

# E-MAILS VER- SCHLÜSSELN



**EINFACH  
GEMACHT**

# Über mich

2018: B.Sc. Wirtschaftsinformatik

2019: Blog [www.privacytutor.de](http://www.privacytutor.de)

2021: [YouTube-Channel](#)



## Meine Mission:

Ich gebe einfach verständliche Praxistipps, mit denen "normale" Internetnutzer mehr Kontrolle über ihren digitalen Alltag erhalten.



# Was interessiert Sie?



# Über was reden wir heute?

Warum sind E-Mails unsicher?

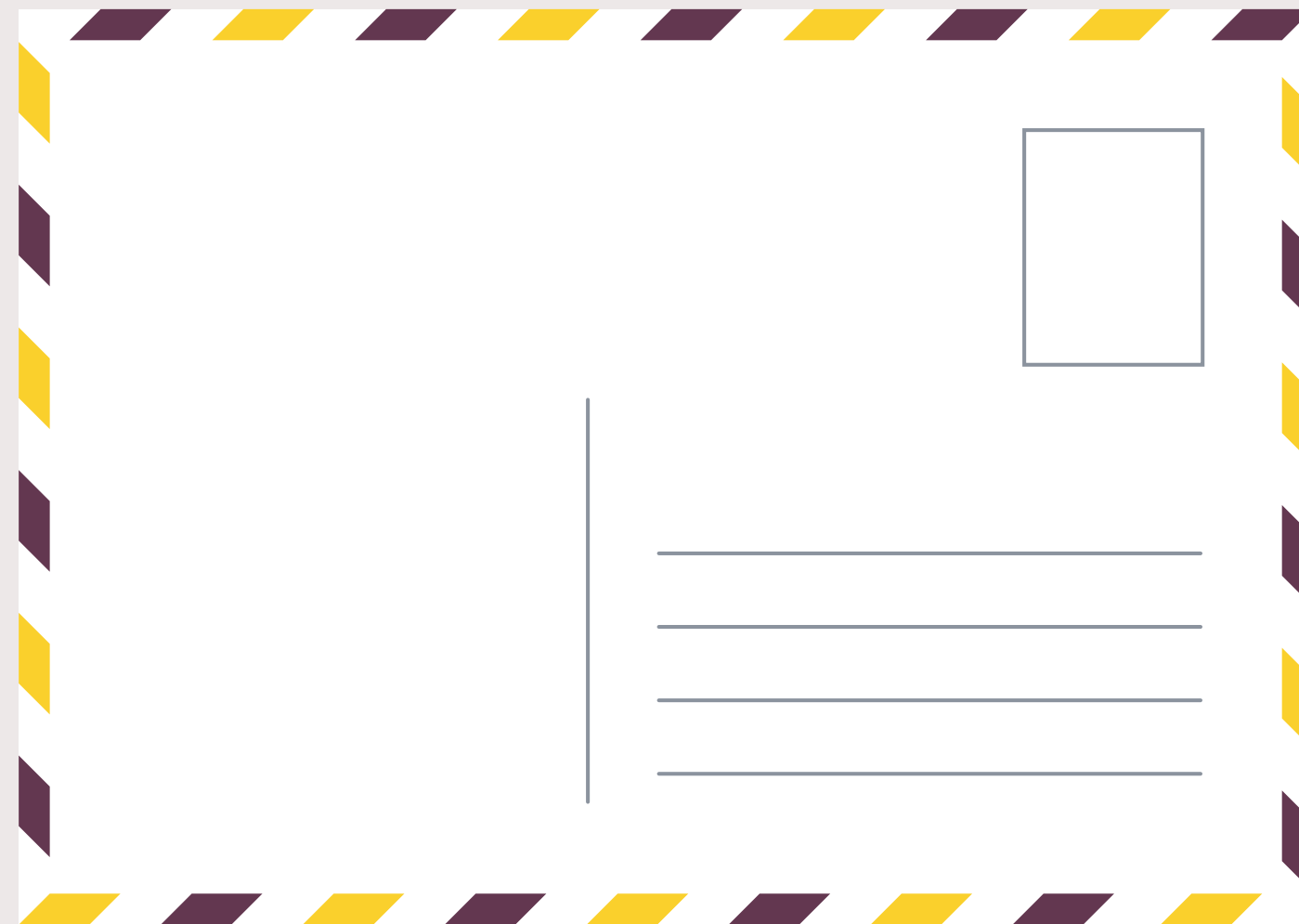
Wie funktioniert die Verschlüsselung?

3 Verschlüsselungs-Varianten

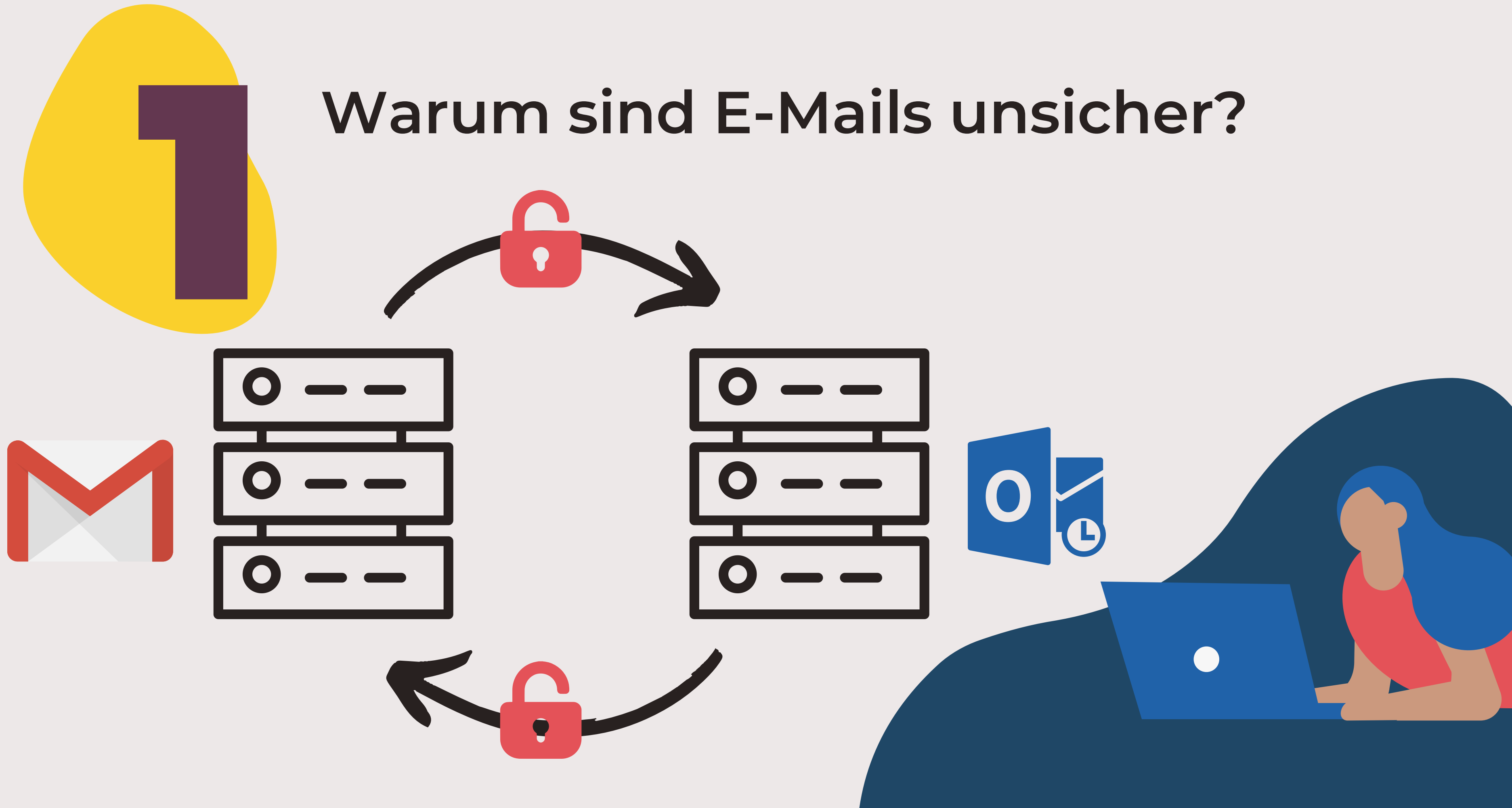




# Warum sind E-Mails unsicher?



# Warum sind E-Mails unsicher?





# Nachteile unverschlüsselter E-Mails

Größeres Risiko bei Schadsoftware & Hackern

Keine Signatur

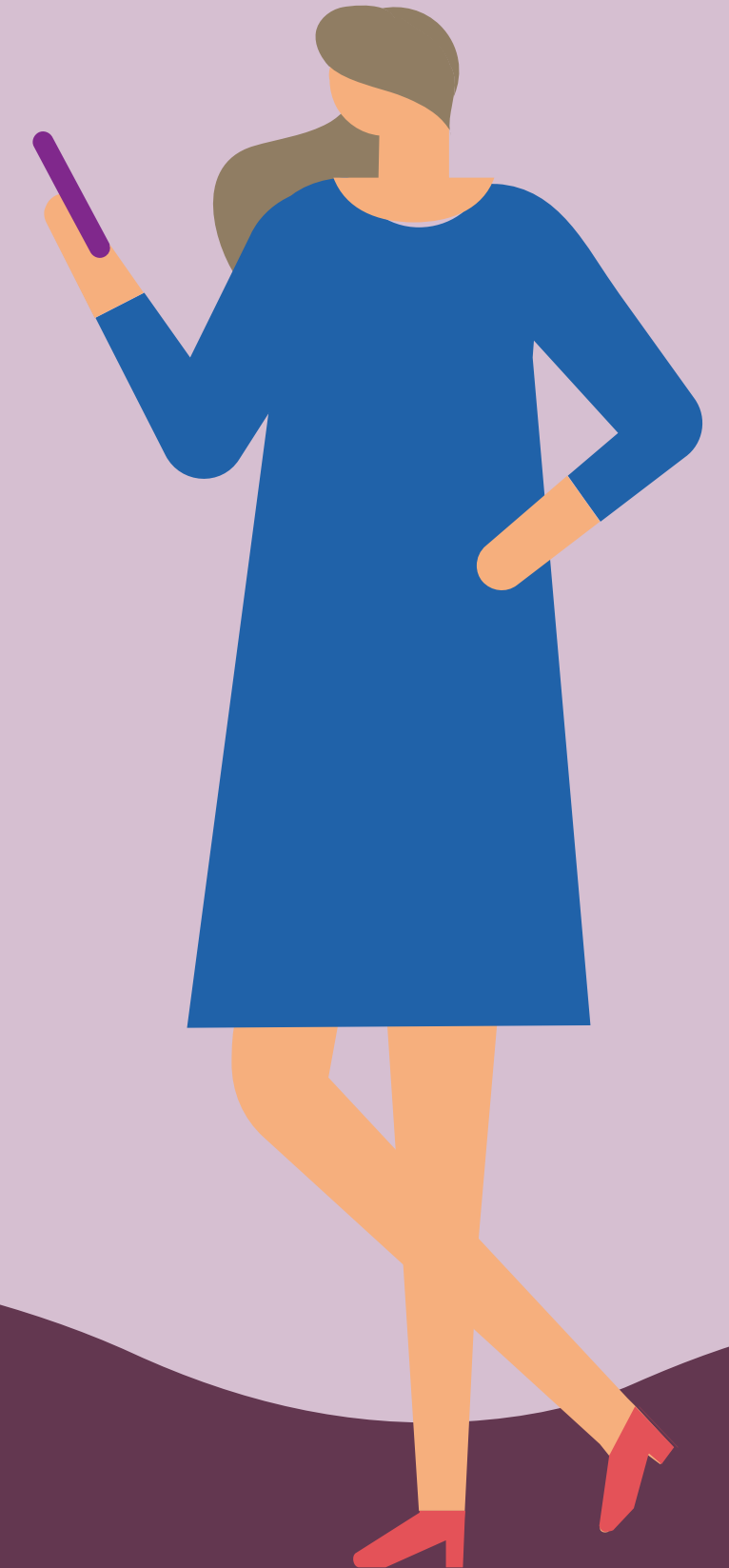
Anbieter & Behörden können mitlesen

"Nach Telekommunikationsgesetz [...] müssen seit dem Jahr 2005 alle Betreiber [...] auf Anordnung eine E-Mail-Überwachung durchführen." [Wikipedia](#)





# Wie funktioniert die Verschlüsselung?



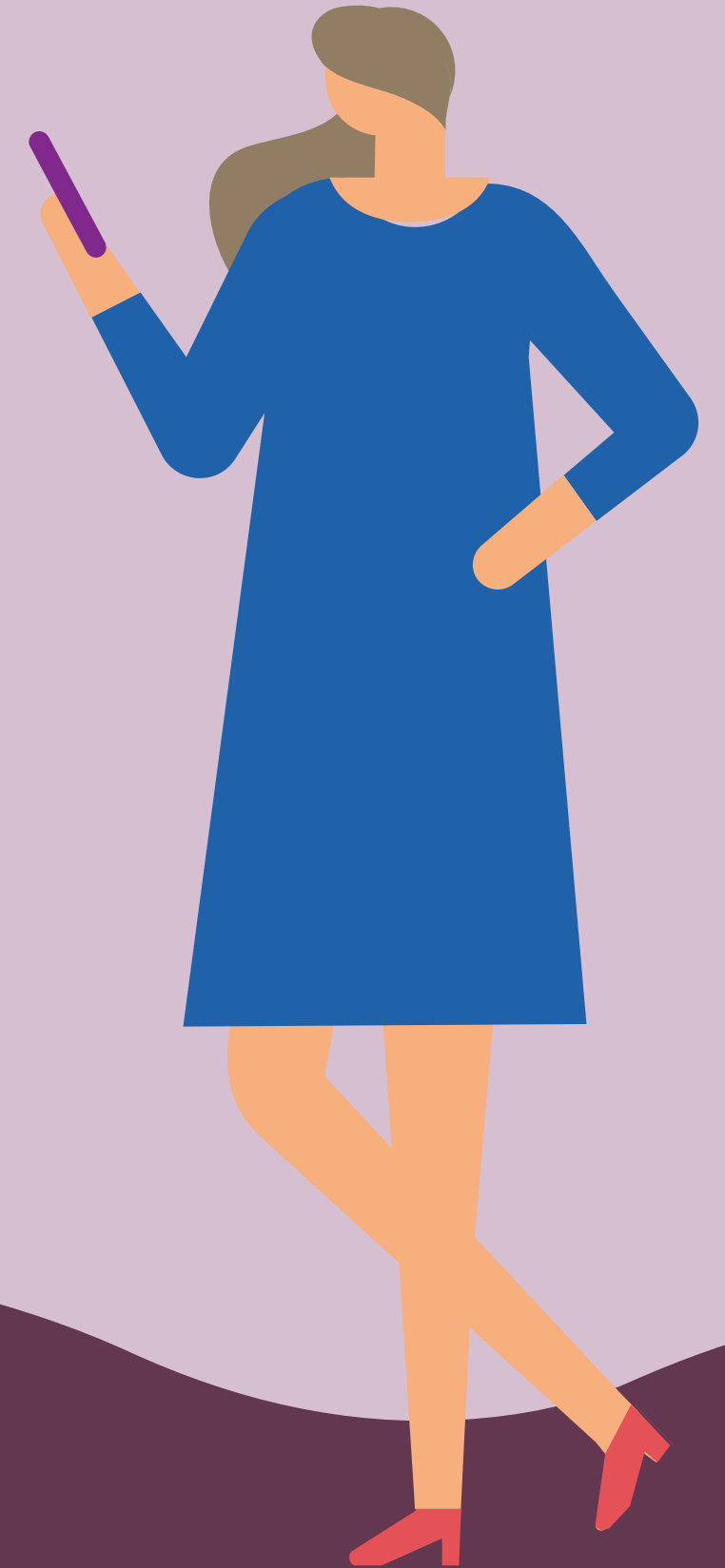


# 2

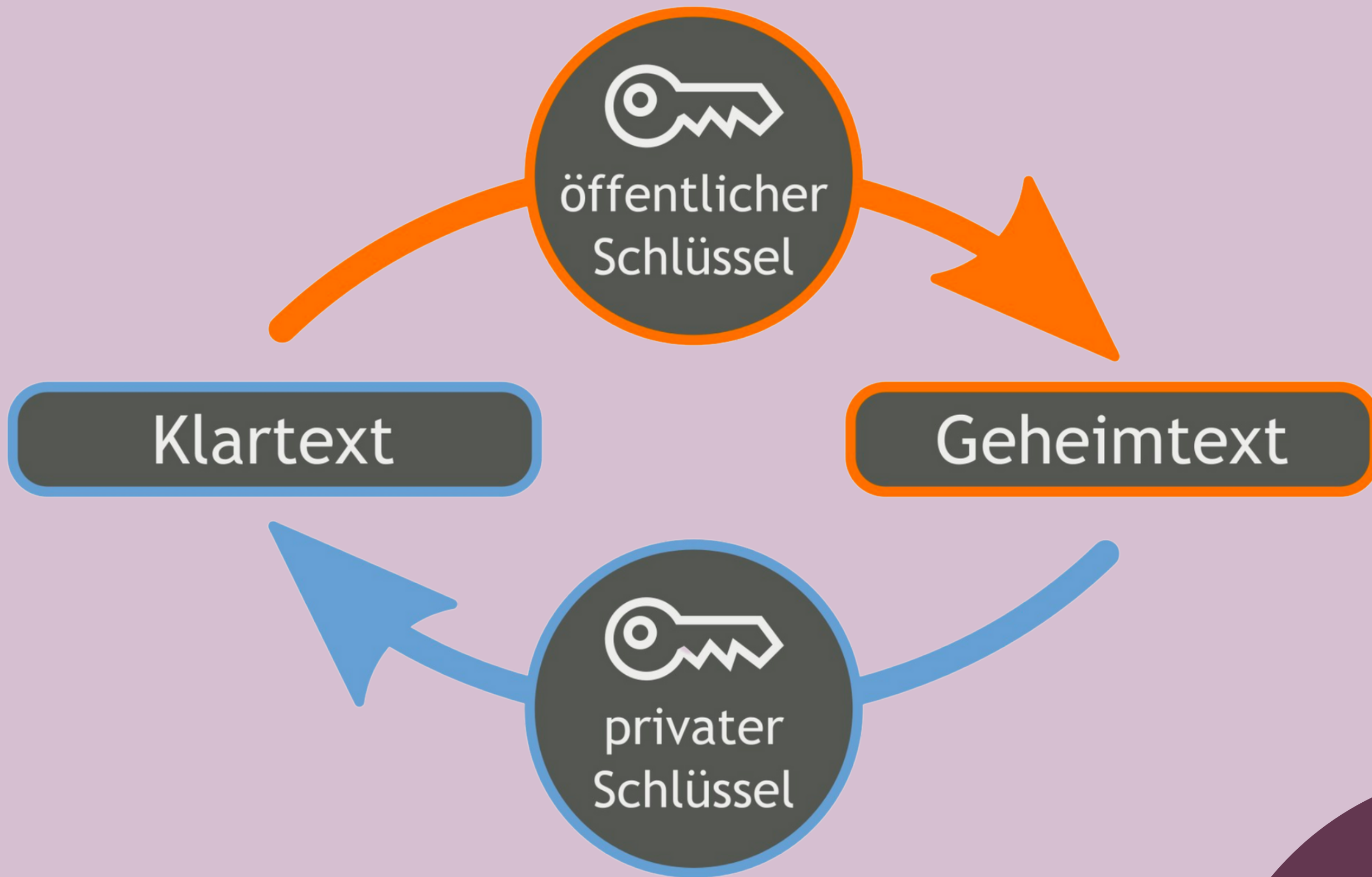
## Wie funktioniert die Verschlüsselung?

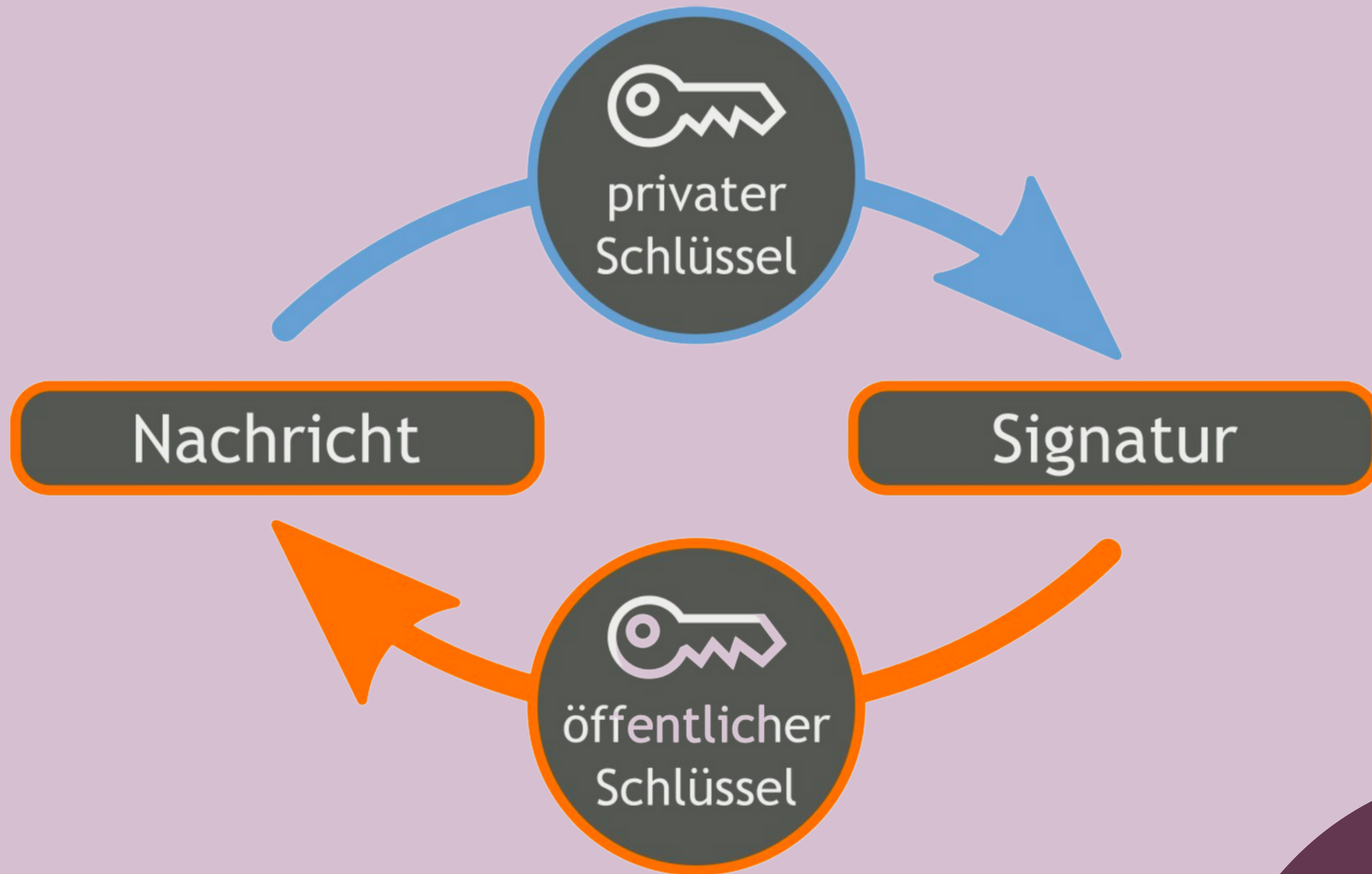


ENDE-ZU-  
ENDE-  
VERSCHLÜS-  
SELUNG







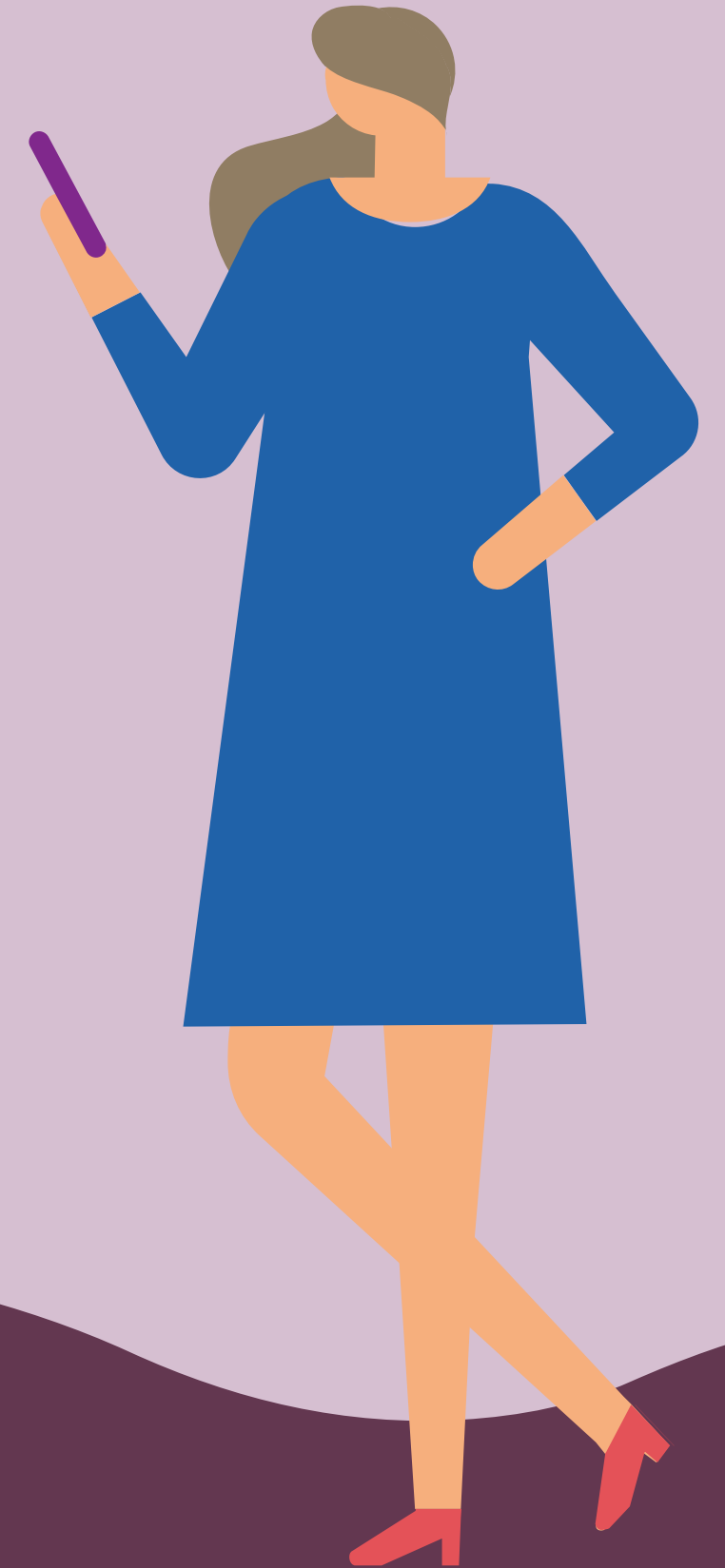




# Verschlüsselungs-Standards

OpenPGP: Offener Standard

S/MIME: Verbreiteter bei Unternehmen





# Variante 1: Verschlüsselte Anbieter



Tutanota<sup>®</sup>



Proton Mail

[matrix]





# Variante 2: Verschlüsselung im Client

Microsoft 365

Gmail

Thunderbird

Apple Mail



➤ Senden    Verwerfen    Anfügen    Signatur    **Verschlüsselung**

🔒 Nur verschlüsseln – Empfänger können diese Nachricht lesen, Inhalt daraus weiterleiten

Von: Alexander Baetz

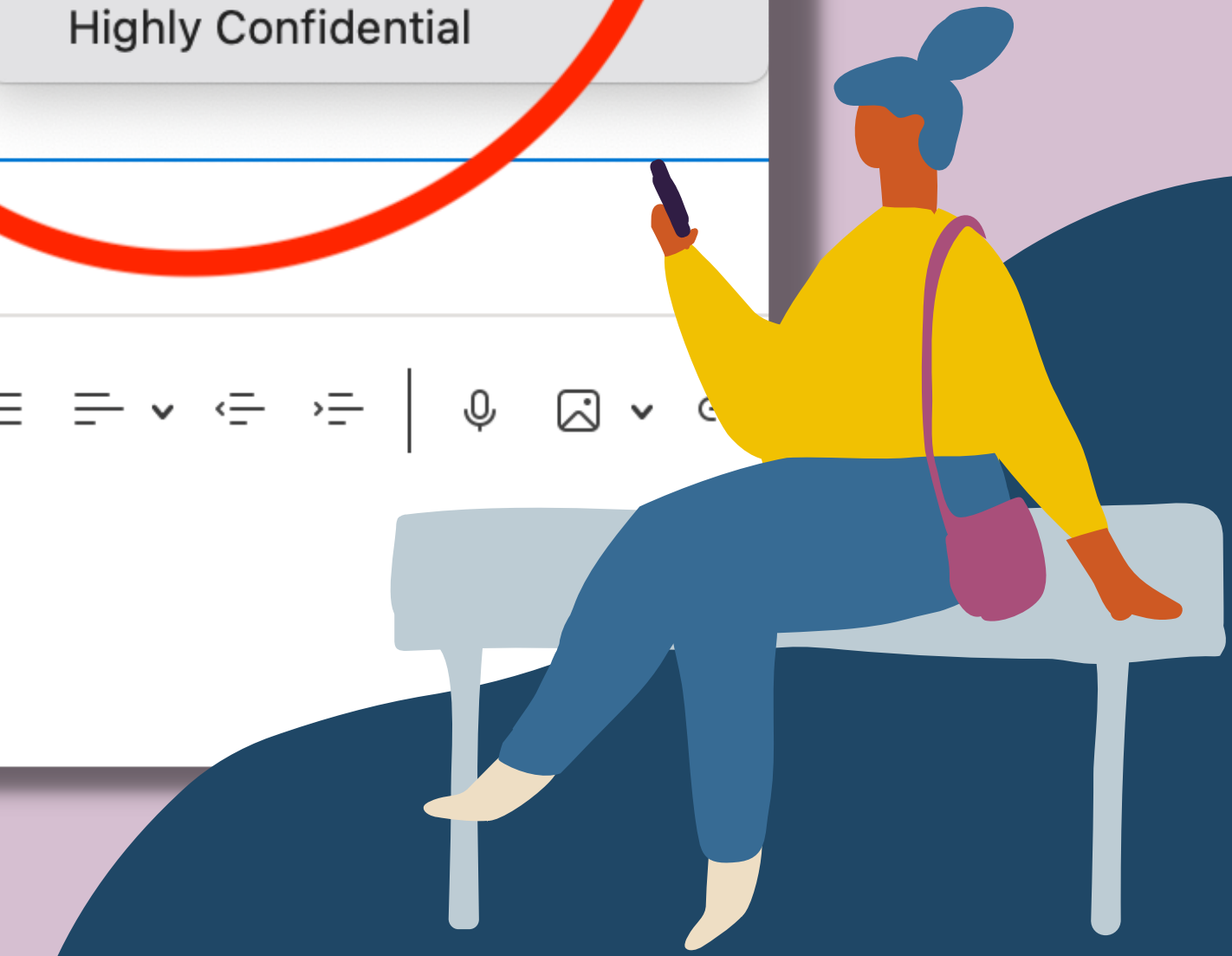
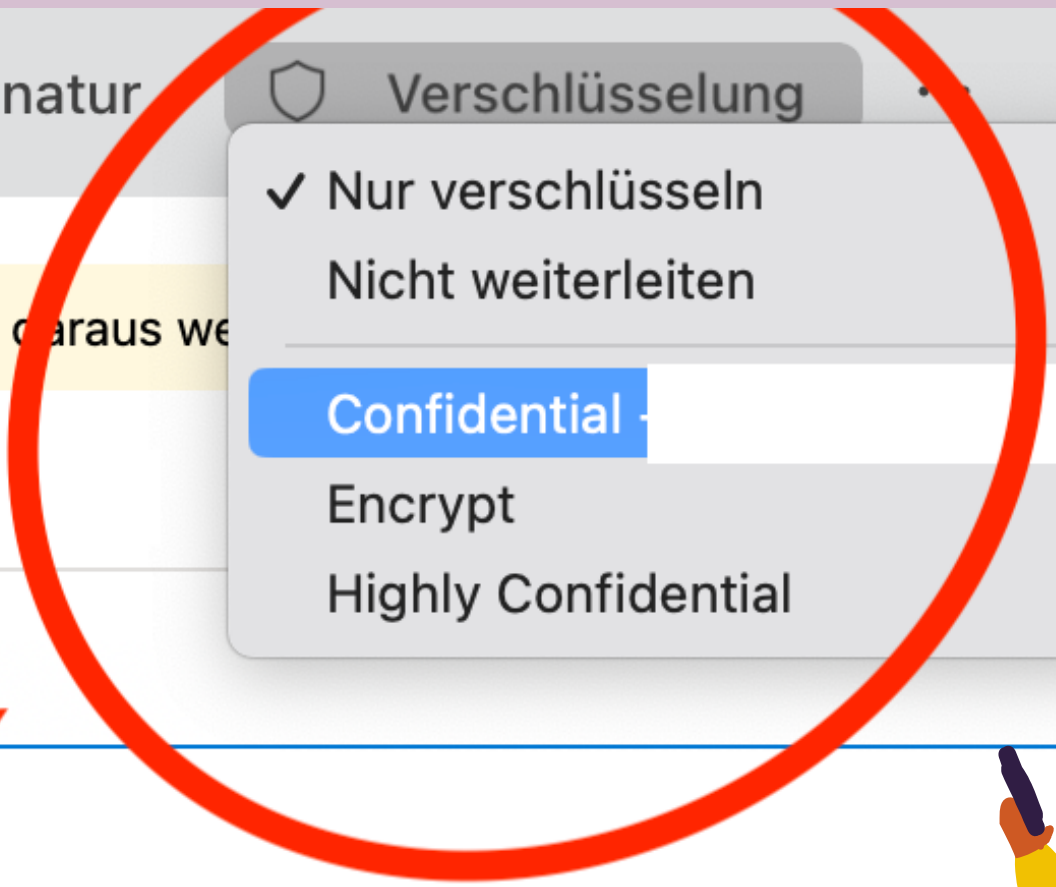
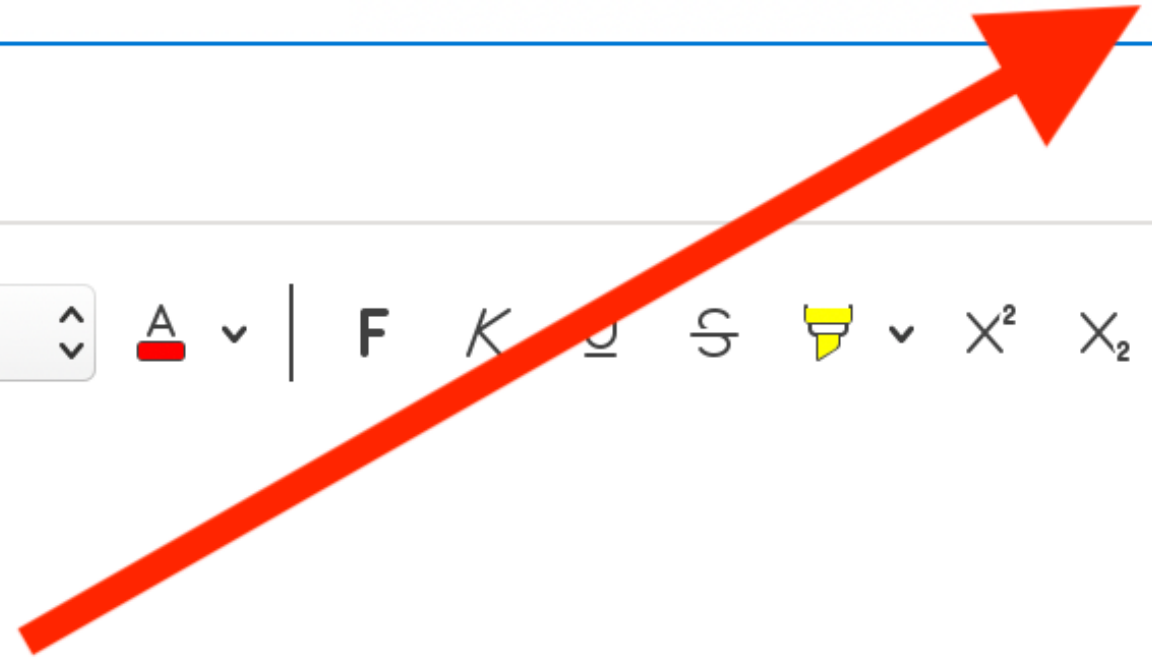
An:

Betreff:

Calibri (Textkör... 11

**F** *K* u S  $X^2$   $X_2$

- ✓ Nur verschlüsseln
- Nicht weiterleiten
- Confidential**
- Encrypt
- Highly Confidential







# Variante 3: Verschlüsselung im Web



Mailvelope



**Haben Sie  
Fragen?**

