Verschlüsselte Kommunikation

Der Schutz Ihrer persönlichen Daten ist uns wichtig! Aus diesem Grund stellen wir Ihnen gerne eine datenschutzkonforme Art der Datenübermittlung für Sie bereit.

Bei Lindy nutzen wir das Verschlüsselungskonzept Pretty Good Privacy (PGP). Dieses beruht auf einer sogenannten Public-Key-Infrastruktur. Jeder Teilnehmer besitzt in diesem System ein Schlüsselpaar mit einem geheimen/privaten sowie einem öffentlichen Schlüssel.

Der von Lindy zur Verfügung gestellte öffentliche Schlüssel für die Mail-Adresse jobs@lindy.de, steht unter folgendem Link zum Download bereit:

https://www.lindy.de/$WS/ld0101/websale8_shop-ld0101/benutzer/templates/ws-customer-ld0101/servicepages/Medien/jobs_lindy_de_pub.asc

E-Mails nach PGP verschlüsseln: So geht's

In aller Regel hat Ihr Mailprovider (z.B. Mailbox.org oder WEB.de) bereits Vorkehrungen zur Verschlüsselung von E-Mails getroffen. Diese sind in den meisten Fällen schnell und einfach einzurichten. Bitte informieren Sie sich auf der Website Ihres Mailproviders oder dem Hersteller Ihres E-Mail Clients.

Allgemeine Vorgehensweise:

1. Sie besitzen eine E-Mail-Adresse deren Mailprovider bereits eine Verschlüsselung anbietet oder haben diese in einem E-Mail Client eingerichtet.
2. Laden Sie jetzt einen **passenden Verschlüsselungsclient** (z.B. GPG4Win oder Enigmail) herunter (passend zu Ihrem Mailprovider/E-Mail Client).
3. Nach der Installation bieten diese Programme die Möglichkeit, je ein Schlüsselpaar für jede angegebene E-Mail-Adresse zu erzeugen.
4. Hierbei müssen Sie ein **Passwort eingeben**. Dieses dient der Sicherheit ihres Schlüssels, für den Fall, dass der Schlüssel dennoch einmal in fremde Hände gerät.
5. Sie besitzen nun einen **öffentlichen Schlüssel** und einen **privaten Schlüssel.** Wie der Name schon sagt, sollte der private Schlüssel privat bleiben, sprich: auf Ihrem Rechner abgespeichert bleiben. Der öffentliche Schlüssel hingegen kann auf einen Schlüsselserver hochgeladen oder an jede E-Mail angehängt werden.
6. Das OpenPGP-Programm im Mailprogramm erkennt selbständig, wenn Sie eine verschlüsselte E-Mail erhalten.
7. Sie können verschlüsselte Mails nur verschicken, wenn Sie den **öffentlichen Schlüssel des Empfängers kennen.** Moderne GnuPG-Clients können prüfen, ob ein öffentlicher Schlüssel auf einem gängigen Schlüsselserver vorliegt.