DSGVO und professionelles Messaging: Warum die meisten unwissentlich dagegen verstoßen

Fast jede Kanzlei, Praxis oder Beratung versendet Kundendokumente über Anwendungen, deren Server sich außerhalb des Europäischen Wirtschaftsraums befinden. Ohne böse Absicht, aber in vielen Fällen verstoßen sie gegen die Verordnung, ohne dass sie jemand davor gewarnt hat.

Das Dokument, das weiter reist, als Sie denken

Eine Alltagssituation: Eine Steuerberaterin erhält per Messaging ein Dokument mit Kundendaten. Ein Vertriebsmitarbeiter leitet per Chat ein Angebot an einen Kollegen weiter. Eine Ärztin teilt auf demselben Weg einen klinischen Bericht mit einem Kollegen. Niemand denkt zweimal darüber nach. Es ist normal. Es ist bequem. Es ist das, was jeden Tag in jeder Kanzlei in jeder Stadt Europas getan wird.

Aber dieses Dokument ist in vielen Fällen gerade zu einem Server in den USA gereist. Es wurde – wenn auch nur vorübergehend, wenn auch "verschlüsselt im Ruhezustand" – in einer Cloud gespeichert, die weder der Fachmann noch sein Kunde kontrollieren. Es hat Systeme passiert, die technisch mit dem Inhalt verknüpfte Metadaten indexieren können. Und die europäische Datenschutz-Grundverordnung hat dazu einiges Klares zu sagen.

Was die Norm fordert

Die DSGVO – und in der Folge die Rechtsprechung des Gerichtshofs der Europäischen Union (insbesondere das Urteil Schrems II, C-311/18, aus dem Jahr 2020) – legt fest, dass personenbezogene Daten europäischer Bürger angemessen geschützt sein müssen. Wenn diese Daten den Europäischen Wirtschaftsraum verlassen, muss der Verantwortliche garantieren, dass der Empfänger ein Schutzniveau bietet, das dem europäischen "im Wesentlichen gleichwertig" ist. In der Praxis bedeutet dies, dass das Versenden von Kundendaten über Dienste, deren Server unter US-Gerichtsbarkeit stehen, ohne eine Folgenabschätzung durchgeführt und ergänzende Garantien – Standardvertragsklauseln, zusätzliche technische Maßnahmen wie überprüfbare Verschlüsselung usw. – implementiert zu haben, einen Verstoß gegen die Verordnung darstellen kann. Auch wenn bisher noch niemand etwas gesagt hat.

Und es geht nicht nur um den Inhalt der Nachrichten. Die Metadaten – wer was an wen sendet, wann, wie oft, von wo aus – sind laut Verordnung nach wiederholter Auslegung des Europäischen Datenschutzausschusses ebenfalls personenbezogene Daten. Ein Dienst, der Metadaten der beruflichen Kommunikation eines Benutzers sammelt, verarbeitet personenbezogene Daten der Kunden dieses Benutzers, ohne dass diese davon Kenntnis haben oder ihre Einwilligung zu einer solchen Verarbeitung gegeben haben.

Das gängige Denkschema – "ich benutze die App nur zum Schreiben; die App ist kein Datenanbieter meines Kunden" – ist rechtlich falsch. Wenn die Daten des Kunden die Infrastruktur eines Dritten passieren, verarbeitet dieser Dritte diese Daten. Und wenn er sie verarbeitet, muss es eine Rechtsgrundlage, einen Auftragsverarbeitungsvertrag und angemessene Garantien geben.

Wer verantwortlich ist

Die Frage, wer die rechtliche Verantwortung trägt, ist nicht akademisch. Die DSGVO unterscheidet zwischen dem *Verantwortlichen* (der entscheidet, welche Daten zu welchem Zweck verarbeitet werden) und dem *Auftragsverarbeiter* (der dies materiell im Namen des Verantwortlichen tut). Der Fachmann, der Kundendokumente versendet, ist der Verantwortliche. Der Anbieter der Messaging-App ist in vielen Fällen faktisch Auftragsverarbeiter. Ohne Auftragsverarbeitungsvertrag – und ohne die meisten Klauseln, die ein solcher Vertrag enthalten sollte – hat der Verantwortliche seine Verpflichtung nicht erfüllt.

Die wohlwollende Interpretation lautet: "Die meisten Fachleute wissen das nicht". Die strenge Interpretation lautet: "Unkenntnis schützt nicht vor Strafe". Und die Interpretation eines jeden diesbezüglich konsultierten Fachanwalts für Datenschutz ist in der Regel die strenge.

Für wen dies konkret wichtig ist

Für jeden Fachmann und jedes Unternehmen, das auch nur gelegentlich mit personenbezogenen Informationen Dritter umgeht:

- Anwälte, die Kundendokumentationen erhalten (Verträge, Klagen, Erklärungen, Vermögensberichte).
- Ärzte und anderes medizinisches Fachpersonal, die Gesundheitsdaten teilen – die nach Art. 9 DSGVO als *besondere Kategorien* mit verstärktem Schutz gelten –.
- Steuerberater und Verwaltungsmanager, die Identifikations-, Steuer- und Bankdaten bewegen.
- Personalabteilungen, die Arbeits- und Personalunterlagen von Mitarbeitern verwalten.
- Vertriebsmitarbeiter, die Kontaktdaten und oft sensible Geschäftsinformationen von Interessenten und Kunden erhalten.

In allen Fällen sind die Informationen durch die DSGVO geschützt. In allen Fällen fließen diese Informationen in der üblichen Praxis über Kanäle, deren Gerichtsbarkeit ohne zusätzliche Garantien nicht als dem europäischen Rahmen "im Wesentlichen gleichwertig" deklariert werden kann. Nicht aus böser Absicht. Aus Gewohnheit. Und aufgrund einer technologischen Infrastruktur, die fünfzehn Jahre lang Bequemlichkeit über Konformität gestellt hat.

Das Argument "Alle machen es"

Man sollte den häufigsten Einwand vorwegnehmen: "Wenn alle es machen, kann es kein wirkliches Problem sein". Es ist ein vollkommen verständliches Argument und hat rechtlich keinerlei Kraft. Die Tatsache, dass eine Praxis weit verbreitet ist, macht sie nicht konform mit der Verordnung. Die Datenschutzbehörden haben in den letzten Jahren mehrere Unternehmen genau wegen Messaging-Nutzungen sanktioniert, die bis zum Moment der Prüfung harmlos erschienen.

Die aktuelle operative Realität ist, dass das Risiko hinsichtlich der Wahrscheinlichkeit gering ist – es ist sehr selten, dass eine Prüfung der Datenschutzbehörde die spezifischen Messaging-Tools einer mittelgroßen Kanzlei auditiert –, aber hinsichtlich der Auswirkungen hoch, wenn es eintritt. Es ist ein Risiko, das die meisten eingehen, ohne zu wissen, dass sie es eingehen. Das heißt, ohne geprüft zu haben, ob das verwendete Tool mit der rechtlichen Verantwortung des Verantwortlichen im Einklang steht.

Digitale Spuren sind rückwirkend

Es gibt ein zweites, fast symmetrisches Argument zum vorherigen, das man vorwegnehmen sollte: *"Wenn dies ein ernstes Problem wäre, hätte die Verwaltung bereits mit der Prüfung begonnen"*. Die aktuelle beobachtete Realität gibt ihm oberflächlich recht. Prüfungen wegen missbräuchlicher Messaging-Nutzung in kleinen Unternehmen und vor allem bei Selbstständigen sind heute fast nicht vorhanden – nicht weil das Verhalten

erlaubt wäre, sondern weil es der Verwaltung in Deutschland und weiten Teilen der EU an den erforderlichen personellen Ressourcen fehlt, um Millionen von Verpflichteten zu auditieren.

Das ist es, was die heute beobachtete Praxis nahelegt. Es ist nicht das, was das nächste Jahrzehnt nahelegt. Zwei Vektoren konvergieren, um das Gleichgewicht in relativ kurzen Zeiträumen zu verändern.

Erstens: Digitale Spuren sind rückwirkend. Jede Nachricht, die über eine Anwendung mit Zentralserver gesendet wird, bleibt – zumindest in den Metadaten – in einer Infrastruktur registriert, die fortbesteht. Was vor sechs Monaten gesendet wurde, ist heute technisch noch prüfbar. Was heute gesendet wird, wird in fünf Jahren noch prüfbar sein. Das Fehlen einer gegenwärtigen Prüfung ist keine Garantie für das Fehlen einer zukünftigen Prüfung. Es ist ein Aufschub der Bewertung, keine Befreiung.

Zweitens: Die administrative Prüfungskapazität wird rasant wachsen. Die Einführung von Werkzeugen der künstlichen Intelligenz in Prüfungsprozesse eliminiert den personellen Flaschenhals, der bisher – faktisch, nicht rechtlich – kleine Unternehmen und Selbstständige geschützt hat. Ein System, das in der Lage ist, massive Metadaten, Steuererklärungen, Handelsregister und Meldepflichten für Sicherheitsverletzungen abzugleichen, benötigt keine Prüfer: Es benötigt Zugang. Und der Zugang ist durch Anforderungen an Anbieter mit rechtlicher Präsenz in der EU unter dem aktuellen Rechtsrahmen vollkommen machbar.

Hinzu kommt ein weniger technischer, aber ebenso entscheidender Faktor: Die europäischen Staaten befinden sich in einem Prozess stetig wachsender Verschuldung und müssen fast ohne Ausnahme ihre Steuerbasis erweitern. Die aus der Nichteinhaltung der DSGVO resultierende Verwaltungssanktion ist in rein fiskalischen Begriffen eine wachsende und politisch bequeme Einnahmequelle. Das ist keine Vermutung: Es ist ein beobachtbarer Trend in den Jahresberichten der europäischen Datenschutzbehörden, in denen das Gesamtvolumen der Sanktionen seit mehreren Geschäftsjahren in Folge steigt.

Die operative Schlussfolgerung für den Verantwortlichen ist nicht alarmistisch, sondern nüchtern: **Die Entscheidung darüber, wie heute die Kommunikation mit Kunden verwaltet wird, wird an der Prüfungskapazität des Jahres gemessen, in dem die Prüfung erfolgt, nicht an der aktuellen.** Und diese Kapazität wird in absehbarer Zeit wesentlich anders sein als heute. Wer heute beginnt, die Dinge richtig zu machen, wird nicht erst ab heute im Reinen sein: Die ab diesem Moment erzeugte Spur wird mit der Norm konform sein, und das schützt rückwirkend den kommenden Abschnitt. Wer so weitermacht wie bisher, wird prüfbare Spuren anhäufen, deren Konformität an den Standards – und Ressourcen – der kommenden Jahre gemessen wird.

Was sich mit einer anderen Architektur ändert

Es gibt technische Alternativen, bei denen die Daten nicht in der Infrastruktur Dritter gespeichert werden, sondern direkt vom Gerät des Senders zu dem des Empfängers reisen. In dieser Architektur hängt die Einhaltung der DSGVO in Bezug auf internationale Übermittlungen nicht von Standardvertragsklauseln, dem guten Willen des Anbieters oder zukünftigen Audits ab. Sie hängt davon ab, dass es *keine Übermittlung* gibt. Und gegen das, was nicht existiert, kann man nicht verstoßen.

Dies ist keine exklusive Lösung und nicht die einzig mögliche. Aber sie ist strukturell anders, und die Einhaltung der Vorschriften ist nicht länger ein verfahrenstechnischer Anhang, sondern wird zu einer direkten Folge des Designs. Für einen Fachmann, der seine Verantwortung als Verantwortlicher ernst nimmt, macht dieser Unterschied einen Unterschied.

Die nächste Ausgabe von Cuadernos wird im Detail das Schrems II-Urteil und seine praktischen Auswirkungen für kleine und mittlere Unternehmen analysieren, die von US-Cloud-Diensten abhängig sind, fünf Jahre nach seiner Veröffentlichung.

Quellen und Rechtsrahmen

- Verordnung (EU) 2016/679 (DSGVO), insbesondere Kapitel V über internationale Übermittlungen.
- EuGH C-311/18 ("Schrems II"), 16. Juli 2020.
- EDSA – Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungsinstrumenten.
- Datenschutzbehörden – Jahresberichte mit Fallbeispielen von Sanktionen wegen missbräuchlicher Nutzung von Instant Messaging in beruflichen Umgebungen.

← ZurückDas Berufsgeheimnis im digitalen ZeitalterWeiter →Wenn niemand dazwischen ist

Aktuelle Lektüre

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 75db01d4209ff72601a5f6b0f8b2a6795e7ab9ab857bad53116cf0ec9682b296

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.