VERSENDEN SIE SENSIBLE KUNDENDATEN VERSCHLÜSSELT

Die wichtigsten Fakten zur E-Mail-Verschlüsselung kurz und bündig

UNVERSCHLÜSSELTE E-MAILS SIND VOR ZUGRIFFEN UNBERECHTIGTER PERSONEN NICHT GESCHÜTZT.

Sie sind ein „offener Brief ohne Umschlag", der durchs Internet transportiert wird und von Dritten gelesen, kopiert oder archiviert werden kann. Die EU-Datenschutzgrundverordnung, das Bundesdatenschutzgesetz und das Strafgesetzbuch machen daher strenge Vorgaben zur Zugriffs- und Weitergabekontrolle personenbezogener Daten.

WAS SIND PERSONENBEZOGENE DATEN?

Die anwendbaren Verschlüsselungsmethoden unterscheiden sich nach der Art der Daten.

VERTRAULICHE DATEN
– Geburtsdatum
– Einkommen
– Bankdaten
– Vorhandensein einer Versicherung etc.

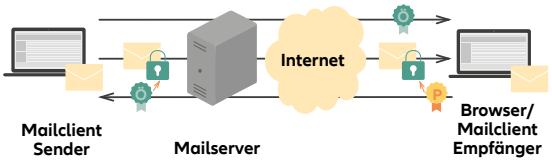
STRENG VERTRAULICHE DATEN
– Informationen zum Gesundheitszustand

HINWEIS

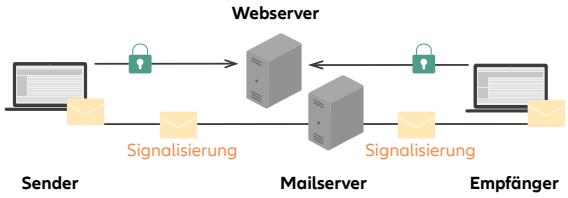
Die genannten Verfahren beziehen sich ausschließlich auf die Kommunikation zwischen Allianz und Ihnen als Vertriebspartner und nicht auf die Kommunikation zwischen Ihnen und End-/Privatkunden. Die Verschlüsselungsverfahren werden auch vom Posteingangszentrum der Allianz akzeptiert bzw. verwendet.

WELCHE VERSCHLÜSSELUNGSMETHODEN UNTERSTÜTZT DIE ALLIANZ?

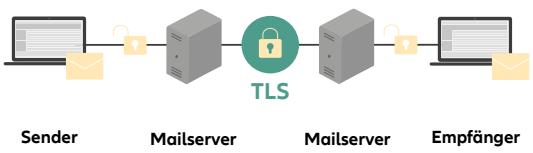
1. Zertifikatsverschlüsselung mit S/MIME



2. #Secure-Verfahren



3. TLS–Verschlüsselung
(bei streng vertraulichen Daten nur mit Kundeneinwilligungserklärung)



Allianz

VERSCHLÜSSELUNGS-METHODE	S/MIME (Schlüsselaustausch Sender & Empfänger)	#SECURE (eigenes „Portal-Postfach“)	TLS (verschlüsselter „Tunnel“)
FUNKTIONSWEISE IM BETRIEB	Verschlüsselung und Signatur von E-Mails mittels Zertifikaten. Die Kommunikation erfolgt wie gewohnt über das eigene E-Mail-Programm, die Verschlüsselung erfolgt über eine separate Verschlüsselungsfunktion im E-Mail-Programm.	Kommunikation über ein separates Portalpostfach, welches die Nachrichten verschlüsselt zur Allianz überträgt. Bei neuen Nachrichten der Allianz erhält der Empfänger eine Signalisierungsmail an Ihre „normale“ E-Mail-Adresse. Die Anmeldung zum Postfach erfolgt mittels E-Mail-Adresse und Passwort. Im Postfach können die Nachrichten gelesen, beantwortet, heruntergeladen oder E-Mails an Allianz Adressen versendet werden.	Ausschließliche Verschlüsselung des Übertragungswegs zwischen den Mailservern des Senders und Empfängers. Die Kommunikation erfolgt wie gewohnt über das eigene E-Mail-Programm, eine gesonderte Verschlüsselung ist nicht notwendig.
EINRICHTUNG	1. Erwerb eines Zertifikats bei einem öffentlichen Zertifikatsanbieter (Liste akzeptierter Zertifizierungs-stellen) 2. Bekanntmachen des öffentlichen Schlüssels bei der Allianz über Versand einer signierten Mail an Collect@cert.allianz.com 3. Download des Zertifikats des gewünschten Allianz Empfängers über die Zertifikatssuche und Hinterlegung des Zertifikats im Mailprogramm (am einfachsten als Download via „Kontakt vCard mit Zertifikat“ und Speicherung des Kontakts) Weitere Informationen zur Einrichtung finden Sie im Maklerportal unter makler.allianz.de/siko.	Einmalige Anlage eines Benutzerkontos für das Portal notwendig (Einrichtung eines Postfachs). Bitte wenden Sie sich zur Einrichtung an Ihren Maklerbetreuer oder eine Kontaktperson im Betriebsgebiet.	Einmalige Einrichtung der Serverkommunikation („Tunnel“) notwendig. TLS muss durch die IT auf beiden Seiten aktiviert werden. Um eine TLS-Verbindung einzurichten, müssen die verwendeten Mailserver TLS-fähig sein und entsprechend konfiguriert werden. Ihr Maklerbetreuer kann für Sie die Konfiguration auf Allianz Seite beantragen.
VORTEILE	– Hoher Sicherheitsstandard – Einfache Verschlüsselung im Mailprogramm (nach Einrichtung)	– Sofort verfügbar nach Einrichtung durch Allianz Mitarbeiter – Passwort verfällt nicht und kann selbstständig bei Vergessen entsperrt werden – keine Installation/ Konfiguration nötig	– Nach einmaliger Einrichtung kann mit der Domain problemlos kommuniziert werden – Kommunikation mit jeder E-Mail-Adresse in der Domain normal möglich – Für E-Mail-Adressen der Initiative „E-Mail made in Germany“ (z. B. GMX, WEB.DE, Telekom, freenet.de, 1&1) automatisch verfügbar
NACHTEILE	– Anerkanntes Zertifikat benötigt – Hoher Einrichtungsaufwand – Zertifikate laufen ab und müssen erneuert werden – E-Mails können nicht durch Stellvertreter gelesen werden	– Separates Postfach, das nicht im Standard-Mailprogramm integriert ist – Extra Passwort nötig – Jeder Mitarbeiter benötigt ein eigenes Postfach, sofern über eine persönliche E-Mail-Adresse kommuniziert wird (z. B. keine „info@...“)	– Einwilligungserklärung des Kunden bei streng vertraulichen Daten erforderlich Sofern keine E-Mail-Adresse der o. g. Initiative verwendet wird: – Mailserver muss administrierbar sein – Einrichtungsaufwand auf beiden Seiten
ANWENDUNGSFALL	Vertrauliche Daten + streng vertrauliche Daten	Vertrauliche Daten + streng vertrauliche Daten	Vertrauliche Daten + streng vertrauliche Daten (mit Kundeneinwilligung)