dsb
datenschutzbeauftragte
kanton zürich

Merkblatt

Messenger und Videokonferenzsysteme

1 Einleitung

Dieses Merkblatt richtet sich an öffentliche Organe des Kantons Zürich. Es unterstützt sie bei der Risikoanalyse und hilft, das für die jeweilige Aufgabenerfüllung geeignete Produkt auszuwählen.

Die Auswahl der Produkte basiert auf Anfragen, die bei der Datenschutzbeauftragten eingegangen sind.

2 Datenschutzrechtliche Voraussetzungen

Werden Messenger oder Videokonferenzsysteme eingesetzt, bearbeiten die Produkteanbieter Daten des öffentlichen Organs und der Nutzerinnen und Nutzer. Für diese Datenbearbeitungen im Auftrag gelten die Rahmenbedingungen des Gesetzes über die Information und den Datenschutz. Die gesetzlichen Anforderungen sind im Leitfaden Bearbeiten im Auftrag zu finden.

Die Auswertung erfolgte nach den aus datenschutzrechtlicher Sicht und für eine Risikoanalyse wichtigsten Kriterien. Sie beschränkt sich auf Unterlagen der Produkteanbieter. Sie sind meistens in den AGB und/oder einer Datenschutzrichtlinie auf der Website veröffentlicht.

Beurteilt wurde wie folgt: datenschutzfreundlich teilweise kritisch kritisch

3 Tipps

1. Immer das datenschutzfreundlichste Produkt nutzen
   – Telefon oder Messenger nutzen statt eine Videokonferenz durchführen
   – ein System eines schweizerischen oder europäischen Anbieters nutzen statt eines aus Ländern mit nicht angemessenem Datenschutzniveau. Speicherung der Daten im europäischen Raum.
2. Das Produkt wenn möglich lokal einsetzen, das heisst, auf eigenen Systemen betreiben
   – insbesondere keine Dokumente mit Personendaten auf Fremdsystemen abspeichern
3. Dienste mit angemessener Authentifizierung nutzen
   – auf eine Anmeldung mit zwei Faktoren achten, wenn die Kommunikation besondere Personendaten beinhaltet
4. Ausschliesslich notwendige Funktionen aktivieren respektive nicht notwendige deaktivieren
   – Attention Tracking deaktivieren
   – Dokumentenablage sperren
5. In Schulen Lernende informieren und instruieren respektive bei nicht urteilsfähigen Kindern deren Eltern

4 Funktionen der Kommunikationssoftware

Die Funktionen der verschiedenen Softwarelösungen lassen sich nicht exakt abgrenzen. Bei der Nutzung sind grob zu unterscheiden:

– Messenger, mehrheitlich mit Telefonie und/oder Videoanruf
– Videokonferenzsysteme ohne Inhaltsspeicherung (Dokumente, Gesprächsinhalt)
– Videokonferenzsysteme mit möglicher Inhaltsteilung, -speicherung und Chats

5 Vorgehen und Risikoanalyse

Das öffentliche Organ bleibt für die durch die Anbieter bearbeiteten und gespeicherten Inhalts- und Randdaten verantwortlich (Name, IP-Adresse, Dauer des Gesprächs). Es muss bei der Auswahl eines Kommunikationstools eine Risikoanalyse durchführen. Die folgenden Fragen und Hinweise helfen, wichtige Punkte zu berücksichtigen:

– Zu welchem Zweck wird die Kommunikationssoftware eingesetzt (interne oder externe Kommunikation, Anzahl Teilnehmende)?
– Welche Art von Informationen soll ausgetauscht werden respektive welchem Schutzbedarf unterliegen sie (Sachdaten, Personendaten, besondere Personendaten)? Je sensitiver die Daten sind, desto höher ist der Schutzbedarf und desto mehr Schutzmassnahmen müssen umgesetzt werden.
– In welchem Bereich soll die Kommunikationssoftware eingesetzt werden (Strafverfolgung, Gerichte, Schule)? Beim Einsatz in sensitiven Bereichen können Rückschlüsse

auf beteiligte Personen gezogen werden, die gravierende Folgen haben können. Deshalb sind zusätzliche Massnahmen umzusetzen. Sie reichen vom Kreieren von geschlossenen Räumen über das Anmelden durch Dritte bis hin zur Wahl eines anderen Produkts.

- Ist schweizerisches Recht anwendbar und ein schweizerischer Gerichtsstand verankert? Werden Dokumente mit Personendaten gespeichert, ist dies zwingend.
- Werden die Randdaten in einem Land mit angemessenem Datenschutzniveau gespeichert?
- Ist die Datenübermittlung und/oder die Datenspeicherung verschlüsselt? Besondere Personendaten müssen immer verschlüsselt übermittelt und gespeichert werden.
- Gibt es eine Zwei-Faktor-Authentifizierung? Bei sensitiven Personendaten und solchen, die einer speziellen Geheimnispflicht unterliegen, wird die Zwei-Faktor-Authentifizierung vorausgesetzt.

6 Übersicht Messenger und Videokonferenzsysteme

	Beekeeper	TeamViewer Meeting	Cisco WebEx	Escola
Art des Dienstes	Messaging, Dokumenten-austausch	Video, Audio, Chat, Bildschirm-teilung	Video, Audio, Chat, Bildschirmteilung	Software für Schuladministra-tion
Anwendbares Recht	CH	D	CH möglich	CH
Gerichtsstand	Zürich	Stuttgart	CH möglich	Zürich
Zweckbindung	Bearbeitung ge-mäss Weisung Auftraggeber	Free version: Auswertung für ei-gene Zwecke	Auswertung Tele-metrie-, Support-, Verwaltungsdaten für eigene Zwecke	Ja
Serverstandort/ Ort der Datenbearbeitung	CH	D	EU / GB / USA	CH / D
Datenregion wählbar	Nein	k/a	Ja	Ja
Cloud Computing / Lokal einsetzbar	Cloud	Cloud	Cloud	Cloud
Verschlüsselter Transport	Ja	Ja	Ja	Ja
Verschlüsselte Speiche-rung von Dokumenten	Ja	k/a	Ja	Ja
Schlüsselmanagement	Anbieter	Anbieter	Anbieter Auftraggeber mög-lich für data at rest	Anbieter
E2EE Nachrichten	Ja	Unklar	Ja	Nein
E2EE Audio / Video (Ende-zu-Ende-Ver-schlüsselung)	-	Unklar	Ja (Meetings) nicht bei der Nut-zung Third Party Client Nein (Teams Mee-tings)	Ja, teilweise. Verbindungen von 2 Teilnehmenden sind E2E ver-schlüsselt
Zwei-Faktor-Authentifizie-rung möglich	Ja	Ja	Ja	Ja
Anonyme/Pseudonyme Nutzung Teilnehmende	Nein	Ja	Ja	Nein
Web-/Client-/App-Nutzung	App	Web/Client/App	Client/App	Web
Website	beekeeper.io/de	teamviewer.com/de	webex.com/de	escola.com/
Besonderheiten	Für interne Kom-munikation Vertrag für öffent-liche Organe ab-schliessen		Individueller Vertrag notwendig Standort EU wählen Aufbewahrungsfris-ten definieren	

	Google Meet Teil von G Suite	**Klapp**	**Microsoft 365 Teams**	**MyMeeting**
Art des Dienstes	Video, Dokumenten-austausch	Messaging, Chat, Dokumentenaus-tausch	Video, Audio, Mes-saging, Chat, Doku-mentenaustausch	Video, Audio
Anwendbares Recht	CH	CH	CH	CH
Gerichtsstand	CH	Baden	CH für Daten-schutzbelange	Baar
Zweckbindung	Nein	Ja	Ja	Ja
Serverstandort/ Ort der Datenbearbeitung	EU / USA / andere	CH	CH / EU	CH
Datenregion wählbar	Für Schulen EU wählbar	Nein	je nach Version	-
Cloud Computing / Lokal einsetzbar	Cloud	Cloud	Cloud	Beim Anbieter
Verschlüsselter Transport	Ja	Ja	Ja	Ja
Verschlüsselte Speiche-rung von Dokumenten	Ja Google Drive	k/a	Ja	-
Schlüsselmanagement	Anbieter	k/a	Anbieter	-
E2EE Nachrichten	Nein	k/a	Nein	-
E2EE Audio / Video	Nein	-	Nein	Nein Nur 1-1
Zwei-Faktor-Authentifizie-rung möglich	Ja	k/a	Für Administratoren	Ja
Anonyme/Pseudonyme Nutzung Teilnehmende	Nein Anmeldung nötig	k/a	Teilweise	Nein
Web-/Client-/App-Nutzung	Web/App	Web/Client/App	Web	Web
Website	apps.google.com/meet/	klapp.pro	microsoft.com	mymeeting.ch
Besonderheiten	Für Schulen siehe Leitfaden G Suite Enter-prise for Educa-tion	Für Sach- und Personendaten geeignet Einseitige Abän-derbarkeit AGB möglich	Für Schulen siehe Leitfaden Microsoft 365 im Bildungsbe-reich Für die Verwaltung gemäss SIK-Rah-menvertrag	CH Anbieter Für alle Daten ge-eignet

	Signal	Threema	Wire Enterprise/Pro	Zoom kostenpflichtige Version
Art des Dienstes	Video (1-1), Audio, Messaging, Chat, Dokumentenaustausch	Video (1-1), Audio, Messaging Chat, Dokumentenaustausch	Video, Audio, Chat, Dokumentenaustausch	Video, Audio, Chat, Bildschirmteilung, Dokumentenaustausch
Anwendbares Recht	Kalifornien	CH	CH	CH
Gerichtsstand	Kalifornien	CH	Zug	Zürich
Zweckbindung	Ja	Ja	Wire Pro Auswertung Telemetriedaten	Ja
Serverstandort/ Ort der Datenbearbeitung	Weltweit Als Zwischenspeicher	CH	EU	EU/USA/Andere
Datenregion wählbar	-	-	Nein	Ja
Cloud Computing / Lokal einsetzbar	Lokal (Endgerät)	Lokal (Endgerät)	Enterprise Cloud und lokal Pro nur Cloud	Cloud Dokumente/Aufnahmen lokal speichern
Verschlüsselter Transport	Ja	Ja	Ja	Ja
Verschlüsselte Datenablage	Ja	Ja	Datenablage auf iOS/Android-Endgeräten verschlüsselt, auf Desktop Clients unverschlüsselt	Ja
Schlüsselmanagement	Lokal	Lokal	-	Anbieter
E2EE Nachrichten	Ja	Ja	Ja	Ja
E2EE Audio / Video	Ja	Ja	Ja	Ja
Zwei-Faktor-Authentifizierung	App mit PIN	App mit PIN	k/a	Ja
Anonyme/Pseudonyme Nutzung Teilnehmende	Telefonnummer erforderlich	Anonyme Nutzung	Wire Enterprise Ja Wire Pro mit E-Mail Adresse	Teilweise (z.B. Webinars)
Web-/Client-/App-Nutzung	App	App / Web-Frontend nutzbar	Web/App	Web/Client/App
Website	signal.org	threema.ch	wire.com	zoom.us
Besonderheiten	Quellcode verfügbar		Für Schulen Rahmenvertrag educa Quellcode verfügbar	Switch ist Reseller procurement @switch.ch

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh