Datensparsame Konfiguration von Threema Work

I. Bei der Installation

a. **Hinterlegen der Telefonnummer**: diese Funktion ist bei Threema optional, der Messenger kann auch ohne Freigabe dieser pbD erfolgen, daher **Empfehlung:** nicht hinterlegen

b. **Hinterlegen der E-Mail-Adresse**: siehe Darstellung oben,
Empfehlung: nicht hinterlegen bzw. hinterlegen Sie nur jene Kontaktadresse, die ggf. eh bereits unter Ihren Adressaten bekannt ist

c. **Synchronisation mit dem Adressbuch**: siehe Darstellung oben
Empfehlung: nicht synchronisieren

II. Einstellungen – Privatsphäre (abrufbar über den ☰ - Button oben rechts)

a. **Kontakte synchronisieren**: **deaktivieren**

b. **Unbekannte blockieren**: **eigene Entscheidung**

c. **Lesebestätigung senden**: **deaktivieren**

d. **Melden wenn ich tippe**: **deaktivieren**

e. **Ausschlussliste**: **nach Notwendigkeit**

f. **Blockierte Kontakte**: **nach Notwendigkeit**

g. **Threema Anrufe aktivieren**: **deaktivieren**

h. **Miniaturen und Screenshots verhindern**: **wird automatisch eingeschaltet, sobald die App per PIN geschützt wird (siehe III.) / deaktivieren**

i. **Inkognito-Tastatur anfordern**: **deaktivieren**

j. **Direct Share**: **deaktivieren**

k. **Symbol für ungelesene Nachrichten**: **kann aktiviert sein**

III. Einstellungen – Sicherheit (abrufbar über den ☰ - Button oben rechts)

Diese Konfiguration bzw. auch der Grad der Intensität ist variabel und hängt stark von den persönlichen Umständen des Nutzers ab.
Wird die Anwendung auf einem privaten Endgerät genutzt, das ferner auch im privaten Umfeld Gebrauch findet, muss der Schutzgrad naturgemäß höher sein als bei einer alleinstehenden Lehrkraft ohne Kinder, die bspw. extra für diese dienstlichen Zwecke ein Zweitgerät besorgt hat.
U. g. Empfehlung basiert auf dem (vermeintlichen) Regelfall, in dem nicht ausgeschlossen werden kann, dass ein Dritter physisch Zugriff auf das Endgerät haben kann.

a. **Zugriffsschutz - Schutzmechanismus**: **PIN oder biometrisch** (insofern das Endgerät diese Funktion unterstützt)

b. **Zugriffsschutz - PIN: mindestens 4 Zeichen, besser 6-8**

c. **Zugriffsschutz - App-Schutz**: **aktivieren**

d. **Zugriffsschutz - Zeit bis zum Sperren**: **so kurz wie möglich, so lang wie nötig (<5 min)**

e. **Verschlüsselung - Passphrase**: **aktivieren**

f. **Verschlüsselung - Passphrase ändern**: **beim ersten Mal**

g. **Verschlüsselung - Neue Nachrichten anzeigen**: **aktivieren**

IV. **Einstellungen – Töne und Benachrichtigungen** (abrufbar über den ☰ - Button oben rechts)

Hier der ergänzende (weniger datenschutzrelevante) Hinweis, dass man unter diesem Punkt eine „Nicht stören"-Funktion konfigurieren kann, welche man bei Bedarf für Außerdienst-Zeiten konfigurieren kann – auch abseits der allgemeinen Vorgaben des Smartphones.
Hier kann und sollte der Nutzer einstellen, wann er Benachrichtigungen über neue Nachrichten in Threema Work erhält und wann nicht. Dies empfiehlt insb. für Lehrkräfte, die ein und das selbe Gerät für dienstliche wie private Zwecke nutzen.

Genehmigungspflicht für Nutzer mit privaten Endgeräten
Wenn Sie sich zur freiwilligen, dienstlichen Nutzung der Anwendung „Threema Work" auf Ihrem **privaten** Gerät entschieden haben, muss dies durch Ihre **Schulleitung genehmigt** werden.
Hierzu muss die Anlage 1 der VwV Datenschutz fortgeschrieben werden. Ergänzen Sie ein ggf. bereits bestehendes Formular um den Eintrag „Threema Work" und stellen Sie dieses Ihrer Schulleitung zur Genehmigung zur Verfügung.