Fragen an Ihren Anbieter

Nachfolgend haben wir für Sie einen Fragenkatalog zusammengestellt. Bevor Sie sich für eine Kommunikationslösung entscheiden, können Sie die Werbeaussagen von Anbietern im Hinblick auf Datenschutz, Datensicherheit und Nachhaltigkeit einem Realitäts-Check unterziehen.

1. Allgemein

• Verfolgt der Anbieter ein ganzheitliches Konzept, das nicht nur eine Komponente zur bestehenden IT hinzufügt, sondern nachhaltig und modular alle Kommunikationsformen integrieren hilft, um langfristig kostensenkend zu arbeiten?	Ja	Nein
• Erlaubt die angebotene Lösung auch aus der Organisation heraus an Dritte zu kommunizieren - kostenlos und ohne Einschränkung bei Sicherheit und Nutzerfreundlichkeit?	Ja	Nein
• Muss das Produkt on-premis installiert werden, um üblichen Anforderungen an Datenschutz und Datensicherheit zu genügen?	Ja	Nein

2. Produktsicherheit Server

• Wird die Server-Software vom Anbieter selbst entwickelt?	Ja	Nein
• Verzichtet die Server-Architektur des Anbieters auf Cloud-Services (z.B. Microsoft Azure, Amazon Web Services - AWS, Google Cloud Services, ...)?	Ja	Nein
• Setzt der Anbieter ausschließlich auf Open Source-Komponenten?	Ja	Nein
• Werden explizit alle Nutzdaten, die die Geräte der Anwender in Richtung Server des Anbieters verlassen dort verschlüsselt gespeichert?	Ja	Nein
• Sind Nutzdaten bereits vor der Übertragung an die Server so verschlüsselt, dass sie ausschließlich von den Empfängern entschlüsselt werden können?	Ja	Nein
• Ist sichergestellt, dass keine Nutzdaten, gleich welcher Art, serverseitig vom Anbieter ausgelesen, analysiert, verknüpft oder fremdverwertet werden können?	Ja	Nein

3. Produktsicherheit Apps

• Werden die Apps vom Anbieter selbst entwickelt?	Ja	Nein
• Liegen alle Nutzerdaten in den Apps stets verschlüsselt vor, und liegen auch die privaten (geheimen) Schlüssel stets nur auf den Geräten der Nutzer?	Ja	Nein
• Sind die geheimen Schlüssel der Nutzer durch Passwörter geschützt, die nur ihnen selbst bekannt sind?	Ja	Nein
• Erfolgen Backups, die die Schlüssel enthalten, verschlüsselt und unterliegen ausschließlich dem Zugriff durch ihre Nutzer?	Ja	Nein
• Kann der Anbieter Accounts und deren Inhalte wiederherstellen, wenn Nutzer kein Backup angefertigt haben und das einzige Gerät, auf dem der Account verwendet wurde, abhandengekommen oder zerstört worden ist?	Ja	Nein
• Lassen sich die Aussagen des Anbieters in Sachen Datensicherheit z.B. durch Open Source- Verfügbarkeit unabhängig bestätigen?	Ja	Nein

4. Produktsicherheit eigenes Personal

• Ist sichergestellt, dass die Accounts von (Ex-)Mitarbeitern sekundenschnell gesperrt werden können und damit sofort der Zugriff auf die Apps und die enthaltenen Daten ausgeschlossen ist?	Ja	Nein
• Könnten Ihre eigenen IT-Administratoren Account-Inhalte Ihrer Nutzer auslesen und/oder anderweitig (unbemerkt) Einsicht in die Kommunikation nehmen?	Ja	Nein

5. Unternehmen / Rechtliches

• Finanziert sich der Anbieter (auch) über Einnahmen aus Werbung oder Big Data oder plant diesbezüglich?	Ja	Nein
• Handelt es sich bei dem Anbieter um eine ordentliche Körperschaft, und befindet sich der Unternehmensstandort in einem EU-Land?	Ja	Nein
• Gibt es einen Unternehmensstandort außerhalb der rechtlichen Wirksamkeit der DSGVO (z.B. CH, GB oder USA)?	Ja	Nein
• Stammen die nennenswerten Anteilseigner des Unternehmens (ab 10% Eigenkapital) ausschließlich aus der EU und unterliegen keiner EU-fremden Rechtsprechung?	Ja	Nein
• Besteht bei dem Anbieter die Gefahr, dass die Versorgung von Kunden in Deutschland und/oder der EU durch politische Verwerfungen unterbrochen und/oder ausgesetzt werden kann?	Ja	Nein