

DATENSCHUTZ IM SPORTVEREIN

E-MAILVERSAND

PERSONENBEZOGENER DATEN

KAPITEL 4 – §64 – ANFORDERUNG AN DIE SICHERHEIT DER DATENVERARBEITUNG

- ▶ Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

PERSONENBEZOGENE DATEN

- ▶ Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. "Identifizierbar" ist eine Person dann, wenn sie direkt oder indirekt, vor allem mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder anderen besonderen Merkmalen identifiziert werden kann. Die **Möglichkeit** der Identifizierung einer Person reicht hier aus!

WIE KANN ICH DAS ERREICHEN

- ▶ **Verschlüsselung der gesamten e-Mail mit GPG**
- ▶ **Verschlüsseln von Office-Dateien**
- ▶ **Verschlüsseln mit Hilfsprogrammen**

GPG – GNU PRIVACY GUARD

- ▶ **kostenloser Download**

<https://www.gpg4win.de>

- ▶ **Handbuch**

<https://files.gpg4win.org/doc/gpg4win-compendium-de.pdf>

- ▶ **Wie funktioniert verschlüsseln I**

Man verschlüsselt (wie einen Raum abschliessen) die Nachricht immer mit dem öffentlichen Schlüssel des Empfängers.

Zum Entschlüsseln (Der Raum wird wieder aufgeschlossen) wird der private Schlüssel beim Empfänger genutzt.

Auch der Absender kann die Nachricht nach der Verschlüsselung nicht mehr lesen! (Im Gesendet Ordner verbleibt allerdings immer eine unverschlüsselte Version)

GPG – GNU PRIVACY GUARD

▶ **Wie funktioniert verschlüsseln II**

Es gibt 2 Schlüssel, einen zum Aufschliessen und einen zum Abschiessen.

Der Schlüssel zum Abschiessen ist öffentlich und kann von jedem benutzt werden.

Der Schlüssel zum Aufschliessen gehört nur dem Empfänger und sollte auch nur von diesem genutzt werden.

Die nächste Seite zeigt ein Beispiel, wenn Eva eine verschlüsselte Nachricht an Adam sendet.

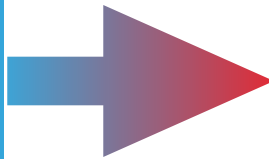
GPG – GNU PRIVACY GUARD

► Wie funktioniert verschlüsseln III

Ausgangstext

Hallo Adam,
der Apfel ist köstlich.
LG Eva

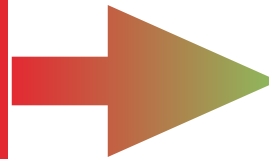
Mit Adams öffentlichem
Schlüssel wird verschlüsselt



Nach Verschlüsselung

LOREM IPSUM DOLOR SIT AMET,
CONSETETUR SADIPSCING ELITR,
SED DIAM NONUMY EIRMOD TEMPOR
INVIDUNT UT LABORE ET DOLORE
MAGNA ALIQUYAM ERAT,

Jeder, der die Nachricht
unterwegs abfängt sieht
nur den verschlüsselten
Text.



Nach Entschlüsselung

Hallo Adam,
der Apfel ist köstlich.
LG Eva

Mit Adams privatem
Schlüssel wird entschlüsselt

GPG – GNU PRIVACY GUARD

▶ **Wie funktioniert verschlüsseln IV**

Ich kann nur verschlüsseln, wenn der Empfänger ein Schlüsselpaar hat und der öffentliche Schlüssel zugänglich ist.

Manchmal muss man den Empfänger nach dem öffentlichen Schlüssel fragen.

VERSCHLÜSSELN VON OFFICE-DATEIEN

▶ Grundlage

Der Gesetzgeber schreibt nur vor, dass die Daten vor dem Zugriff Dritter während des Transportes geschützt werden müssen.

Um dem Gesetz genüge zu tun reicht es also aus, Office-Dateien mit einem Kennwort zu schützen.

Auch wenn man dieses Kennwort knacken kann habe wir aber die gesetzlichen Vorgaben erfüllt, denn das Knacken stellt wiederum eine kriminelle Handlung dar.

VERSCHLÜSSELN VON OFFICE-DATEIEN

▶ Teil I

Öffnen Sie die Datei, um die es geht.

Öffnen Sie das Menü **Datei** und klicken Sie bei **Informationen** auf **Dokument schützen/Mit Kennwort verschlüsseln**.

In Excel finden Sie dasselbe unter **Arbeitsmappe schützen** und sogar bei PowerPoint heisst es **Präsentation schützen**.

Tippen Sie ein Kennwort ein, das Sie sich sehr gut merken müssen.

Nach der Eingabe des Kennworts klicken Sie auf **OK** und tippen das Kennwort zwecks Bestätigung noch einmal ein.

Klicken Sie auf Speichern. Das Viereck bei Dokument (oder Arbeitsmappe) schützen wird gelb hervorgehoben. Dies ist das Zeichen, dass die Datei jetzt verschlüsselt ist.

VERSCHLÜSSELN VON OFFICE-DATEIEN

▶ Teil II

Öffnen Sie die Datei erneut, wird Office nach dem Kennwort fragen. Wie schon erwähnt: Ohne das Kennwort bekommen Sie diese Datei **nicht** wieder geöffnet.

Zum Entfernen des Kennworts öffnen Sie die Datei.

Anschliessend erneut zu **Datei/Dokument schützen/Mit Kennwort verschlüsseln**.

Löschen Sie die (nicht lesbaren) Zeichen des vorhandenen Passworts, indem Sie das Passwortfeld einfach per Delete-Taste leeren. Klicken Sie auf OK. Die farbliche Hervorhebung bei «Dokument schützen» verschwindet. Schliessen und speichern Sie das Dokument, dann ist der Kennwortschutz wieder aufgehoben

VERSCHLÜSSELN VON OFFICE-DATEIEN

▶ Teil III

Hinweis:

Wenn man sich die Passworte nicht alle merken möchte, oder sie auch nicht auf diversen Zetteln notieren will kann man einen sog. Passwort-Manager benutzen.

<https://keepass.info>

VERSCHLÜSSELN MIT HILFSPROGRAMMEN

▶ **Encrypto**

kostenloses Programm, welches sowohl auf dem Mac als auch unter Windows läuft.

<https://macpaw.com/encrypto>

▶ **Bitlocker**

Dies ist ein in den Pro-Versionen von Windows enthaltenes Programm um neben einzelnen Dateien auch ganze Platten zu verschlüsseln.

VERSCHLÜSSELN MIT HILFSPROGRAMMEN

- ▶ **TrueCrypt**

kostenloses Programm, welches seit 2014 zwar nicht mehr weiterentwickelt wird, aber immer noch eine gute Alternative darstellt.

- ▶ **VeraCrypt**

Der Nachfolger von TrueCrypt.

- ▶ **TruPax** und auch **Folder Access**



**VIELEN DANK FÜR IHRE
AUFMERKSAMKEIT**

**HANS-PETER DÖLLE
EDV-BERATUNG DÖLLE
MOERSER STR. 103
40667 MEERBUSCH**

[HTTPS://WWW.EDV-BERATUNG-DOELLE.DE](https://www.edv-beratung-doelle.de)

02132 / 91 11 02