.

In Falle der Chat- und Videoberatung wird beim Betreten des Raumes ein temporäres Schlüsselpaar erstellt. Die öffentlichen Schlüssel werden dann mit allen Teilnehmern geteilt. Der Schlüssel wird also für ein Gespräch erstellt, zwischen den Gesprächspartner*innen ausgetauscht und verfällt bei Beendigung des Gesprächs wieder (vgl. Punkt 3.3).

Lediglich die Metadaten der Nachrichten werden während des Gesprächs ausschließlich über eine TLS Verbindung verschlüsselt. Diese werden zur Zustellung der Inhalte benötigt (vgl. Punkt 3.4.2)

Im Falle der Protokolle sind auch diese verschlüsselt. Hier verbleiben allein Metadaten des Raumes unverschlüsselt.

3.4.2. Was ist NICHT verschlüsselt?

Es gibt Daten, die unverschlüsselt in der Datenbank stehen bzw. ohne zusätzliche Verschlüsselung übertragen werden. Zumeist handelt es sich um Systeminformationen / -einstellungen. Doch auch die Metadaten der Gesprächsverläufe sowie einzelne systemrelevante Nutzungsdaten. Eine TLS/SSL Verschlüsselung und die weiteren Sicherheitsmaßnahmen der Anwendung, schützen natürlich auch diese Daten. Eine Liste finden Sie hier:

- Account und Kommunikations-Verschlüsselung
    - Accountname, Rolle, Mailadresse
    - Alle Beratungsstellen-Settings
    - Mail Metadaten wie Uhrzeit, Teilnehmer*innen
    - Kategorien
    - Profilbilder und Logos
    - Termin Metadaten: Datum, Uhrzeit, Teilnehmer, Zu- bzw. Absagen.
- Protokoll-Verschlüsselung
    - Terminname & Ggf. Sprechzimmername
    - Zugehörige Beratungsstelle
- Chat-Verschlüsselung*
    - Chat-Metadaten
        - Link zum Profilbild
        - Uhrzeit des Chatbeitritts
        - Anzeigename (im Falle von eingeloggten Usern auch der Nutzername) der Sender*Innen und der Empfänger*Innen
        - Termintitel und ggf. Sprechzimmername
- Video-Verschlüsselung*
    - Video-Metadaten
        - Link zum Profilbild
        - Uhrzeit des Chatbeitritts

- Anzeigename (im Falle von eingeloggten Usern auch der Nutzername) der Sender*Innen und der Empfänger*Innen
- Termintitel und ggf. Sprechzimmername

– Evaluation-Verschlüsselung
  – Evaluations-Metadaten
    - Name der teilnehmenden Personen
    - Zeitpunkt der Beantwortung

*Diese Daten werden nicht dauerhaft gespeichert. Sie werden ausschließlich für die Zeit des Chats benötigt. Mit Verlassen des Chats bzw. spätestens mit Schließen dessen, werden diese Daten gelöscht.

4. Sicherheit der Daten

4.1. Server- und Datenbanksicherheit

4.1.1. Datentrennung

Im Sinne der Verfügbarkeit, Risikominimierung und der Mandantentrennung sind unsere Systeme auf unterschiedlichen Ebenen getrennt.

4.1.1.1. Beratungsstellen

Im Bereich der Beratungsstellen, trennen wir das System in zwei Ebenen. Die Ressorts und die einzelnen Beratungsstellen.

Ein Ressort enthält 20-50 unterschiedliche Beratungsstellen. Die Beratungsstellen eines Ressorts teilen sich einen Docker-Stack. Durch die Trennung der Beratungsstellen in kleine Gruppen erhöhen und verbessern wir die Verfügbarkeit, Belastbarkeit und die Wiederherstellbarkeit.

Jede Beratungsstelle hingegen verfügt über eine eigene Datenbank inklusive eigenem Datenbanknutzer, auf die nur aus dem jeweiligen Docker-Stack zugegriffen werden kann. Zudem wird jeder Beratungsstelle

ein eigener Upload-Ordner bereitgestellt. So erreichen wir eine starke Mandantentrennung und können die Zugriffe im Sinne der Zugriffskontrolle auf Inhalte einer Beratungsstelle auf diese reduzieren.

Um die Verfügbarkeit sicherzustellen sind die Entwicklungs- und Testsysteme darüber hinaus von den Produktivsysteme getrennt.

4.1.1.2. Chat- bzw. Video-Cluster

Die Chat- und die Videoanwendung sind darüber hinaus komplett ausgelagert und stellen je ein eigenes Cluster da. Die Gespräche aller Beratungsstellen laufen über diese dedizierten Cluster. Neben der technischen Infrastruktur liegen hier (im Falle des Chat-Clusters) zusätzlich die Protokolle.

Räume und Sprechzimmer erhalten eine zufällige ID inklusive einer Referenz auf die zugehörigen Räume bzw. die Lobby, wodurch keine Rückschlüsse auf Beratungsstellen und Themen möglich sind.

Chat-Protokolle: Für jeden Raum / jedes Sprechzimmer wird ein eigener Ordner angelegt. In diesem Ordner, erhält jede*r Berater*In, der/die ein Protokoll in diesem Raum / Sprechzimmer erstellt, einen eigenen Unterordner. In diesen werden dann die verschlüsselten Protokolle abgelegt. Diese Ordner sind von außen nicht erreichbar.

4.1.2. Datensparsamkeit

Wir sammeln keine Daten, die nicht für den Betrieb notwendig sind. Dazu zählen 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 Nutzername und ein Passwort zwingend benötigt. Berater*innen und Administrator*innen benötigen darüber hinaus noch eine eigene Mailadresse. Neben den angegebenen Informationen, wird auch das Registrierungsdatum vermerkt. Alle weiteren

Vorgaben und Anforderungen an die Registrierung werden durch die Beratungsstelle selbst getroffen. So ist beispielsweise die zwingende oder optionale Angabe einer Mailadresse für Klient*innen durch die Beratungsstelle aktivierbar. Im Gegensatz dazu, kann die Beratungsstelle aber auch auf „Anonym" gesetzt werden. Dies nimmt den Ratsuchenden die Möglichkeit der freiwilligen Eingabe solcher Daten in den Kontoeinstellungen.

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. Das Logging umfasst drei Logs, die jeweils für 14 Tage gespeichert werden und keine personenbezogenen Daten beinhalten.

- Fatal-Error-Log → Logt schwerwiegende Fehler, welche die Nutzung der Anwendung stark einschränken oder verhindern. Enthalten sind ein automatisch generierter Fehlercode sowie Ort und Aktion, die zu dem Fehler führten.

4.2.4. Metadaten

Nachrichten in Chat und Mail gehen immer auch mit Metadaten einher, die für die Zustellung und den Ordnungsgemäßen Betrieb notwendig sind und mit den Nachrichten gespeichert werden. Zu Metadaten gehören z.B. die Informationen:

- Sender / Empfänger
- Datum und Uhrzeit des Sendens
- Zugehöriger Beratungsverlauf / Chatraum
- Gelesen / Ungelesen Status der Nachricht

4.2.5. Chat- und Video-Gespräche

Alle Chats und Video-Gespräche sind flüchtig. Es findet außerhalb der Protokolle (vgl. Punkt 3.2) keine Speicherung der Chat- und Videoinhalte statt. Die verschlüsselten Inhalte nutzen den Cluster lediglich als „Zusteller".

4.2.6. Basis Statistik

Beratungsstellen haben immer eine aktive „Basis Statistik". Diese gibt eine auf Metadaten beruhende Information über die Aktivität innerhalb der Beratungsstelle. Zu den Daten gehören Informationen über die Menge der Neu-Registrierungen, Nachrichten oder Terminen. Diese Daten enthalten keinen Personenbezug.

4.2.7. Evaluationsdaten

Mit Hilfe des Evaluations-Moduls können Beratungsstellen auf Wunsch Fragebögen erstellen und an unterschiedlichen Orten ausspielen lassen. Ob und welche Daten erfasst werden, liegt einzig im Ermessen des/der Betreiber*in der Beratungsstelle. AYGOnet hat keinen Zugriff auf die gesammelten Evaluationsdaten, da die so gesammelten Antworten immer mit den zugehörigen Keys verschlüsselt sind.

Die so gesammelten Daten können abhängig von der Konfiguration der Fragebögen einen Personenbezug haben.

4.3. Zugriffskontrolle (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 („Sonderzeichen“?)

Diese Anforderungen können auf schriftliche Anfrage durch die Beratungsstelle reduziert werden. So lässt sich unter anderem die Mindestlänge reduzieren oder erhöhen. Darüber hinaus können bis zu zwei der der anderen Anforderungen deaktiviert werden.
Eine Reduzierung der geforderten Passwortstärke ist jedoch nicht zu empfehlen und sollte nur dann erfolgen, wenn die Passwortanforderungen eine zu große Hürde für die Zielgruppe darstellen und somit eine Teilhabe an dem Angebot stark erschwert wird.

4.3.2. Login / Nutzernamen

Nutzernamen müssten eine Mindestlänge von 6 Zeichen besitzen. Sie dürfen aus Groß-, und Kleinbuchstaben, sowie Zahlen bestehen. Leerzeichen und Sonderzeichen sind nicht erlaubt.

Nutzernamen müssen beim Login immer in der Form angegeben werden, wie Sie bei der Registrierung hinterlegt wurden. Somit ist beim Login auf die gewählte Groß- und Kleinschreibung zu achten.
Diese Anforderung kann auf schriftliche Anfrage deaktiviert werden, so dass eine Prüfung der Groß- und Kleinschreibung des Nutzernamens nicht mehr durchgeführt wird.
Da eine Reduzierung dieser Anforderung, die Sicherheit des Logins reduziert, empfehlen wir diesen Schritt nur zu gehen, wenn die Prüfung der Groß-, und Kleinschreibung eine zu große Hürde für die Zielgruppe darstellen und somit eine Teilhabe an dem Angebot stark erschwert wird.

Die Nutzung der möglicherweise hinterlegten E-Mail-Adresse für den Login ist nicht möglich. Lediglich zum Zurücksetzen des Passworts kann diese genutzt werden. Eine Auskunft über den Nutzernamen über die E-Mail-Adresse erfolgt systemseitig ebenfalls nicht.

4.3.3. 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. Ressortadministrator*innen können dies auch nicht deaktivieren.

Den administrativen Rollen der Beratungsstelle ist eine Deaktivierung jedoch möglich, wenn auch nicht empfohlen.

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.

4.3.4. Session TimeOut

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

4.3.5. Gültigkeit der Systemlinks

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

4.3.6. 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 davon unberührt.

- 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

4.4. Modul Spezifika

Einige der zur Verfügung stehenden Module bringen Besonderheiten mit sich. Diese sollen in diesem Kontext genauer betrachtet werden.

4.4.1. Chat- & Video-Modul

Wie zuvor beschrieben, befinden sich die Chat- und Video-Module auf je einem eigenen Cluster. Beide haben eine dedizierte und von den anderen dauerhaften Schlüsseln getrennte Verschlüsselung. Zusätzlich gibt es die Protokollfunktion. Die über die zuvor genannten Informationen hinausgehenden Punkte sollen hier thematisiert werden.

4.4.1.1. Chat / Video-Termine

Wie unter Punkt 3.3 beschrieben verfügen die Chat- und die Video-Beratung über eine vollwertige Ende-zu-Ende Verschlüsselung, bei welcher die Server nur als Broadcast für die verschlüsselten Nachrichten und die Public Keys dienen. Auf den Servern findet (außerhalb der verschlüsselten Chat-Protokolle – vgl. Punkt 3.2) keine Speicherung der Nachrichten statt.

- Bei Terminen mit Buchung, können optional E-Mail-Adressen angegeben werden. Diese wird verwendet um die Anmeldung zu bestätigen, den Termin Link zu übermitteln und bei Bedarf über eine Absage zu informieren. Die E-Mail-Adresse wird in der Datenbank der Beratungsstelle abgelegt vom System verarbeitet und ist weder für Berater*Innen noch Administrator*Innen sichtbar. Bei Ratsuchenden, die nicht eingeloggt sind, erfolgt auch keine Verknüpfung zu möglichen bestehen Konten.
  Die Löschung erfolgt unter folgenden Bedingungen – abhängig davon, welche Bedingung zuerst eintritt.
  - nach Terminende
  - nach Deaktivierung des Chat- / Video-Moduls (mit Latenz)
  - bei Löschung der Beratungsstelle
- Betreten Ratsuchende oder Berater*Innen den Chat, nachdem bereits eine Unterhaltung erfolgte, werden diese Nachrichten an die neuen Teilnehmer*Innen verteilt. Dies erfolgt über eine*n andere*n Nutzer*in im Chat, welche*r als Broadcast fungiert. Neuen Ratsuchenden erhalten so die letzten 5 Minuten und Berater*Innen die komplette bisherige Kommunikation des betretenen Raums.

4.4.1.2. Chat- / Video-Server

Es gibt nur eine Einweg-Kommunikation. Die Cluster / Beratungsstellen können zum Chat- /Video-Cluster kommunizieren, um so z.B. Nutzernamen, Termininformationen und ähnliches zu übergeben. Eine Kommunikation in die andere Richtung, von diesen Media-Clustern zur Beratungsstelle gibt es nicht.

Neben den Termindaten werden beim Aufruf eines Chats / Video Gesprächs noch folgende Daten übermittelt.

- Authentifizierung „Token“: Auf Seiten der Beratungsstelle wird ein Token erzeugt. Mit diesem werden dann die Metadaten zum Chat übertragen und der User verifiziert.
  - Profilbild URL (nur bei Chat)
  - Pub-Key für Protokoll (nur bei Berater*innen im Chat)

- Textbausteine (nur bei Chat)
- Name

4.4.1.3. Chat-Protokolle

Innerhalb des Chats können Protokolle erstellt werden. In der Lobby ist die Protokollierung immer aktiviert. Sprechzimmer hingegen haben einen vertraulicheren Charakter: hier werden die Protokolle nur nach Zustimmung der Teilnehmer geschrieben. Beim Schließen eines Sprechzimmers wird geprüft, ob alle beteiligten Personen eine Zustimmung abgegeben haben. Ist dem so, wird das Protokoll gespeichert. Fehlt mindestens eine Zustimmung, gibt es kein Protokoll. Ob ein Protokoll aktiv ist, kann auch im Chat nachvollzogen werden.

Die Protokolle werden dann für jede*n Berater*In erstellt und mit dem persönlichen Protokollschlüssel verschlüsselt abgelegt. Das Protokoll eines Raumes liegt also so oft vor, wie Berater*Innen an der Kommunikation teilgenommen haben. Das verschlüsselte Protokoll wird in einer .txt-Datei (base64 encoded) und ohne auslesbare Schlüsselinfos oder sonstige Metadaten abgelegt.

WICHTIG: Protokolle werden nur erzeugt, wenn die beteiligten Berater*Innen einen Protokollschlüssel erstellt haben.

Die Protokolle werden so lange vorgehalten, bis eine der folgenden Bedingungen eintrifft:

- manuelle Löschung durch Berater*Innen innerhalb der Beratungsstelle
  - Diese Löschung muss jede*r Berater*In für das eigene Protokoll vornehmen
- Automatisiert, wenn das Chat-Modul deaktiviert wird (mit Latenz von 2 Monaten)
- Automatisiert mit Löschung der Beratungsstelle

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 Punkt 5.2.1 beschrieben behandelt und durch einen Cronjob nach 48 Stunden gelöscht. Die Löschung eines Berater*innen-Accounts setzt die Verschiebung der verknüpften Beratungsstränge an andere Berater*innen 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 Berater*innen 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 anschließend noch ein Jahr 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.

5.2.3. Protokolle

Protokolle bleiben per-se erst einmal unbegrenzt erhalten. Protokolle können jedoch über zwei Wege gelöscht werden:

1. Manuell in der Terminverwaltung des betroffenen Termins. Hier können alle Protokolle einzeln entfernt werden.
2. Automatisiert bei der Löschung der Beratungsstelle (wie oben beschrieben nach max. 48 Stunden) oder mit einer Latenz von 2 Monaten nach der Deaktivierung der Chatfunktion innerhalb der 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 die privaten Schlüssel, mit welchem die eigenen Beratungsverläufe verschlüsselt sind, durch das eigene Passwort verschlüsselt sind, kann dieser auch nur mit diesem entschlüsselt werden. Im Falle eines Passwortverlustes wäre somit eine Entschlüsselung mangels Zugriffes auf die Schlüssel nicht mehr möglich. Dies betrifft alle dauerhaften Schlüssel.

Um dieses Szenario in der „Account und Kommunikations-Verschlüsselung“ sowie der „Beratungsstellen Verschlüsselung“ 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. Ausgenommen hiervon sind Berater*innen in Teamberatungsstelle.

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 dem/n Berater*innen in Kontakt treten. Berater*innen haben dann die Möglichkeit, die Inhalte für die Klient*innen freizugeben (neu zu verschlüsseln). So kann eine / ein Klient*in sich zuvor erklären und so (nach Entscheidung der / des Beraters*in) wieder auf die alten Inhalte zugreifen.

Für die Protokoll-Verschlüsselung ist dieses Verfahren nicht möglich.

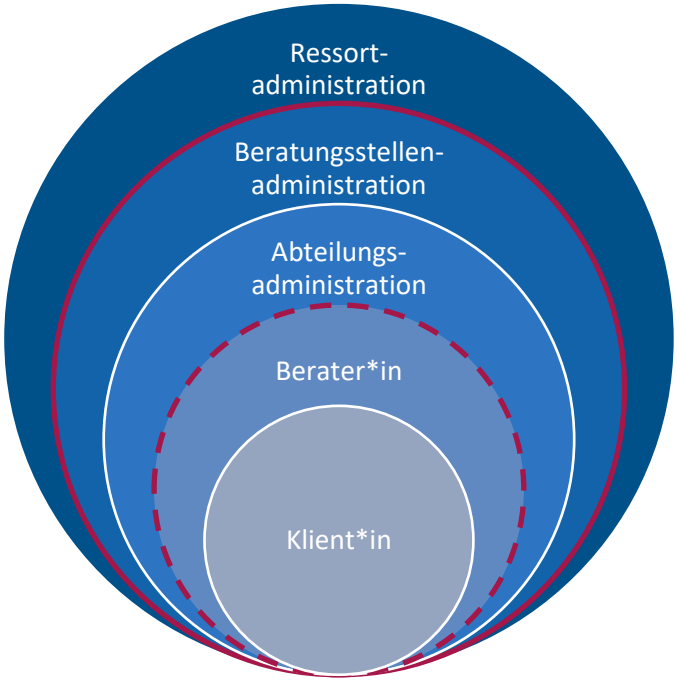
6. Wer darf was?

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. →



Dabei im roten gestrichelten Bereich jene Rollen, die Zugriff auf Beratungsinhalte haben. Alle anderen Rollen sind rein verwalterischer Ausrichtung.

6.1.1. Ressortadministration

An dieser Stelle werden alle Beratungsstellen eines Ressorts verwaltet. Es werden Beratungsstellen angelegt und bearbeitet. Zudem erhält diese Rolle einen stark reduzierten 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 bei der Anwendung darstellen.

Eine Verwaltung der Nutzer*innen und Gruppen sind für diese Ebene ebenso wenig möglich, wie die Einsicht in Beratungs- oder Evaluationsinhalte.

6.1.2. Beratungsstellen- / Abteilungs-Administration

Die Administration einer Beratungsstelle sowie einer Abteilung sind sich sehr ähnlich. 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 freizuschalten.

Wichtig ist zudem, dass die Administratoren Rolle keine Beratungen durchführen oder einsehen kann. 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 am längsten 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 administrativer Accounts.

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

Die Beratungsstellenadministration liegt immer in der Hand der Kundin / des Kunden. Eine Administration auf Beratungsstellenebene durch die AYGOnet GmbH erfolgt nicht.

6.1.3. Berater*innen

Accounts der Berater-Rolle haben stets nur Zugriff auf die eigenen Daten und die zugeordneten Klient*innen. Die Änderung der Daten Dritter ist in dieser 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.

Berater*Innen können darüber hinaus mit bis zu zwei von drei „Sub-Rollen“ versehen werden.

- Supervision: Supervisoren haben keine besonderen Rechte. Sie können in einer Regelberatungsstelle jedoch für bestehende Beratungen angefragt und hinzugezogen werden. Mehr unter Punkt 6.1.5.
- Berater*Innen mit Zuweisungsrechten: Diese Sub-Rolle erlaubt es neue Anfragen zuzuweisen. Diese Zuweisung muss von den Zugewiesenen jedoch zunächst bestätigt werden.
- Peer-Berater*Innen: Diese Sub-Rolle reduziert die Einsicht der Beratungsstränge auf die eigenen Beratungen (relevant in Teamberatungsstellen) oder den ihnen zugewiesenen neuen Anfragen.

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. Das Hinzuziehen 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 Freigabe der Beratungsverläufe erfolgt bevor die / der Klient*in eine Zustimmung 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 3.4.2 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 entsprechenden Zugang erstellen.

6.3. Schnittstellen / Dritte

Innerhalb von AYGOnet werden weder Schnittstellen zu Dritten noch Inhalte Dritter eingebunden. Neben den unten (Punkt 9.1) 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. Darüber hinaus liegt ein maßgeblicher 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 auf Anfrage und im persönlichen Gespräch jedoch eine Orientierungshilfe für die eigenen Datenschutzbestimmungen bereit. Da die Einstellungen je Beratungsstelle variieren können und wir keinen Einblick in den Umgang mit den Daten innerhalb einer Beratungsstelle haben, können wir keine allgemeingültige Datenschutzbestimmung für die Nutzung bereitstellen. Zur Erstellung sollten die in diesem Dokument bereitgestellten Informationen jedoch dienlich sein.

Beratungsstellen können den Livebetrieb zudem nur aufnehmen, wenn die Beratungsstellen eigene Bestimmungen (Text oder Link) hinterlegt haben.

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 anders 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 besten 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 Statusseite https://aygonet.de/status-der-anwendung 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 beispielsweise bei Sicherheitslücken oder länger anhaltenden ausfällen, welche einer 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. Technische und organisatorische Maßnahmen

Unsere technischen und organisatorischen Maßnahmen für alle Arbeiten innerhalb der AYGOnet GmbH erhalten Sie gerne auf Anfrage

Die jeweils gültige Version des Whitepapers deckt die technischen und organisatorischen Maßnahmen bezogen auf die Anwendung ab.

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. Dieser orientiert sich an den Standardvertragsklauseln der Europäischen Kommission vom 04.06.2021.
Abweichend von diesen Standardvertragsklauseln wurden unter 7.5 Anpassung in den Begrifflichkeiten vorgenommen. Ein Protokoll über diese und daraus resultierende Änderungen erhalten Sie auf Anfrage im Zuge der Vertragsprüfung.

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 Datenschutzkoordinators

8.2. Pentests

Durchführendes Unternehmen	Prüfart und geprüfte Inhalte	Prüfergebnis	Datum
TÜV TRUST IT GmbH	Graybox Pentest | Module: Core, Mail, Intern	Bestanden	Q3 2022
TÜV TRUST IT GmbH	Graybox Pentest | Module: Termin, Chat	Bestanden	Q3 2023

8.3. Datenschutzprüfung

Durchführendes Unternehmen	Geprüfte Inhalte	Datum
SCO-CON:SULT GmbH	Module: Core, Mail, Intern	Q3 2022
SCO-CON:SULT GmbH	Module: Termin, Chat	Q2 2023

9. Verantwortliche und Dienstleister

9.1. Dienstleister / Unterauftragnehmer

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

- Die Medialen GmbH (Buchhaltung)
  Colmantstraße 39, 53115 Bonn
  info@diemedialen.de | www.diemedialen.de

9.1.1. Hosting

Das Hosting stellt unser Dienstleister Databay AG in Form eines Housings.
Das Hosting erfolgt in einem ISO 27001 Zertifizierten Rechenzentrum in Deutschland bei der RelAix Networks GmbH (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

AYGOnet GmbH

Herr Lukas Oettinghaus

Colmantstraße 39 | 53115 Bonn

datenschutz@aygonet.de | www.aygonet.de

10. Kontakte

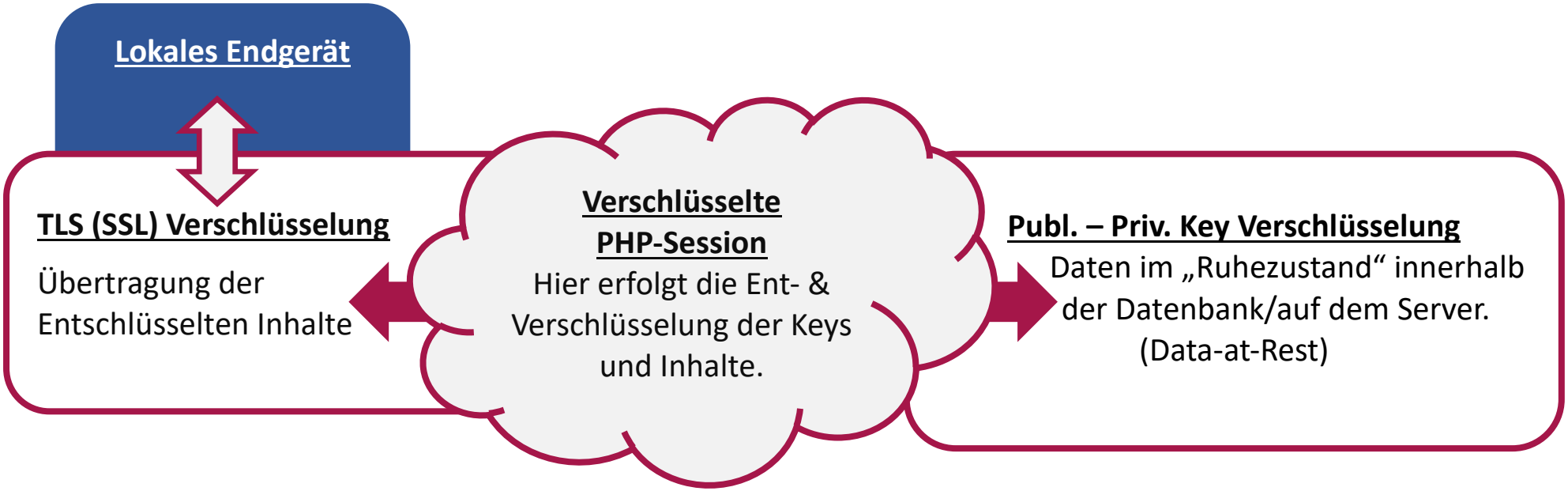
- Vertrieb: info@aygonet.de | +49 228 85 44 77 90
- Support: support@aygonet.de | +49 228 85 44 77 99

11. Anlagen

11.1. Schaubilder

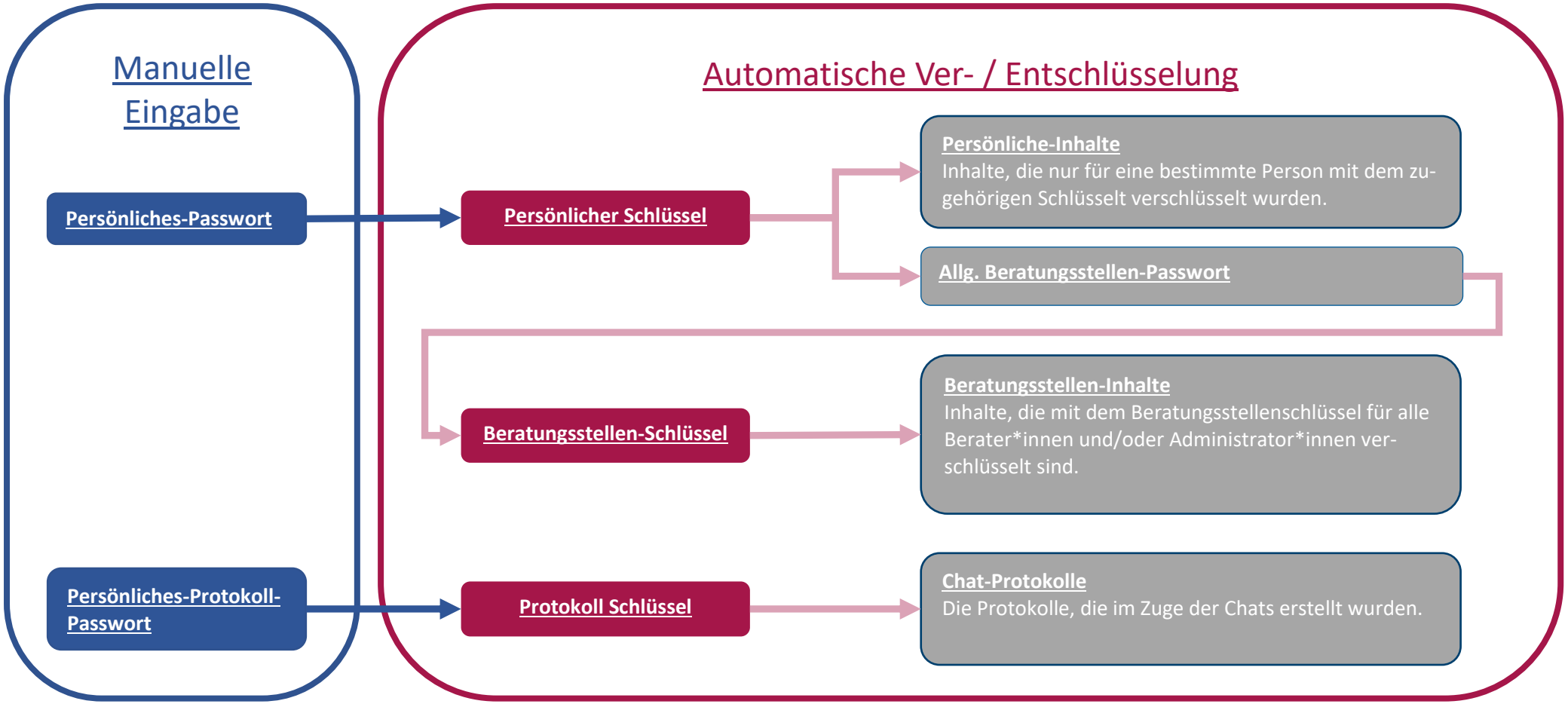
11.1.1. Account-, Beratungsstellen- und Kommunikations-Verschlüsselung (vgl. Punkt 3.1)

Data-in-Transit - Verschlüsselungsschichten

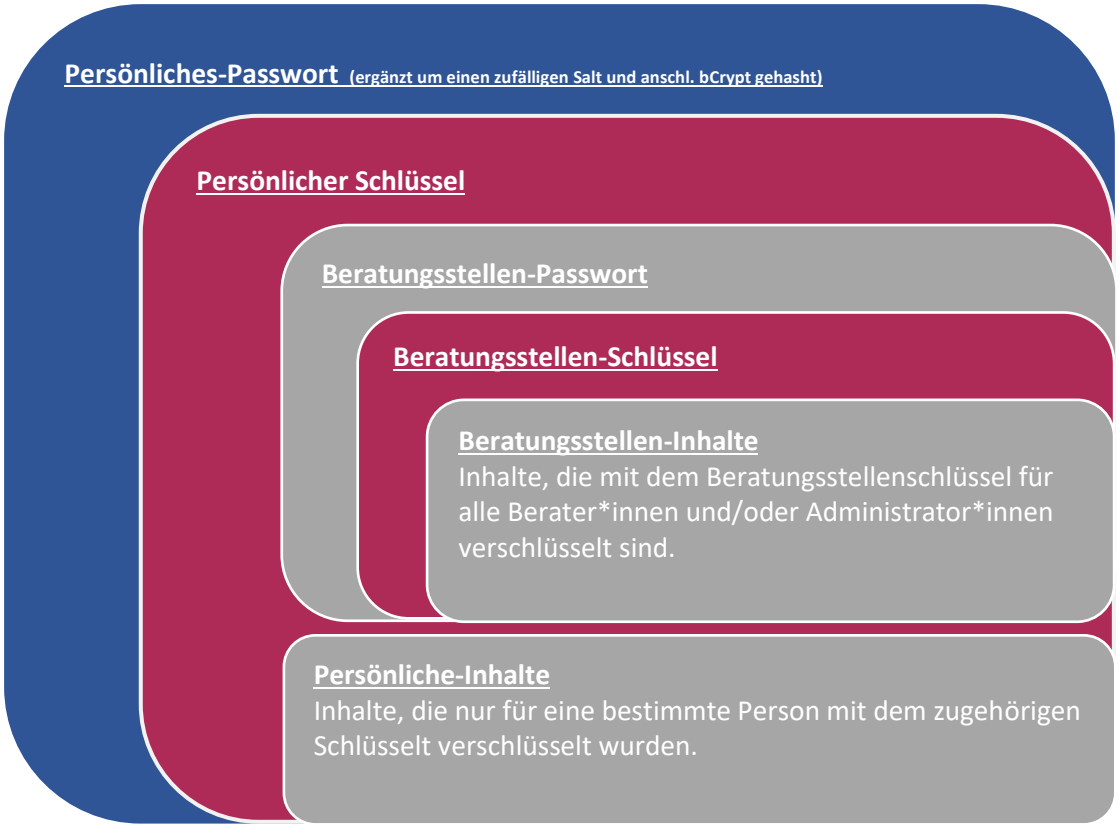


Data-at-Rest – Verschlüsselungsschichten

Die Inhalte (grau) werden mit den Keys (rot) der Empfänger verschlüsselt. Die Keys (rot) werden wiederum mit den Passwörtern mit einem Paswort+Salt-Hash AES-256-CBC verschlüsselt. Die Passwörter, werden dann ergänzt um einen Salt bCrypt doppelt gehasht, wobei eine Ebene bei jedem Login neu generiert wird.



Anders dargestellt, schützt also das persönliche Passwort alle Beratungsinhalte – Analog dazu funktioniert auch die Protokollverschlüsselung.



12. Änderungshistorie des Whitepapers

Im Folgenden sollen die Änderungen des Whitepapers protokolliert werden.
Dies soll der besseren Nachvollziehbarkeit nach Änderungen dienen.

- 04.10.2022
  - Initiale Veröffentlichung
- 09.11.2022
  - Optische und Inhaltliche fein Justierung zur Verbesserung des Verständnisses
- 10.05.2023
  - Optische und Inhaltliche fein Justierung zur Verbesserung des Verständnisses
- 23.06.2023
  - Ergänzung der Informationen zum Chat und Termin Modul
  - Ergänzung Prüfung durch Dritte für die Module Termin und Chat unter Punkt 8
- 03.08.2023
  - Ergänzen des Status zum aktuellen Graybox Test unter Punkt 8
- 13.02.2024
  - Anpassung der Dienstleister und Zuständigkeiten unter Punkt 9
- 04.06.2024
  - Ergänzung der Informationen zur Video-Beratung und Evaluation
  - Umstrukturierung des Menüpunkt 3 „Verschlüsselung“ zur besseren Verständlichkeit der unterschiedlichen Verschlüsselungsschichten
  - Ergänzung des Schaubilds zur Account-, Beratungsstellen- und Kommunikations-Verschlüsselung
  - Ergänzung des Schaubilds zur Rollen-Herachie
  - Neuplatzierung zur Information zum Stand des Dokuments
- 05.06.2024
  - Ergänzung des Prüfergebnisses unter Punkt 8.
  - Ergänzung des Punkt 12 Protokollierung der Anpassung innerhalb des Whitepapers
  - Anpassung der Dienstleisterkontaktdaten
- 15.05.2025
  - Ergänzung der Sprachnachrichten und Dateianhängen an Terminen unter Punkt 3.1.7
  - Anpassung der Grafiken unter Punkt 6.1 und Punkt 11

- 27.01.2025
    - Entfernen der Informationen zum InvalidPath-Log und zum Cron-Log aus der Liste der erstellten Logs (Punkt 4.2.3 Loging: Integrität & Sicherheit), da das Loging im System reduziert wurde.
    - 7.6 AV Vertrag: Konkretisierung der verwendeten Standardvertragsklausel.
    - 3.1.7 Versendete Dateien & Sprachnachrichten: Ergänzung der Informationen zur Dateiablage
    - 5.2.2 Accounts: Konkretisierung der Speicherdauer der Accountnamen gelöschter Accounts