# Datenschutz-Verfahren und Folterwerkzeuge

Übermedien: „Nach „Ausforschung“ von Journalisten: Datenschutz-Verfahren gegen Stasi-Unterlagenbehörde“.

Die Sache, die ursprünglich nur die Akte Lammel war, zieht immer weitere Kreise. „Wie nun bekannt wurde, hat Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), kurz nach der Veröffentlichung ein datenschutzrechtliches Prüfverfahren in die Wege geleitet. Dem Beauftragten für die Stasi-Unterlagen, Roland Jahn, wurde ein Fragenkatalog übersandt mit einer ungewöhnlich kurzen Bearbeitungsfrist von nur einer Woche. Seit dem 7. Mai liegt Jahns Antwort im Haus von Kelber vor. Sie bestätigte die Vorwürfe und Recherchen – und stellt den Bundesdatenschutzbeauftragten offenbar nicht zufrieden.“

Der Bundesdatenschutzbeauftragte hat Jahn und seiner Behörde offensichtlich die Folterwerkzeuge gezeigt, wenn weiter gemauert würde: *Im Anschluss hieran wird zu prüfen sein, ob die bisher durch BStU getroffenen Maßnahmen ausreichend sind, oder weiterer Handlungsbedarf besteht, der erforderlichenfalls auch mit aufsichtsrechtlichen Maßnahmen durchzusetzen wäre.* Dem Bundesdatenschutzbeauftragten stünden in diesem Falle umfangreiche Mittel zur Verfügung.“

„Grundlage für die nun eingeleitete Prüfung waren Hinweise darauf, dass Medienanträge einiger weniger Redaktionen in der Stasi-Unterlagenbehörde auch dann bearbeitet wurden, wenn sie erkennbar unzulässig waren – und so teils privateste Informationen die Behörde verließen.“

Als kleines Schmankerl kommt hinzu: Ulrich Kelber ist Sozialdemokrat. Die Jahn-Behörde unterliegt der Dienstaufsicht durch die Bundesbeauftragte für Kultur und Medien (BKM, aka

Kulturstaatsministerin) Monika Grütters, und die ist CDU. Da haben zwei ein Interesse, sich vor den Wahlen noch zu profilieren, und zu meinem Vergnügen nicht miteinander.

---

# Unter Faxern

Versendet hier jemand noch Faxe? (via Fefe) „Telefax ist nicht Datenschutz konform“.

---

# Offener Brief an den Vorstand des DJV Berlin – JVBB

Offener Brief an den Vorstand des DJV Berlin – JVBB

Liebe Kolleginnen und Kollegen des Vorstands des DJV Berlin – JVBB,

die Veröffentlichungen von BuzzFeed, Übermedien, Berliner Zeitung, Frankfurter Rundschau, mdr 360G, Turi2, HNA und Merkur über die unzulässige Ausforschung von Mitgliedern unserer Gewerkschaft durch die Behörde des Bundesbeauftragten für die Stasi-Unterlagen (BStU) aufgrund von Medienanträgen des rbb und der Bild-Zeitung sind dem Vorstand inzwischen sicher bekannt. Die Abfragen des rbb im Zeitraum von 2010 bis 2017 betreffen fast 50 Funktionäre des damaligen DJV Berlin aus sämtlichen Gremien wie Vorstand, Fachausschüssen und Ehrengericht – bei einzelnen Personen sogar rückwirkend bis zum Jahr 2000.

Der DJV-Bundesvorstand hat sofort nach Kenntnisnahme der Ergebnisse eines internen Prüfverfahrens der BStU den daraus ersichtlichen Aktenskandal öffentlich benannt und Konsequenzen von der dienstaufsichtführenden Staatsministerin für Kultur und Medien im Bundeskanzleramt, Monika Grütters, vom BStU und dem Bundesdatenschutzbeauftragten gefordert.

Der Vorstand unseres Landesverbandes will offenbar selbst nicht handeln und hat sich in dieser Frage – außer durch wenige Zeilen unseres Vorsitzenden Steffen Grimberg im Newsletter – bisher auch nicht geäußert. Das wirkt auf uns sehr befremdlich. Er sollte dafür sorgen, dass die Ausforschung von Mitgliedern unseres Verbandes, verbunden mit Verstößen gegen das Stasiunterlagengesetz (StUG), das Bundesdatenschutzgesetz und die Datenschutzgrundverordnung (DSGVO) nicht unter den Teppich gekehrt wird!

Die Unterzeichnenden waren Mitglieder des DJV Berlin und sind heute Mitglieder im DJV Berlin – JVBB. Wir alle wurden vom BStU unrechtmäßig ausspioniert. Das hat die Behörde in einem internen fachaufsichtlichen Gutachten selbst zugegeben. Was mit unseren Daten geschehen ist und wer immer noch darauf Zugriff hat, wissen wir nicht.

Wir erwarten vom Vorstand, Maßnahmen zu ergreifen, die Rechte seiner Mitglieder durchzusetzen. Dazu gehören Beschwerden beim Landesdatenschutzbeauftragten Berlin und beim Kultursenator, ebenso bei der Intendanz und Chefredaktion des rbb sowie bei der Verlagsgeschäftsführung des Springer-Verlags und der Chefredaktion der Bild-Zeitung. Wir verlangen, dass der Vorstand uns bei weiteren Schritten sowohl gegen den BStU als auch gegebenenfalls gegen die Bild-Zeitung und den rbb in Sachen Persönlichkeitsrecht und Datenschutz individuellen persönlichen Rechtsschutz gewährt.

Im Zuge eines Drittbeteiligungsverfahrens, das durch einen Antrag nach Informationsfreiheitsgesetz (IFG) der rbb-Reporterin Gabi Probst durch den IFG-Beauftragten der BStU

eingeleitet worden ist, sind sowohl die Medienanträge von Gabi Probst zu Mitgliedern des DJV Berlin als auch die behördeninternen Unterlagen zu den Ausforschungen offenkundig geworden. Die BStU hat in dem erwähnten Gutachten festgestellt, dass bereits die Medienanträge von rbb und Bild unzulässig waren.

Wir fordern, dass die Kollegin Gabi Probst ihr Amt im Aufnahmeausschuss niederlegt und dass der Vorstand sie dazu auffordert. Ihre Recherche-Methoden schädigen das Ansehen des Verbandes, auch angesichts der Presseberichte zu diesem Thema. Aus unserer Sicht ist der Fall Gabi Probst eine Angelegenheit für das Schiedsgericht des DJV Berlin – JVBB.

Mit kollegialen Grüßen

Simone Ahrend
Clemens Glade
Prof. Dr. Peter Kolbe
Inge Kundel-Saro
Bernd Lammel
Caroline Methner
Ann Schäfer
Burkhard Schröder
Dr. Wolf Siegert

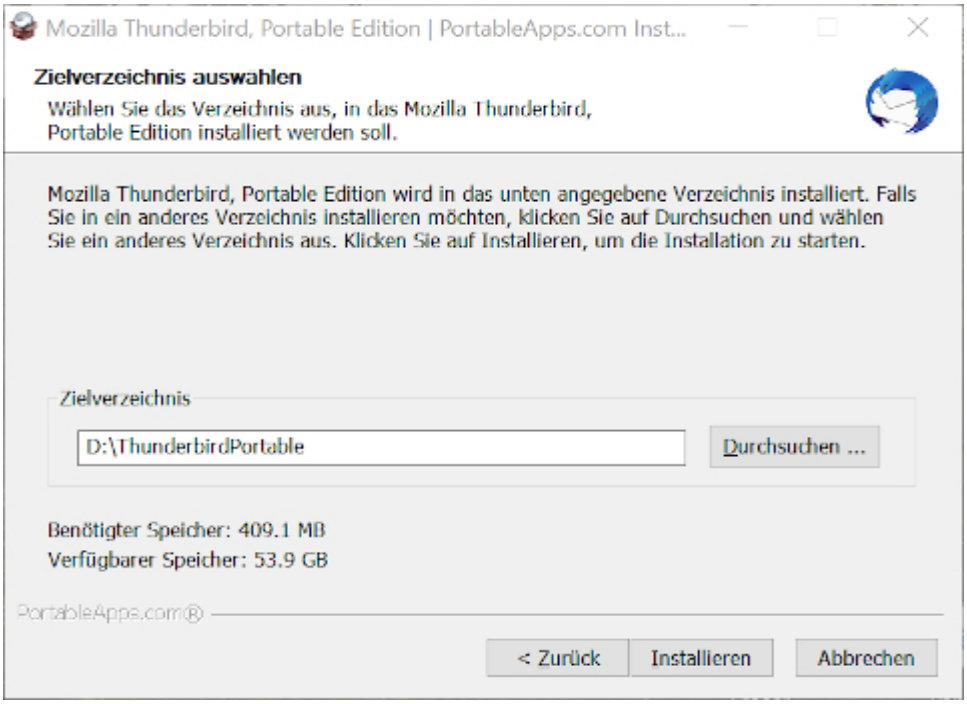
---

# Kein gutes Signal

Vielen Dank an das nerdige Publikum!

---

# E-Mails verschlüsseln [Thunderbird Portable auf einem USB-Stick]




Neues Tutorial auf der Website des Vereins *German Privacy Fund:* E-Mails verschlüsseln [Thunderbird Portable auf einem USB-Stick, Windows].

---

# Tutorial: E-Mails verschlüsseln per Browser und Mailvelope

*Ich habe ein neues Tutorial von der Website des Vereins German Privacy Fund kopiert und bitte das sachverständige Publikum zu kommentieren, zu berichtigen und auf Fehler hinzuweisen.*

**Lernziele:**
**– Installieren des Browser-Add-ons Mailvelope**
**– (einmaliges) Erzeugen eines Schlüsselpaares,**
**– Export und Import öffentlicher Schlüssel,**
**– Senden einer verschlüsselten E-Mail.**
**Dauer: ca. 30 Minuten**

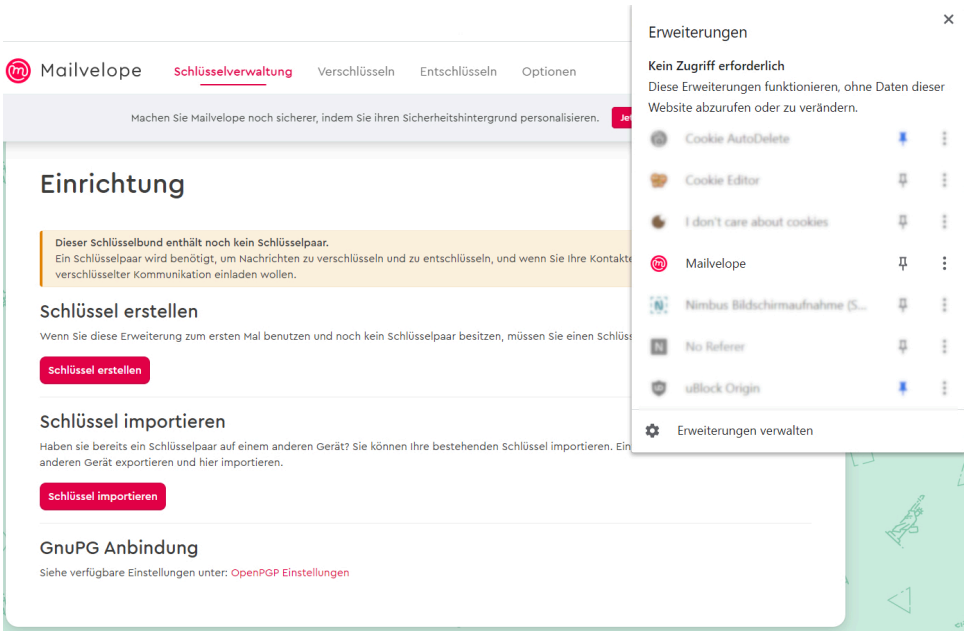

Zeitaufwand: fünf Minuten (und etwas Zeit zum Downloaden des Add-ons)
Schwierigkeitsgrad: leicht

Installieren Sie das Browser-Add-on Mailvelope für Chrome (Windows) und Chromium (Linux) – Mailvelope für Firefox (Windows) und Firefox (Linux) – Mailvelope für Microsoft Edge (Windows) – Mailvelope für Opera.

**Hinweise:**
– Das Add-on funktioniert für alle Browser und Betriebssystem fast identisch.
– Mailvelope gibt es auf für das MacOS-Mail-Programm Mail , aber nur kombiniert mit GPGtools (das jedoch ist nicht gratis).
– Ihr Provider muss das Feature unterstützen, die meisten großen Provider tun das.
– Diejenigen, mit denen Sie verschlüsselt kommunizieren wollen, müssen Mailvelope *nicht* benutzen, nur GnuPG oder E-Mail-Programme wie Thunderbird, die das Verschlüsselungsprogramm implementiert haben.
– Mailvelope funktioniert *nicht* bei Browsern mobiler Endgeräte.
– Die „häufig gestellte Fragen“ (FAQ) auf der Website von Mailvelope und das Tutorial sind hervorragend und selbsterklärend. Sie würden jedoch zwei Wochen brauchen, um alles zu lesen. Das Wichtige wird nicht vom weniger Wichtigen getrennt.

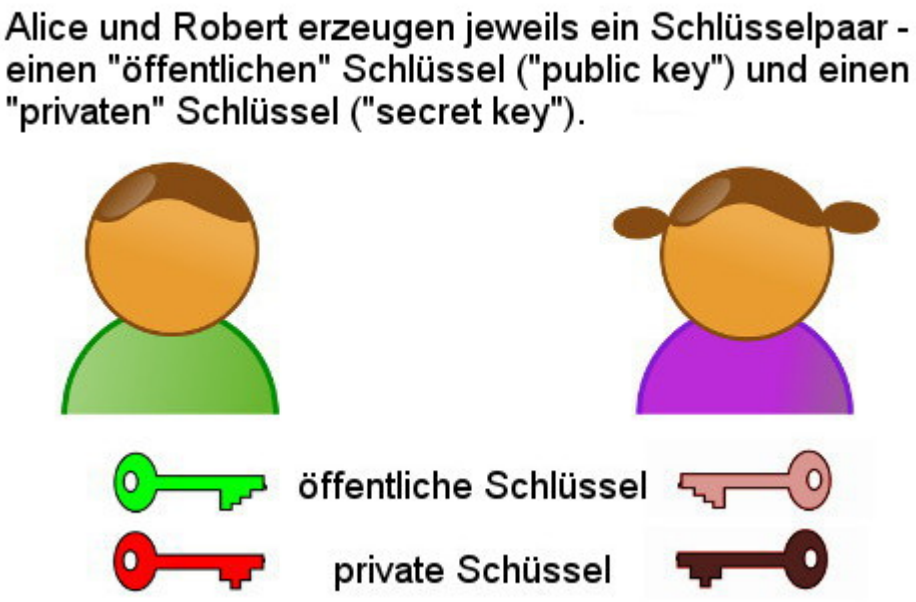
## Vor- und Nachteile von Mailvelope

Sie sollten dieses Add-on nur benutzen, wenn Sie ihre E-Mails ausschließlich per Webmail, also mit dem Browser lesen. Sie müssen Mailvelope aber auf jedem der von Ihnen genutzten Browser installieren und auch Ihr Schlüsselbund dorthin kopieren – eine Alternative ist nur copy & paste eines schon verschlüsselten Textes in das geöffnete Webmail-Fenster. Das kann mühsam werden. Wenn Sie aber schon GnuPG und dessen Feature *Kleopatra* installiert haben, können Sie genau das (copy & paste) auch von dort aus tun und brauchten Mailvelope nicht.




Die Grafik anklicken, um sie zu vergrößern.


## Erzeugen eines Schlüsselpaares – eines *öffentlichen* und eines *privaten* Schlüssels.



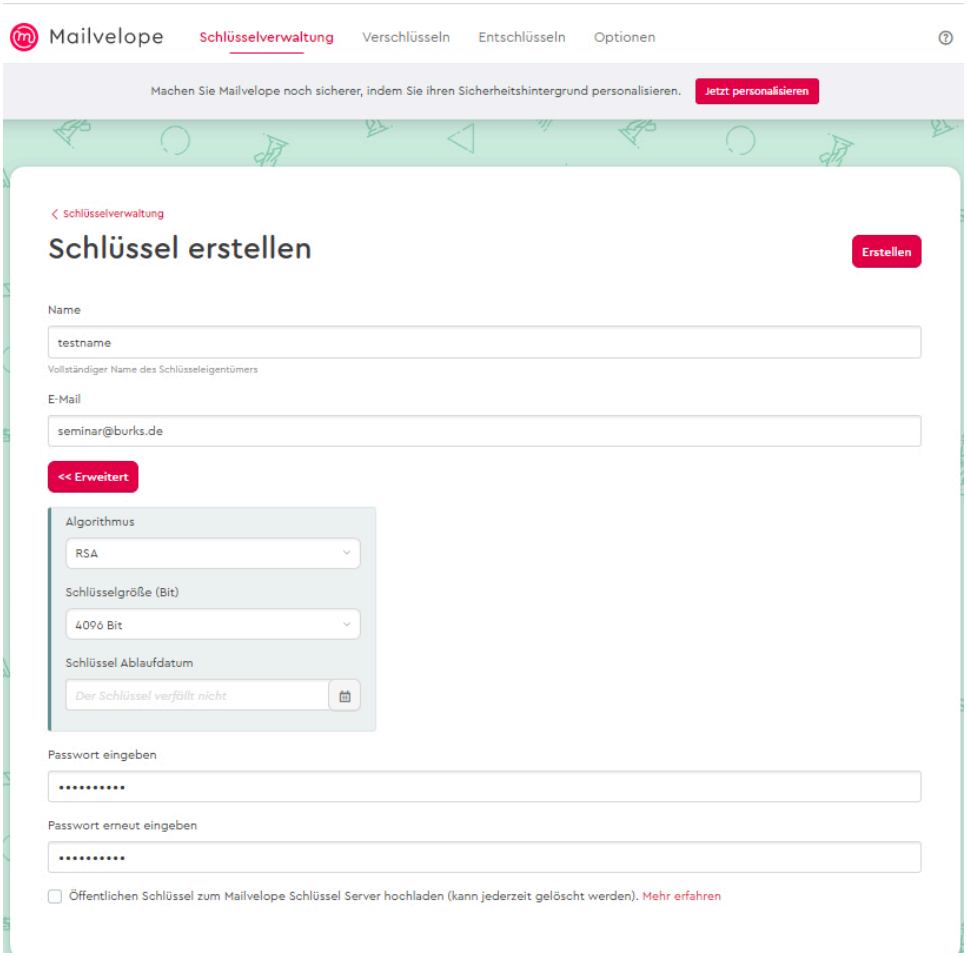

5 MINUTEN

Zeitaufwand: fünf Minuten
Schwierigkeitsgrad: leicht

Nur Verschlüsselungssysteme, die mit einem öffentlichen Schlüssel („public key“) und einem privaten Schlüssel („private key“) arbeiten, sind sicher – so wie dieses.

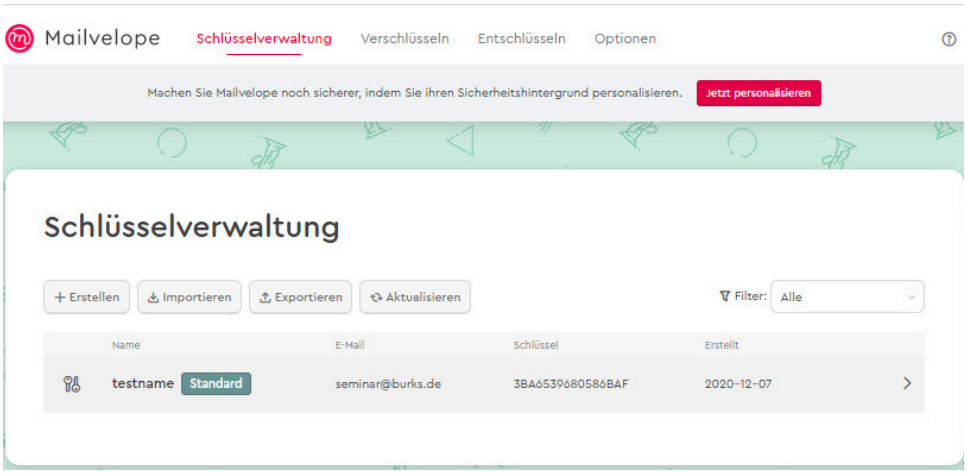
Rufen Sie Mailvelope auf – es versteckt sich oben rechts in der Leiste, wo Sie vielleicht schon andere Add-ons installiert haben und sieht aus wie ein Klecks oder ein Blatt. Sie können alle Menüs bzw. Optionen des Add-ons Mailvelope vorerst ignorieren, außer Schlüssel verwalten“ und „Schlüsselbund“ (zwei Wörter für eine Opion).

Sie *erstellen* jetzt ein Schlüsselpaar (oder importieren ein schon vorhandenes). Sie können auch einen Testschlüssel erstellen, den sie später wieder löschen.




Die Grafik anklicken, um sie zu vergrößern.

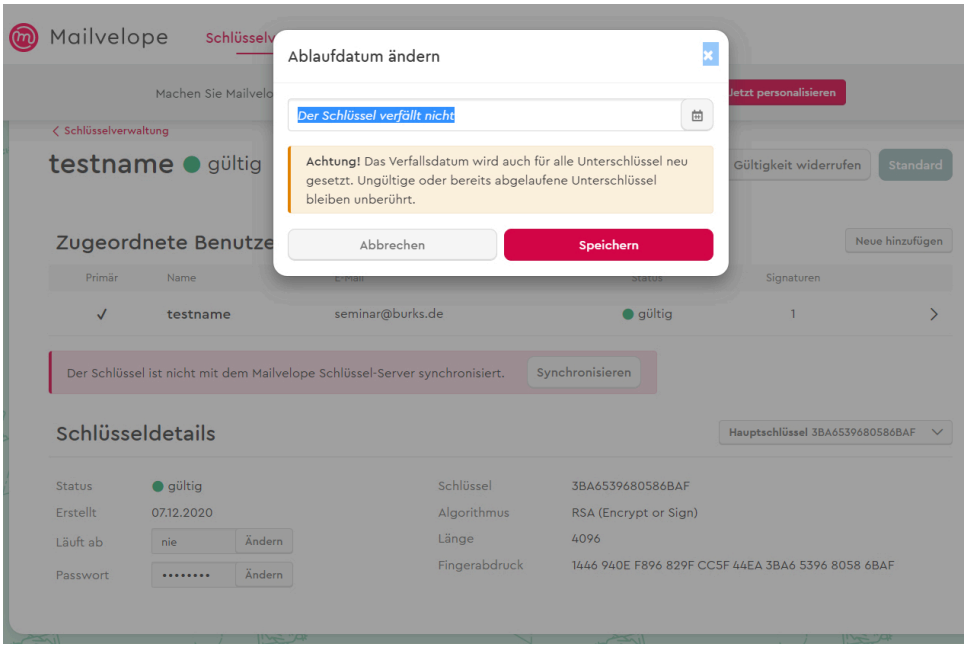
Folgen Sie den Anweisungen, die sind auch für Laien verständlich. Es sind auch Schlüssel ohne Passwort möglich, wir empfehlen das nicht.




Die Grafik anklicken, um sie zu vergrößern.

Sie müssen jetzt nicht (wenn überhaupt) mit dem Schlüsselserver von Mailvelope synchronisieren. Dieses Feature werden Sie vermutlich nie benötigen.

Im Beispiel oben haben wir einen Schlüssel „testname“ mit der E-Mail-Adresse seminar@burks.de erzeugt. In der Grafik unten sehen Sie dessen Eigenschaften, zum Beispiel den „Fingerprint“, eine Art unveränderliche „Quersumme“.




3. SCHRITT

## Exportieren des eigenen öffentlichen Schlüssels – Importieren „fremder“ öffentlicher Schlüssel

5 MINUTEN

Zeitaufwand: fünf Minuten
Schwierigkeitsgrad: leicht

Um starten zu können, müssen Sie jetzt den *öffentlichen* Schlüssel derjenigen Person, mit der sie verschlüsselte E-Mails tauschen wollen, *importieren* sowie Ihren eigenen *exportieren* und den offen verschicken. Den Fehler, den *geheimen* Schlüssel zu exportieren und zu versenden, können Sie nicht machen, weil Mailvelope davor warnt. (Das Feature brauchen Sie nur für eine Sicherheitskopie Ihres Schlüsselpaares.)


Die Grafik anklicken, um sie zu vergrößern.

Bei diesem Beispiel haben wir den öffentlichen Schlüssel von burks@burks.de genommen, Sie können aber auch den von unserem Impressum nehmen (rechte Maustaste, speichern unter).

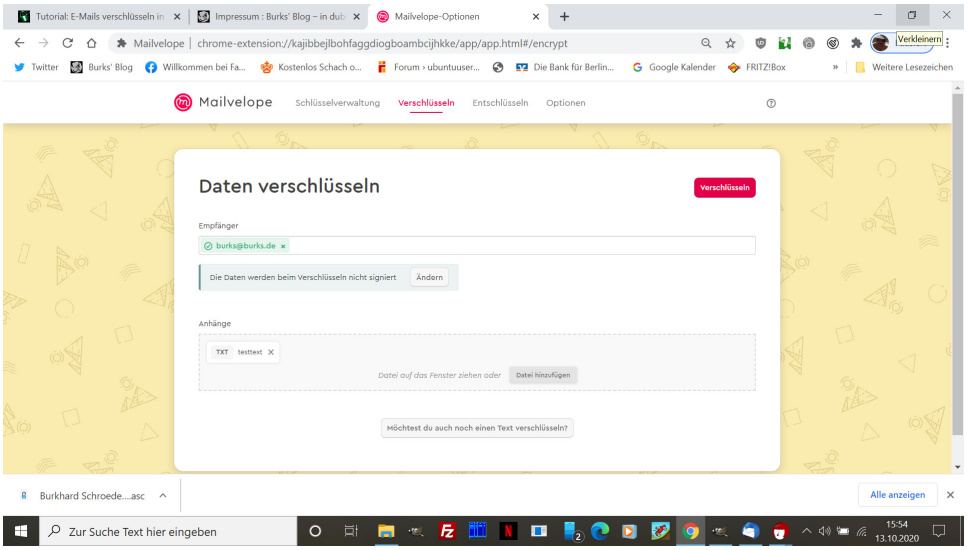
4. SCHRITT

## Senden einer verschlüsselten E- Mail

5 MINUTEN

Zeitaufwand: fünf Minuten

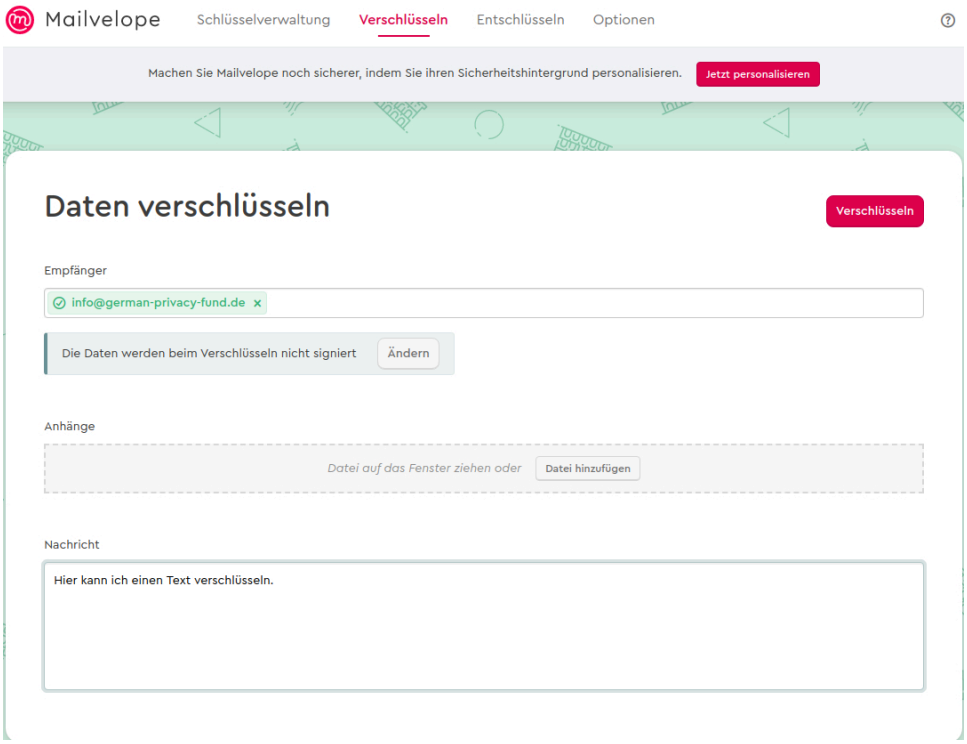
Schwierigkeitsgrad: leicht



Die Grafik anklicken, um sie zu vergrößern.

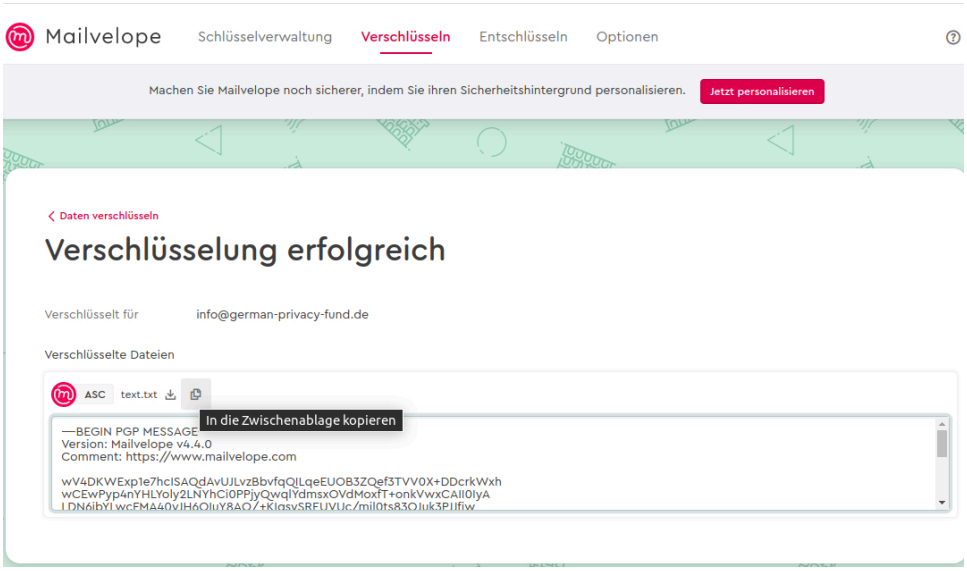
Sie können Dateien verschlüsseln (vgl. Grafik oben) und per Attachment versenden oder einen Text im Webmail-Fenster Ihres Browsers (unten).

Das Feature, den Text einer E-Mail zu verschlüsseln, verbirgt sich leider unter „Datei verschlüsseln“ und dann unter dem Button „möchtest du auch einen Text verschlüsseln?“ Dann erst öffnet sich ein Textfeld.



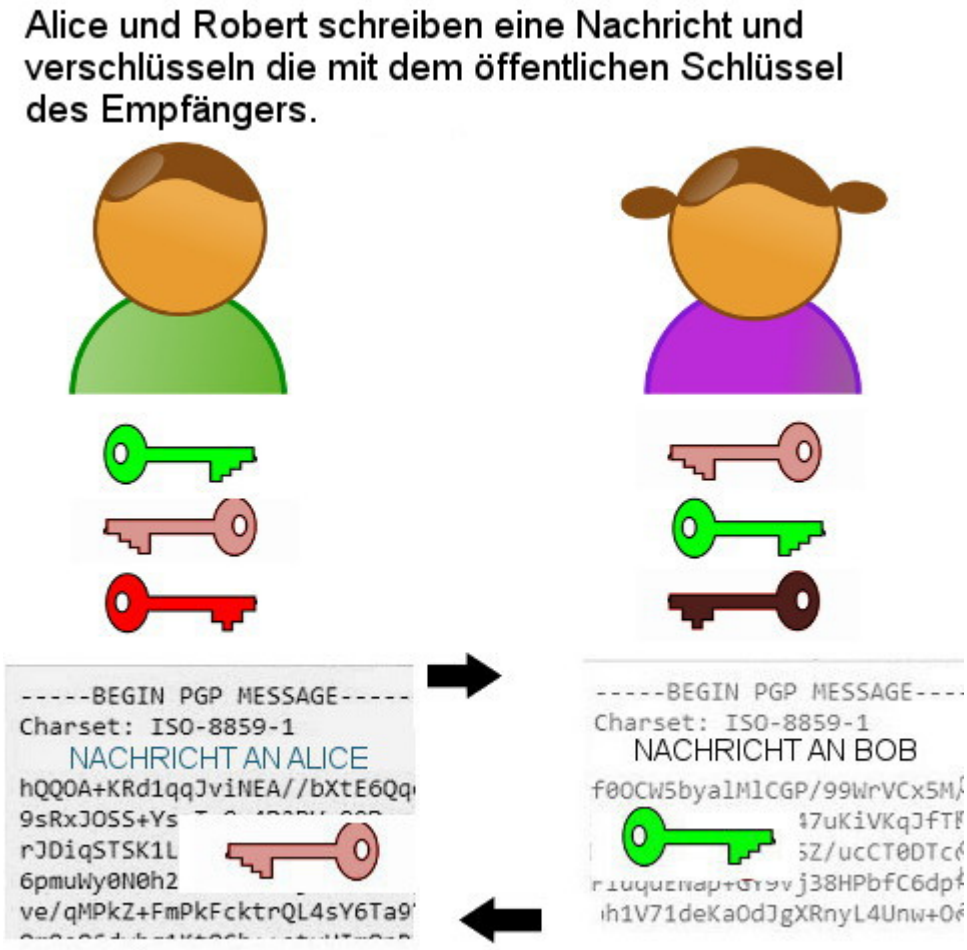

Die Grafik anklicken, um sie zu vergrößern.

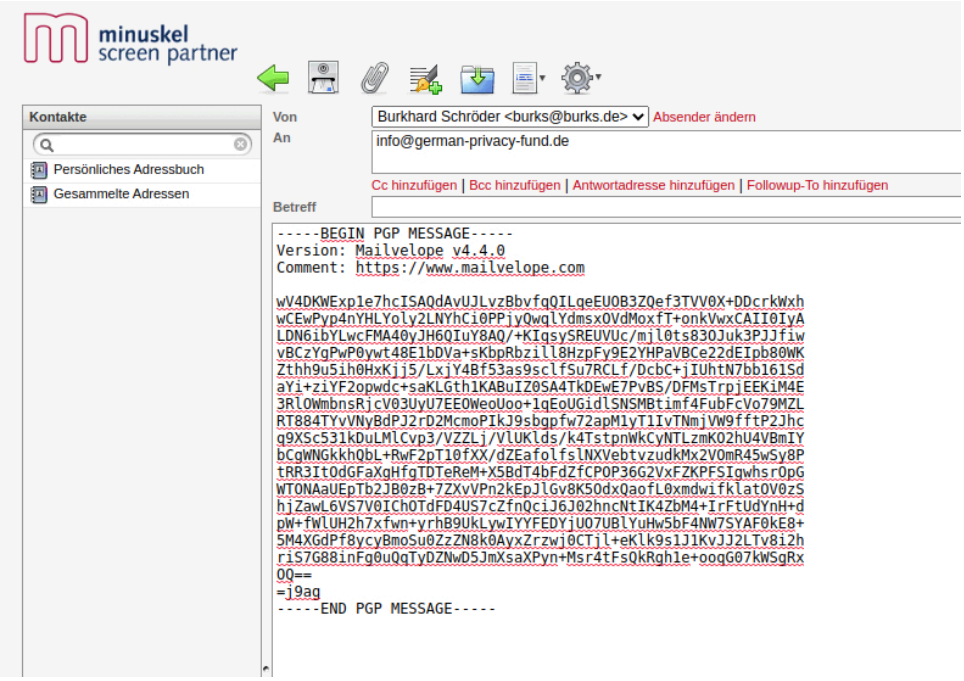
Wenn Sie den Klartext geschrieben haben, wählen Sie den Empfänger anhand seiner E-Mail-Adresse aus. Dessen Schlüssel müssen Sie schon vorher in ihr Schlüsselbund importiert haben. Dann drücken Sie auf den roten Button „verschlüsseln“ – und der Text verwandelt sich in Datensalat.



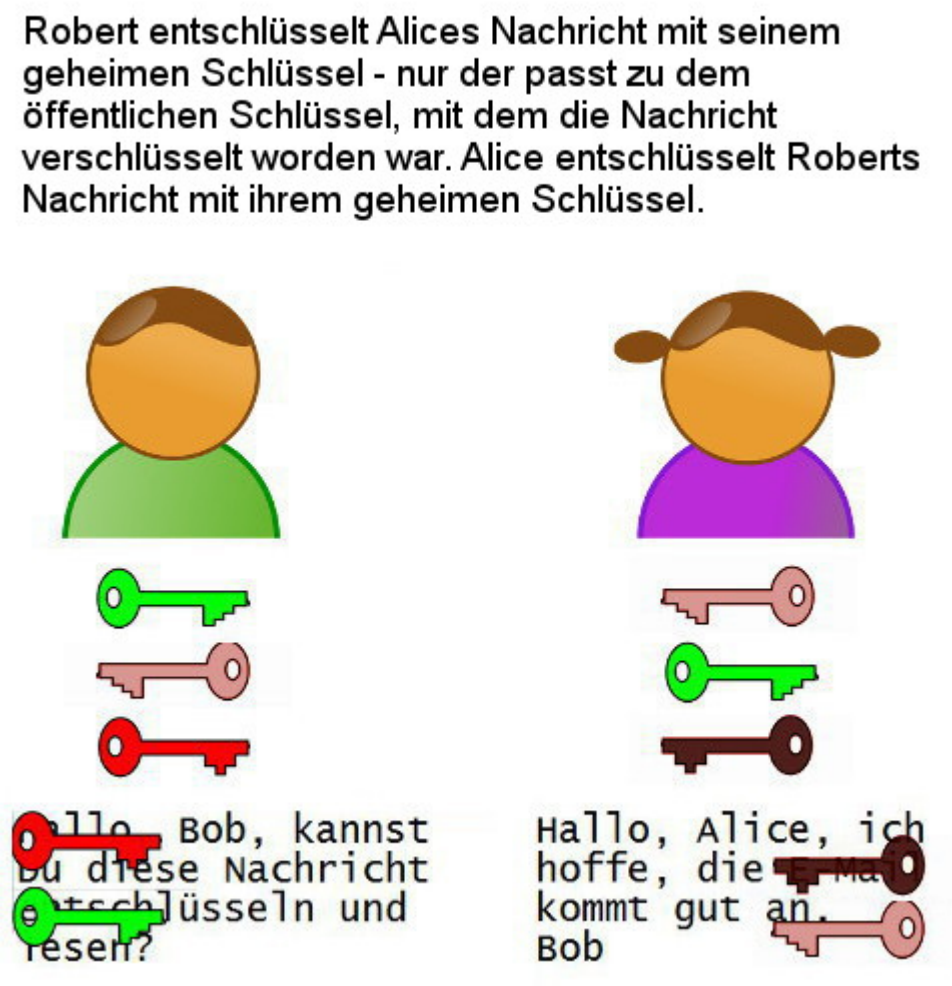

Die Grafik anklicken, um sie zu vergrößern.

Den verschlüsselten Text kopieren Sie in das Webmail-Feld Ihres Browsers. Nur derjenige, der im Beispiel (Grafik unten) den *geheimen* Schlüssel des Empfängers info@german-privacy-fund.de hat, könnte die Nachricht wieder entschlüsseln.



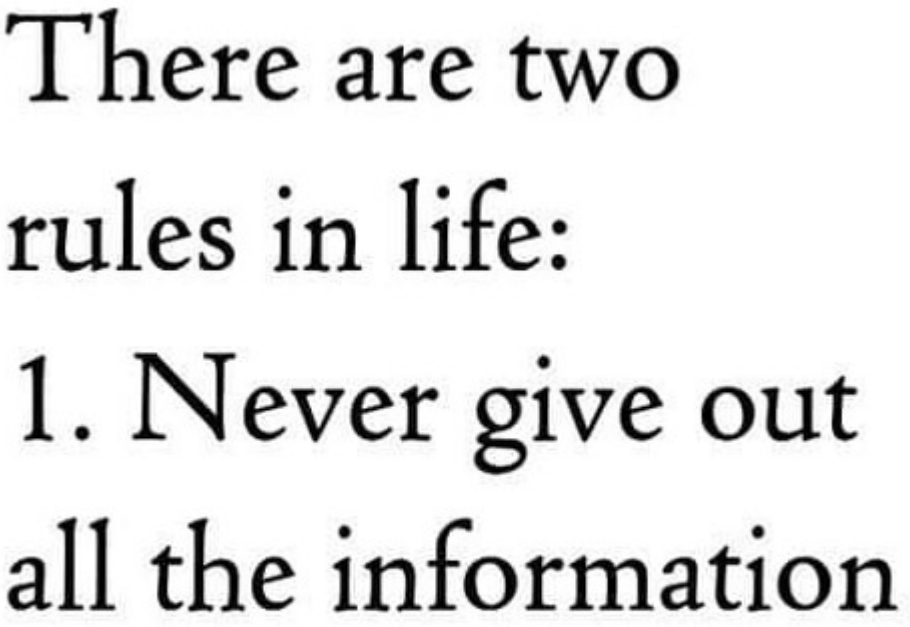



Die Grafik anklicken, um sie zu vergrößern.




Last update: 08.12.2020

# Mehr Sand ins Getriebe!




– Die Möglichkeiten des Staates, zur Strafverfolgung oder Terrorabwehr auf persönliche Daten von Handy- und Internetnutzern zuzugreifen, sind verfassungswidrig. Laut Urteil des Bundesverfassungsgerichts ist die Eingriffsschwelle nicht verhältnismäßig geregelt.

– DerEuGH kippt die EU-US-Datenschutzvereinbarung „Privacy Shield“. – „Mit einem lange erwarteten Urteil hat der Europäische Gerichtshof (EuGH) am Donnerstag den transatlantischen „Privacy Shield“ und damit eine der wichtigen Rechtsgrundlagen für den Transfer personenbezogener Daten europäischer Bürger in die USA für nichtig erklärt. Grund dafür sind in den Vereinigten Staaten bestehende Gesetze, die Sicherheitsbehörden weitreichende Befugnisse zur

Überwachung „ausländischer Kommunikation“ in die Hand geben.“

---

# □□□□□!?

| Location | How long did it take for the number of total confirmed deaths to double? | Total confirmed deaths<br>ECDC data. Up to date for 10 AM (CET) on March 22. | Daily new confirmed deaths<br>ECDC data. Up to date for 10 AM (CET) on March 22. |
|---|---|---|---|
| World | doubled in 7 days | 12,942 total<br>March 22 | +1,690 new<br>March 22 |
| Italy | doubled in 5 days | 4,827 total<br>March 22 | +795 new<br>March 22 |
| China | doubled in 36 days | 3,267 total<br>March 22 | +6 new<br>March 22 |
| Iran | doubled in 6 days | 1,556 total<br>March 22 | +123 new<br>March 22 |
| Spain | doubled in 3 days | 1,326 total<br>March 22 | +324 new<br>March 22 |
| France | doubled in 3 days | 562 total<br>March 22 | +112 new<br>March 22 |
| United States | doubled in 2 days | 340 total<br>March 22 | +80 new<br>March 22 |
| United Kingdom | doubled in 3 days | 233 total<br>March 22 | +56 new<br>March 22 |
| Netherlands | doubled in 3 days | 136 total<br>March 22 | +30 new<br>March 22 |
| South Korea | doubled in 13 days | 104 total<br>March 22 | +1 new<br>March 22 |
| Belgium | doubled in 2 days | 67 total<br>March 22 | +30 new<br>March 22 |
| Germany | doubled in 3 days | 67 total<br>March 22 | +22 new<br>March 22 |

Natürlich sind die wohlwollenden Leserinnen und geneigten Leser genau so informiert wie ich über die gegenwärtige Pandemie, wenn nicht sogar besser, weil alle vor den Geräten

hängen. Wie vorhergesagt, steigt die Rate der Infektionen auch hierzulande exponentiell, weil geeignete Maßnahmen viel zu spät und und zu halbherzig getroffen wurden.

Auch wenn so genannte Experten noch im Januar abwiegelten: COVID-19 ist nicht mit Influenza vergleichbar. In Italien lässt man Leute in meinem Alter mittlerweile elend verrecken.

Mal sehen, ob unserer herrschende Klasse und die hiesigen Medien ihre ~~antikommunistischen~~ sinophoben Vorurteile ablegen kann und die Hilfe Chinas annimmt.

Die Volksrepublik China hat alles richtig gemacht, auch wenn es einem bei der High-Tech-Überwachung, die eingesetzt wird, gruselt. (Übrigens: Li Wenliang wurde posthum rehabilitiert. Hoffentlich lernen die was daraus.)

---

# We have updated our privacy policy

---

# #metoo


Mein Beitrag zur #metoo-Diskussion.

---

# Nix auf Vorrat

Ich zitiere mal den Schockwellenreiter: „Klatsche für die GroKo: Gericht stoppt Vorratsdatenspeicherung“. Quod erat demonstrandum. Aber sie werden es wieder und wieder versuchen.

---

# Gehacktes

Wenn ich in Mainstream-Medien lesen, dass wieder etwas „gehackt“ wurde, weiß ich, dass sich in 95 Prozent der Fälle jetzt der Bullshit-Faktor um ein Vielfaches erhöht. „Twitter-Accounts wurden gehackt“ oder so ähnlich. Fast so realistisch wie eine Online-Durchsuchung, ohne dass das „Opfer“ das vorher willentlich oder aus Dummheit gestattet hat.

Wer wissen will, wie man das macht, braucht nur auf diversen Websites nachlesen, was das ~~Spionage~~ Analyse-Tool „The Counter“ alles tun darf, mit dem sich jetzt jemand Zugang zu den Passwörtern der „Opfer“ verschafft hat. Da bleibt kein Auge trocken. Wer sich so eine App installiert, verdient kein Mitleid, sondern sollte zur Strafe ein Jahr lang nur mit Lynx surfen dürfen.

---

# Keep cool and safe


Nur Heise berichtet nüchtern und sachlich über die neuesten Enthüllungen von Wikileaks. Jürgen Kuri, der schon beim Thema „Online-Durchsuchungen“ als einer der wenigen Journalisten einen kühlen Kopf bewahrt hatte, bringt es auf den Punkt: „Da trommelt ja Wikileaks ganz schön für Zeugs, das eigentlich wenig Substanz für neue Erkenntnisse hat. Und die CIA spioniert aus Botschaften und Konsulaten heraus? Welche Sensation! Dass nun manche gleich wieder übertreiben müssen und die Verschlüsselung etwa für Signal als geknackt berichten, obwohl es in den Dokumenten nur darum geht, über Sicherheitslücken Smartphones zu kapern, macht das Ganze auch nicht wirklich besser.“

Nein, Signal ist weiterhin sicher. Und vieles andere auch. Das Problem sitzt immer vor einem Monitor und hat zwei Ohren.

Man muss es deutlich sagen: Zeit online lügt. Die CIA kann *nicht* jedes Telefon „hacken.“ Die FAZ lügt: der amerikanische Geheimdienst CIA Menschen kann *nicht* Telefone „offenbar nach Belieben ausspähen“ („Offenbar“? Soll das Journalismus sein?)

Zur weiteren Lektüre empfehle ich Monika Ermert (Heise) und Bruce Schneier.

PS: Wie viele Menschen, die „was mit Medien“ machen, schicken mir verschlüsselte E-Mails?

---

# Dumm, dümmer, grün

„Auch die Grünen benutzten eine stark veraltete Softwareversion, die zahlreiche Angriffsflächen bietet, reagierten aber auf die BSI-Warnung nicht. Gegenüber dem SPIEGEL verwies die Partei nun darauf, man plane, die Installation bald abzuschalten; man habe dort “insbesondere‘ Wahlkampfmaterialien gelagert. Die Plattform werde „bei einem externen Dienstleister betrieben, der auch für die Sicherheit verantwortlich“ sei. ‚Insofern war von unserer Seite keine Reaktion notwendig.'“