Einwilligung zur Teilnahme an einer Webkonferenz

Liebe Teilnehmer/in,

aufgrund der Coronakrise biete ich meine Kurse und, in dafür geeigneten Fällen, auch die Sprechstunde derzeit über eine Webkonferenz-Software an. Diese Software wird mir von der Plattform *hebammenkurs.de* bereitgestellt und basiert auf der Software *gotomeeting* – einer der sichersten Webconferencing-Produkte weltweit.

Die Zugangsdaten zur Teilnahme an einem meiner virtuellen Meetings erhältst du von mir. Indem du dich mit diesen Daten einloggst, und somit den virtuellen Raum betrittst, erklärst du dich mit der Tatsache einverstanden, dass du an einem Meeting teilnimmst, dessen Daten per Internet übertragen werden.

Mit deiner Unterschrift bestätigst du, dass du der Teilnahme an einem meiner virtuellen Veranstaltungen zustimmst und die Informationen zum Datenschutz gelesen hast.

Für Rückfragen stehe ich dir gerne zur Verfügung.

_____

Name der Hebamme

_____

Datum und Unterschrift Teilnehmer/in

Information zum Datenschutz:

Liebe Hebammen,
liebe Kursteilnehmer/innen,

seit Beginn der Coronakrise stellt *hebammenkurs.de* zahlreichen Hebammen deutschlandweit einfach und unkompliziert virtuelle Kursräume zur Durchführung von Kursen und zur Sprechstunden bereit. Trotz der Krisensituation steht der Schutz eurer Daten und Gesprächsinhalte selbstverständlich an höchster Stelle. Die von uns angebotenen virtuellen Kursräume basieren auf Basis der Software *gotomeeting*. Diese Software gehört zu den sichersten Webconferencing-Produkten weltweit und unterscheidet sich hinsichtlich der Vorkehrungen zum Datenschutz in vielerlei Hinsicht von anderen bekannten Anbietern (wie z.B. Skype, Zoom u.ä.).

Um deine Daten und Gesprächsinhalte zu schützen bestehen folgende Sicherheitsvorkehrungen:

- Die von uns eingesetzte Software **entspricht** in jeder Hinsicht der **EU-DSGVO**.

- Es ist **niemals** nötig, dass **persönliche Daten** eingegeben werden müssen. Weder von der Hebamme noch von den Teilnehmern. Zum Login als Moderatorin stellen wir der Hebamme eine Alias-Emailadresse bereit. Beim Eintritt in den Raum muss lediglich irgendein Name zur Identifikation eingegeben werden.

- Sämtliche Meetings müssen zwingend durch die Moderatorin mit einem **Kennwort** geschützt werden. Dieses Kennwort wird nur an die Teilnehmer/innen weitergegeben. Für jedes einzelne Meeting wird das Kennwort neu definiert. Personen können somit nur den Raum betreten, wenn der Zugangslink und das entsprechende Kennwort bekannt sind. Weiterhin kann die Moderatorin den **virtuellen Raum** zu jedem gewünschten Zeitpunkt **sperren**. Dieser zusätzliche Schutz führt dazu, dass ab diesem Moment niemand mehr den Raum betreten kann - auch wenn Passwort und Zugangslink bekannt sind.

- Es ist wichtig zu beachten, dass das **Meeting-Kennwort nie an uns übertragen** wird. Dies bietet die zusätzliche Gewissheit, dass keine unbefugten Personen (einschließlich unserer Mitarbeiter) an einer Sitzung teilnehmen können.

- Jede im Raum anwesende Person wird jedem Teilnehmer in der **Anwesenheitsliste** angezeigt. Es ist nicht möglich Inkognito im Raum anwesend zu sein – auch für unsere Mitarbeiter nicht.

- Die **Bild- und Tonübertragung** während der Gespräche werden **nicht gespeichert**.

- Die Moderatorin hat theoretisch die Möglichkeit das **Gespräch aufzuzeichnen**. **Dies ist grundsätzlich nicht zulässig.** Sollte doch eine Aufzeichnung durch die Moderatorin stattfinden, wird dies **jedem Teilnehmer** im Raum deutlich sichtbar als **Warnung** angezeigt. Teilnehmer können keine Aufzeichnungen vornehmen.

- Die gesamte Kommunikation erfolgt über **SSL-geschützte Verbindungen**, um eine Offenlegung der Sitzungsidentifikationsdaten zu verhindern. Zusätzlich müssen die Teilnehmer eine **„End-to-End-Authentifizierung"** beim Organisator der Sitzung durchführen. Diese basiert auf einem geheimen Zufallswert, der vom Service Broker bereitgestellt wird (läuft im Hintergrund ab).

- Die End-to-End-Authentifizierung erfolgt über das **SRP-Protokoll** (Secure Remote Password). SRP ist ein etabliertes, robustes und sicheres kennwortbasiertes Authentifizierungs- und Schlüsselaustauschverfahren. SRP widersteht einer Vielzahl von Angriffen, darunter sowohl passives Abhören und als auch aktives Knacken von Kennwörtern.