Hallo jemand,

die üblichen Hinweise wie:
"E-Mail ist nicht sicher. Es gibt ein Risiko, dass Nachrichten verfaelscht beim Empfaenger ankommen. Auch liegt es in der Verantwortung des Empfaengers, angehaengte Dateien vor dem Laden auf Viren zu untersuchen. Die in dieser E-Mail enthaltenen Informationen sind vertraulich. Diese E-Mail ist ausschließlich für den Adressaten bestimmt und jeglicher Zugriff durch andere Personen ist nicht zulaessig. Falls Sie nicht der beabsichtigte Empfaenger sind, ist jegliche Veroeffentlichung, Speicherung, Vervielfaeltigung, Verteilung oder sonstige in diesem Zusammenhang stehende Handlung untersagt. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtuemlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail." sind sind auch rechtlich so wirksam, wie der berühmte Aluhut (https://de.m.wikipedia.org/wiki/Aluhut)... besser wäre eine Ende-zu-Ende Verschlüsselung wie unten beschrieben.

Damit ich das Rad nicht noch einmal neu erfinden muss, habe ich einige Links strukturiert zusammengestellt. So sollte die schrittweise Herangehensweise dieser "Anleitung" für das grundlegende Verständnis helfen und ist nicht direkt als 1:1-Kochrezept anwendbar. (Die Voraussetzungen sind verschieden und die Programme ändern sich...)

========== Datenschutzhinweis:
Früher gab es noch das Post + Fernmeldegeheimnis - Willkommen im Heute!

Zum Thema die Kurzfassung:
http://www.openpgp-schulungen.de/fuer/bekannte/
https://digitalcourage.de/digitale-selbstverteidigung
/vertrauenswuerdige-e-mail-anbieter

WAS ist die Aufgabe? Vertraulichkeit, Integrität und Verfügbarkeit fehlen im Internetz.
https://www.gpg4win.de/doc/de/gpg4win-compendium_7.html

WIE wird es erreicht? durch Verschlüsselung (und persönliches Vertrauen)
digitales Briefgeheimnis auf alemannisch: http://vimeo.com/17610962
(oder hier: https://digitalcourage.video/w/wVfxRz93q5eVVPg6VaXbXD)
https://www.kuketz-blog.de/verschluesselte-e-mails-mit-gnupg-als-supergrundrecht/

WER ist für die Maßnahme verantwortlich? Beide: Sender und Empfänger
Anleitung für PGP: https://emailselfdefense.fsf.org/en/infographic.html

WANN wird sie ausgeführt?
Nach Vorbereitung & während der vertraulichen Kommunikation
Der Erste fängt an:
er gibt seinen öffentlichen Schlüssel bekannt und unterschreibt (signiert) diesen. Das persönliche Vertrauen wird hergestellt, indem die zugehörige Schlüssel-Kurzfassung (Fingerprint) auf sicherem Weg eigenhändig & augenscheinlich verglichen wird. (+ umgekehrt) neu:
https://keys.openpgp.org/about

WO wird sie durchführt? vorzugsweise in sicherer Umgebung
z.B. am PC mit E-Mail-Client:
https://www.privacy-handbuch.de/handbuch_32j.htm

Diese E-Mail und die Anhänge wurden elektronisch unterschrieben; d.h. diese Nachricht kann jeder lesen und die Unversehrtheit prüfen.
Wenn also die Unterschrift stimmt (s.Bild im Anhang: Überprüfung =?=), wurde die Nachricht (E-Mail= Datei) unterwegs nicht verändert.

Zur Vervollständigung dieser Einladung ist mein öffentlicher PGP-Schlüssel als *.asc-Datei zur weiteren Verwendung anbei.

...und ja, das braucht Aufmerksamkeit und Zeit.
Viele Grüße!