

Empfehlungen zum sicheren Versand von Dokumenten per E-Mail

Oktober 2005

Herausgeber:

AvenirSocial
Professionelle Soziale Arbeit Schweiz
Schwarztorstrasse 22, PF/CP 8163
3001 Bern
T. +41 (0) 31 382 28 22
F. +41 (0) 31 382 11 25
info@avenirsocial.ch
www.avenirsocial.ch

Autor:

Urs Vogel

Quellen:

www.edsb.ch; www.datenschutz-zug.ch; www.datenschutz.ch

Januar 2006

Allgemeines

Die Kommunikation via elektronische Medien ist aus dem Arbeitsalltag nicht mehr wegzudenken. Speziell für den Sozialbereich ist jedoch, dass es sich dabei in den meisten Situationen um den Datentransfer von besonders schützenswerten Personendaten (Art. 3 lit. c DSGVO: gemeint sind z.B. Daten über Gesundheit, Intimsphäre und Massnahmen sozialer Hilfe) handelt. Ob der elektronische Mailverkehr gewählt wird, ist auf Grund der Vertraulichkeit der Information zu entscheiden. Für streng vertrauliche Dokumente (z.B. Gutachten, Sozialberichte etc.) ist der Briefverkehr oder die persönliche Übergabe einer elektronischen Zustellung auf jeden Fall vorzuziehen.

Besonders schützenswerte Personendaten dürfen keinesfalls unverschlüsselt¹ via E-Mail versendet werden, da die unverschlüsselte E-Mail-Kommunikation via Internet weniger vertraulich ist als der Versand einer Postkarte!

E-Mail-Botschaften und ihre Anhänge sind auf dem Übertragungsweg an vielen Orten für Dritte einsehbar, können kopiert und verändert werden. Zudem besteht mit der Automatisierung der E-Mailprogramme die Gefahr, dass durch Unachtsamkeit E-Mail-Nachrichten an falsche Adressaten geschickt werden.

Besondere Vorkehrungen sind deshalb notwendig, um die Kommunikation per E-Mail entsprechend den Anforderungen der Datenschutzgesetzgebung sicher zu gestalten.

¹ d.h. mit einem Passwort geschützt (siehe dazu weiter unten)

Generelle Vorkehrungen

Zu unterscheiden ist zwischen der E-Mail-Nachricht und den angehängten Dokumenten. In der E-Mail-Nachricht, den Betrefflinien und im Dokumentnamen dürfen keine Namen oder andere Daten erscheinen, welche Rückschlüsse auf die betroffene Person ermöglichen (z.B. Institutionsnamen, Initialen, Geburtsdatum). Die angehängten Dokumente, welche die konkreten Informationen enthalten (Word, Excel, Access, PowerPoint, andere Dateiformate etc.), sind zu verschlüsseln.

E-Mailverkehr im Intranet

Grössere Organisationen, staatliche Institutionen, Gemeinden, Kantonsverwaltungen etc. verfügen in vielen Fällen über ein Intranet (Datenverkehr über einen internen Server). Gegenüber aussenstehenden Dritten gilt das Intranet, sofern die entsprechenden Sicherheitsvorkehrungen getroffen sind, als sicher gemäss Datenschutzgesetzgebung. Dies bedeutet, dass der interne elektronische Postverkehr grundsätzlich geschützt ist. Da es sich bei den Daten aus dem Sozialbereich aber um besonders schützenswerte Personen- und Sachdaten handelt, ist es auch hier notwendig, die Dokumente mit den Personen- und Sachinformationen nur verschlüsselt zu versenden, denn Fehlleitungen und unbefugte Einsicht innerhalb der Organisation sind auch hier möglich.

E-Mailverkehr im Internet

Im Internet (Datenverkehr über einen externen Server) dürfen die Dokumente mit den besonders schützenswerten konkreten Personen- und Sachdaten in jedem Fall nur verschlüsselt gesendet werden. Auch Terminvereinbarungen, Kurzmitteilungen unter Bezug auf Namen oder Orte sind zu verschlüsseln, es sei denn, es handle sich um allgemeine, allen zugängliche Informationen (Öffnungszeiten, Ferienabwesenheiten etc.).

Möglichkeiten der sicheren Verschlüsselung

Neben den Vollverschlüsselungsprogrammen (wie z.B. PGP¹) gibt es einfache Möglichkeiten, Dokumente sicher zu verschlüsseln und damit den Anforderungen der Datenschutzgesetzgebung zu genügen. Die einzelnen Dokumente, welche im Anhang der E-Mails geschickt werden, können individuell mit einem Passwort verschlüsselt werden und sind damit vor unbefugtem Zugriff geschützt.

Folgende Voraussetzungen sind bei der Wahl eines sicheren Passwortes zu beachten:

- Das Passwort muss mindestens 8 Zeichen beinhalten.
- Gross- und Kleinbuchstaben sind zu verwenden und mit Zahlen und Sonderzeichen zu vermischen.
- Das Passwort darf kein gewöhnliches Wort - auch nicht in einer Fremdsprache - sein.

Zu empfehlen sind Passwörter, welche aus den Anfangsbuchstaben von Wörtern eines Satzes zusammengestellt sind. So sind die Anforderungen an die Gross- und Kleinschreibung sowie die Vermischung mit Zahlen und Sonderzeichen gewährleistet, und zudem können diese Passwörter problemlos an Hand des Satzes memoriert werden.

Beispiel: IhiK5Yu3Eg (Ich habe im Kühlschrank fünf Yoghurt und drei Eier gesehen)².

Unerlässlich ist, dass die Passwörter dem Empfänger auf sicherem Weg zugestellt werden. Dies kann mündlich, via Telefon oder mittels gewöhnlicher Briefpost geschehen, keinesfalls aber via E-Mail.

Im Folgenden werden zwei Arten der Verschlüsselung vorgestellt. Die erste befasst sich mit der Verschlüsselung einzelner Dokumente der Office-Produkte (Word, Excel, Access, Powerpoint etc.), die zweite erfordert die Installation des WinZip-Programms (kostenlose Testversion erhältlich³).

¹ <http://www.pgpi.org/>

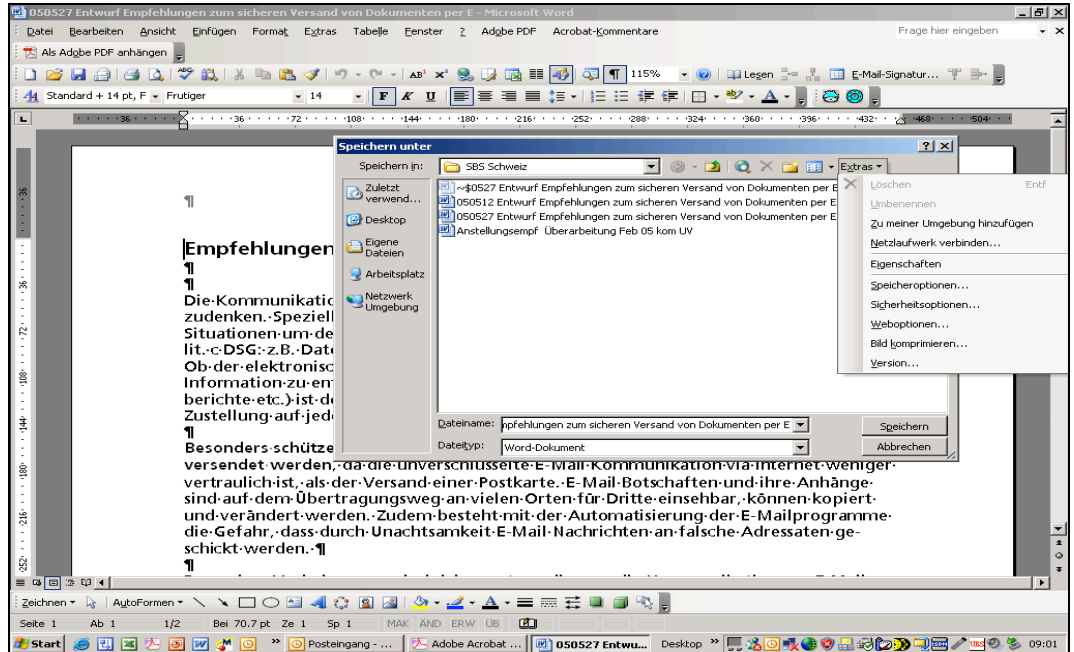
² <https://passwortcheck.datenschutz.ch/check.php?lang=de>

³ <http://www.winzip.com/downwz.htm>

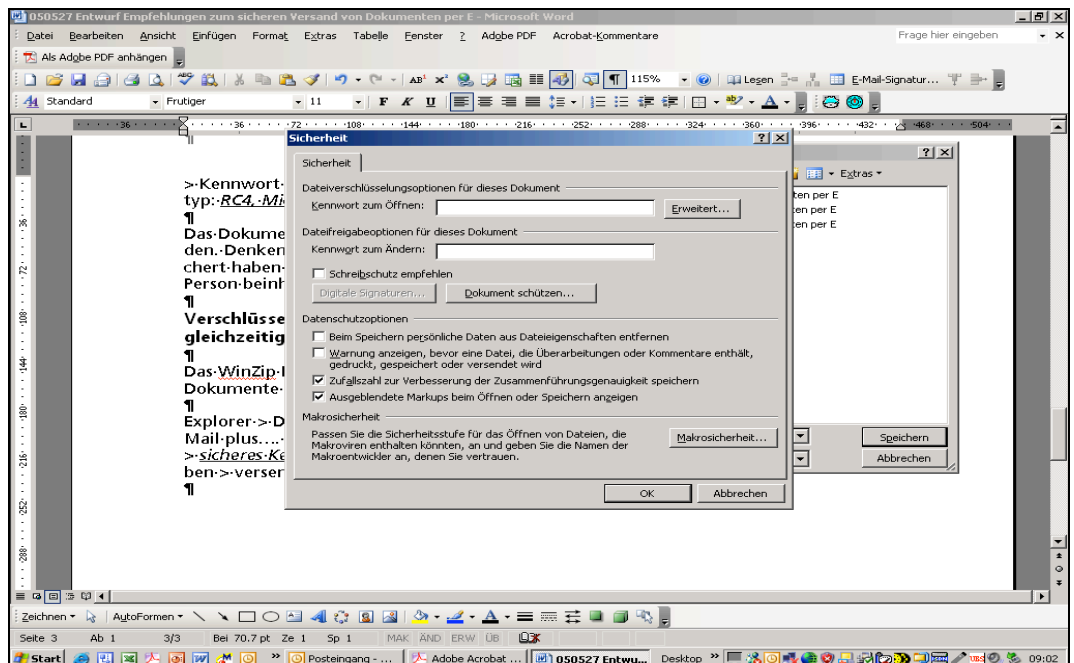
Verschlüsseln eines Office-Dokuments

Schreiben Sie das Dokument oder öffnen Sie ein bereits bestehendes Dokument. Starten Sie die Verschlüsselung, indem Sie in Ihrem PC folgende Schritte ausführen (durch Punkte klicken):

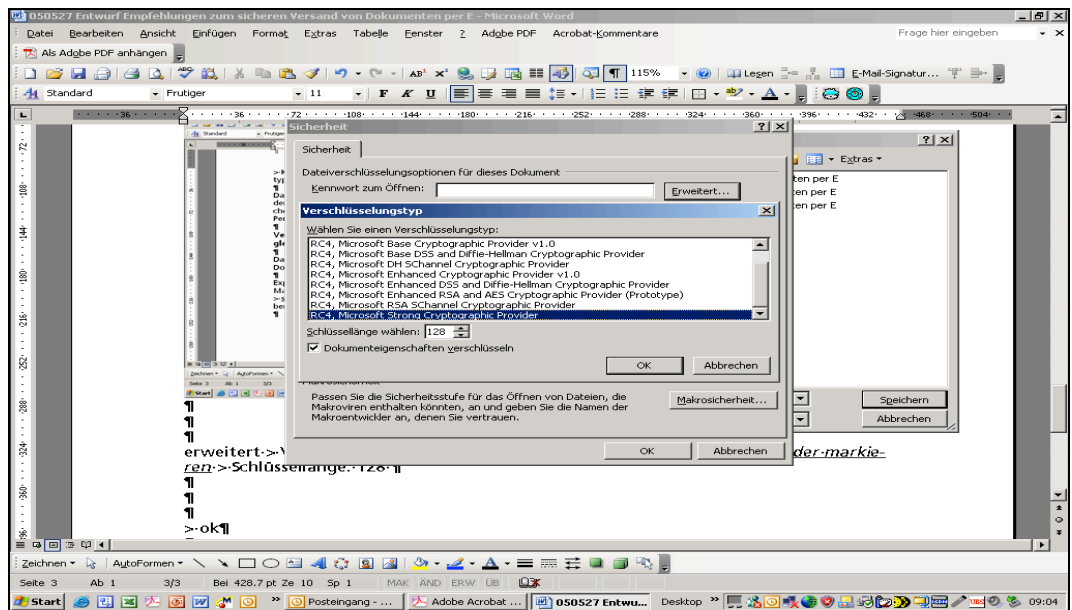
1. Datei (Menuliste) > Speichern unter... > Extras > Sicherheitsoptionen... >



2. > Sicherheit/ Kennwort zum Öffnen: *sicheres Kennwort eingeben* >



3. (zusätzliche Option, sonst zu Schritt 4 gehen) > Erweitert... > Verschlüsselungstyp: RC4, Microsoft Strong Cryptographic Provider markieren > Schlüssellänge: 128 wählen > ok >



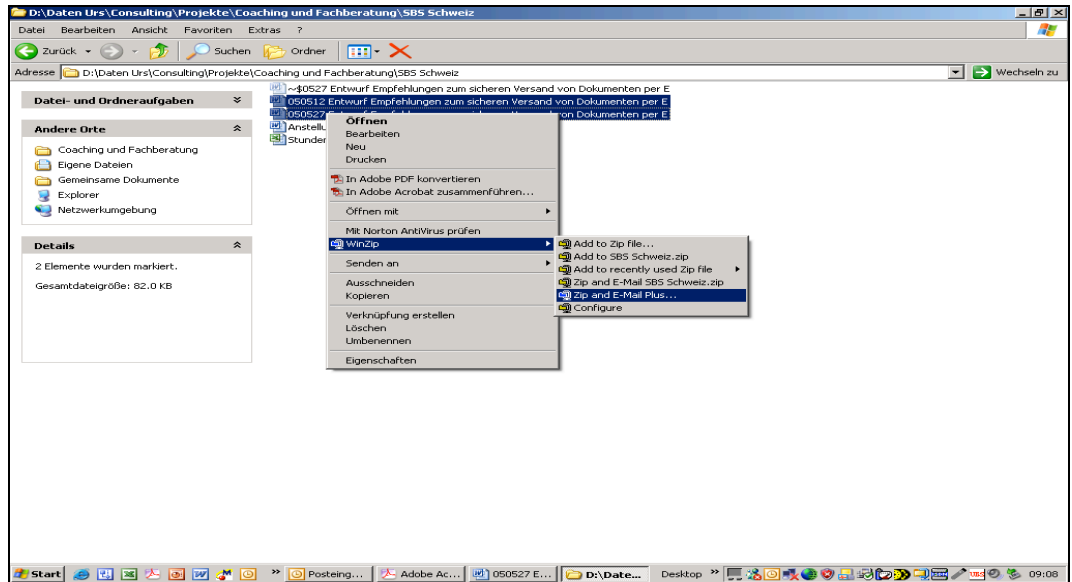
4. > Kennwort bestätigen: *Kennwort erneut eingeben* > ok > ok > speichern.

Das Dokument ist somit verschlüsselt und kann an die E-Mail-Nachricht angehängt werden. Denken Sie daran, dass der Dokumentname, unter dem Sie das Dokument gespeichert haben, und die Betreffzeile des E-Mails keine Namen oder Daten der betroffenen Person beinhalten dürfen.

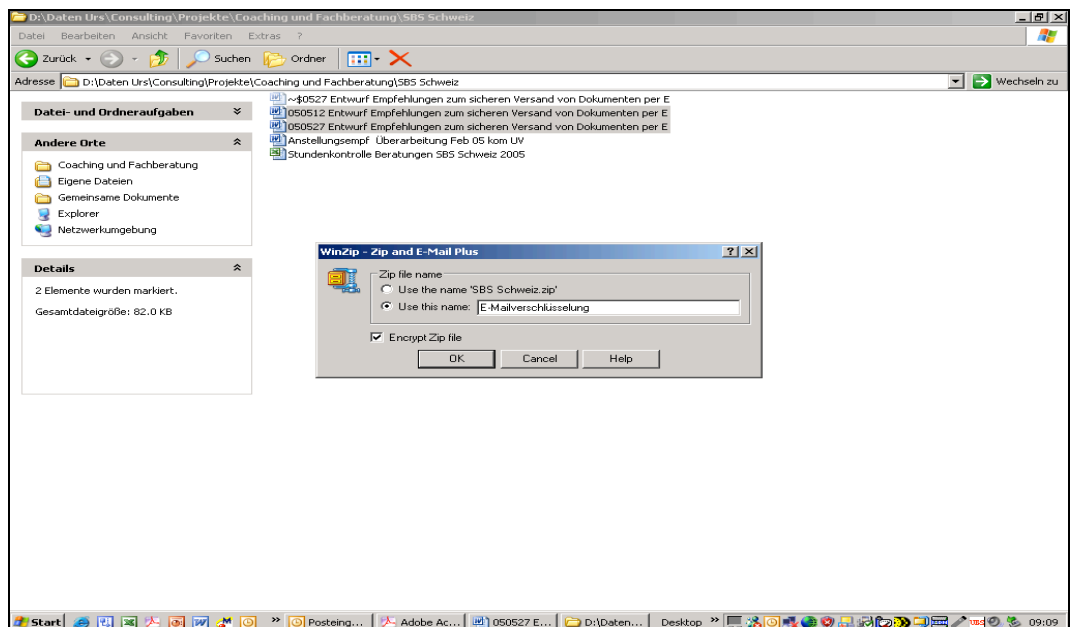
Verschlüsselung von anderen Dokumentarten oder mehreren Dokumenten gleichzeitig

Das WinZip¹-Programm bietet die Möglichkeit, verschiedene Dateiformate sowie mehrere Dokumente gleichzeitig sicher zu verschlüsseln. Sie gehen bei der Gratisversion des WinZip nach folgenden Schritten vor:

1. Explorer oder Dateiordner: *Datei (oder Dateien) markieren* > rechter Mausklick > WinZip > Zip und E Mail Plus.... >

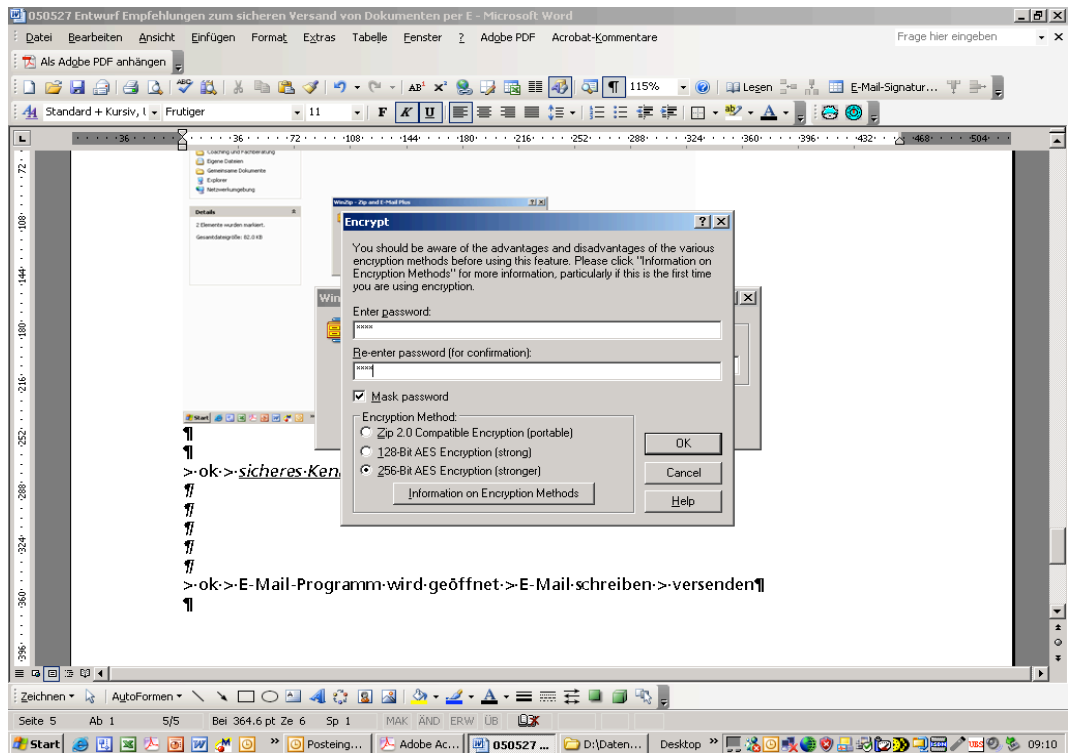


2. > Zip file name: *neutralen Dokumentnamen eingeben* > Encrypt Zip file: *Kästchen aktivieren* > ok >



¹ Eine Gratisversion kann unter <http://www.winzip.de/downautowz.htm> heruntergeladen werden.

> *sicheres Kennwort eingeben (2x)* > 256-Bit Verschlüsselung: *anwählen* > ok >



> E-Mail-Programm: *wird geöffnet* > *E-Mail schreiben* > *versenden*.

Die vorliegenden Empfehlungen wurden vom Vorstand Schweiz von AvenirSocial am 3. September 2005 verabschiedet.