

# Tipp: Backup Ihres PGP-Schlüssels anlegen

E-Mails, die von Ihren Kommunikationspartnern mit Ihrem öffentlichen Schlüssel verschlüsselt und dann unseren Servern übermittelt wurden, können nur mit dem passenden privaten Schlüssel und dem entsprechenden Passwort wieder in Klartext verwandelt werden. Dasselbe gilt, falls Sie das verschlüsselte Postfach aktiviert haben.

Wir, das Team von mailbox.org, haben keinen Ersatz- oder Zweitschlüssel. Ihre verschlüsselten E-Mails können wir sogar dann nicht dechiffrieren, wenn Sie Ihren privaten Schlüssel im Guard hinterlegt haben, da er wiederum durch ein Passwort geschützt ist. Wir verfügen über **keinerlei Möglichkeit**, den Klartext Ihrer E-Mails wiederherzustellen. Wenn wir das könnten, dann wäre Verschlüsselung sinnlos und für Sie auch kein Gewinn an Sicherheit.

Bitte bewahren Sie daher immer ein **Backup Ihres privaten Schlüssels** an einem sicheren Ort auf, beispielsweise in einer verschlüsselten Container-Datei! Für die zugehörigen Passwörter empfehlen wir ein Backup in einer verschlüsselten Passwortdatenbank wie KeePass oder KeePassX.

## Verwandte Artikel

- [YubiKey Neo als OpenPGP-Smartcard nutzen](#)
- [S/MIME beim verschlüsselten Postfach](#)
- [E-Mails von der automatischen Verschlüsselung ausnehmen](#)
- [E-Mail verschlüsselt - durch Absender oder verschlüsseltes Postfach](#)
- [Sind Kalender und Adressbuch verschlüsselt](#)