

An die

Senatorin für Kinder und Bildung

-Personalstelle-

**über die Schulleiterin / den Schulleiter
der Schule**

Erklärung zum Einsatz privater Datenverarbeitungsgeräte nach § 3 Abs. 2 Bremisches Schuldatenschutzgesetz (BremSchulDSG)

Zur Erfüllung meiner dienstlichen Aufgaben beabsichtige ich, private Datenverarbeitungsgeräte zur Verarbeitung personenbezogener Daten von Schülerinnen und Schülern zu nutzen. Die Datenverarbeitung dient unmittelbar der Aufgabenerfüllung in meinem dienstlichen Verantwortungsbereich.

Ich verpflichte mich deshalb nach § 3 Abs. 2 BremSchulDSG zur Beachtung der datenschutzrechtlichen Vorschriften und sichere zu,

- bei der Verarbeitung der personenbezogenen Daten von Schülerinnen, Schülern und von Erziehungsberechtigten die Datenschutzbestimmungen des Schuldatenschutzgesetzes und des Bremischen Datenschutzgesetzes zu beachten,
- der Landesbeauftragten für den Datenschutz und Informationsfreiheit und dem Datenschutzbeauftragten bei der Senatorin für Kinder und Bildung zur Überwachung der Einhaltung der einschlägigen Bestimmungen meine privaten DV-Geräte vorzulegen,
- die personenbezogenen Daten nur persönlich zu verarbeiten und sie keinem Dritten zugänglich machen und somit auch keine internetbasierten Datenablagen/Cloud-Speicher, wie z.B. DropBox zu verwenden, sowie
- gespeicherte personenbezogene Daten spätestens nach dem Ende des jeweils nächsten Schuljahres zu löschen.

Ich habe folgende Maßnahmen zur Sicherung gegen den Zugriff Unbefugter ergriffen:

- Die gespeicherten Daten sind verschlüsselt und durch Passwort geschützt.¹
- ☐ Das Datenverarbeitungsgerät wird **ausschließlich von mir benutzt**, der Zugang ist durch ein sicheres Passwort geschützt. Ich versichere adäquate Schutzmaßnahmen gegen Viren und Manipulation des Endgerätes zu ergreifen. Ich werde hierfür eine Antivirensoftware installieren und diese regelmäßig aktualisieren. Des Weiteren werde ich zeitnah alle wichtigen Sicherheitsupdates (Patches) meines Systems installieren.²

Die Daten sind in einem verschlüsselten Bereich abgelegt.

oder

- ☐ Es ist ein **eigenes Benutzerkonto** angelegt, der Zugang ist durch ein sicheres Passwort geschützt. Ich versichere adäquate Schutzmaßnahmen gegen Viren und Manipulation des Endgerätes zu ergreifen. Ich werde hierfür eine Antivirensoftware installieren und diese regelmäßig aktualisieren. Des Weiteren werde ich zeitnah alle wichtigen Sicherheitsupdates (Patches) meines Systems installieren.²

Die Daten sind in einem eigenen verschlüsselten Bereich abgelegt, der nur mit meinem persönlichen Benutzerkonto eingesehen werden kann.

Mir ist bekannt, dass ich nur die in der Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden in der jeweils gültigen Fassung aufgeführten personenbezogenen Daten verarbeiten darf.

- Vor der Weitergabe der verwendeten Datenträger (z. B. beim Verkauf des alten Geräts, Weitergabe oder Entsorgung des Datenträgers) werde ich die verschlüsselten Daten löschen und den Schlüssel vernichten.
- Die elektronische Übermittlung von Schülerdaten erfolgt ausschließlich in verschlüsselter Form.
- Ich nehme zur Kenntnis, dass ein Verstoß gegen diese Verpflichtung entsprechende disziplinarrechtliche Maßnahmen zur Folge haben kann.

Datum: _____

.....
Unterschrift

Schule

1. Kenntnis genommen
2. Zur Personalakte

Bremen,

.....
Stempel und Unterschrift der Schulleiterin/des Schulleiters

¹Eine Handreichung hierzu findet sich unter www.subiti.de/info/verschluesselung.pdf

²Individuelle Empfehlungen hierzu erteilt das Referat 15 auf Anfrage.

Die Senatorin für Kinder und Bildung

Merkblatt über die Pflichten nach dem Bremischen Datenschutzgesetz (Brem DSG) Belehrung über das Datengeheimnis

Bei der Verarbeitung von personenbezogenen Daten haben die damit beschäftigten Personen die Bestimmungen des Gesetzes zum Schutze vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bremisches Datenschutzgesetz - BremDSG) vom 14. Oktober 1987 (Brem.GBl. Seite 263) zu beachten. Beim Einsatz in Schulen haben sie darüber hinaus das Gesetz zum Datenschutz im Schulwesen BremSchulDSG) vom 27. Februar 2007 (Brem.GBl. S. 181) zu beachten.

Nach § 5 BremDSG ist es diesen Personen untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung Ihrer Tätigkeit.

In den Fällen, in denen die Personen für die Verarbeitung von personenbezogenen Daten private mobile Datenträger für den Transport und/oder Datenverarbeitungsgeräte verwenden wollen (z.B. Laptop, Tablets, Smartphones, Speichermedien etc.), haben sie vor deren Verwendung eine schriftliche Erklärung zum Einsatz privater Datenverarbeitungsgeräte nach § 3 Abs. 2 Bremisches Schuldatenschutzgesetz (BremSchulDSG) abzugeben.

Verstöße gegen das Datengeheimnis können nach § 37 BremDSG mit einer Freiheits- oder Geldstrafe oder nach § 38 BremDSG mit einer Geldbuße geahndet werden; disziplinar- oder arbeitsrechtliche Maßnahmen werden dadurch nicht ausgeschlossen. Eine Verletzung des Datengeheimnisses wird in den meisten Fällen gleichzeitig eine Verletzung der Amtsverschwiegenheit bzw. einen Verstoß gegen die arbeitsvertragliche Schweigepflicht darstellen, auch kann in ihr zugleich eine Verletzung spezieller Geheimhaltungspflichten liegen.

Handreichung zur Datenverschlüsselung mit 7-ZIP

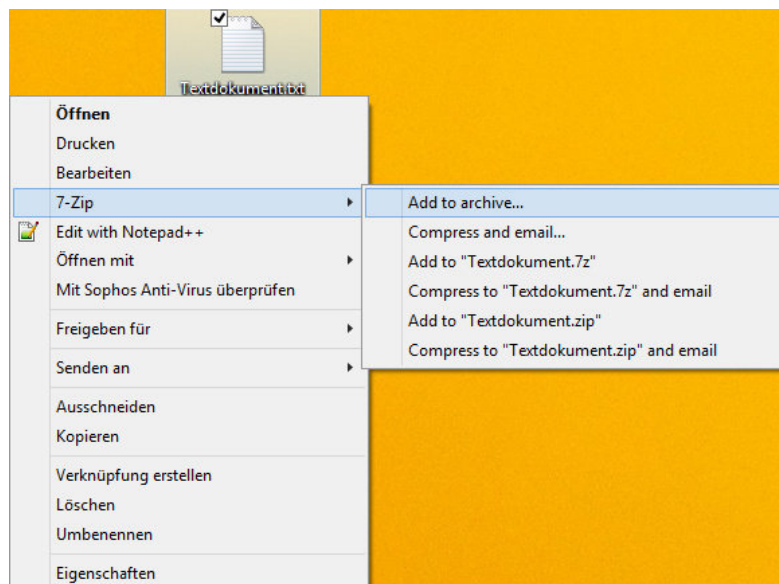
Daten werden verschlüsselt, um sie davor zu schützen, von Unberechtigten mitgelesen oder ausspioniert zu werden. Auf gemeinsam genutzten Computern können durch Verschlüsselung sensible Daten für die Mitbenutzer sowie Personen, die sich unberechtigt Zugang zu dem Gerät verschaffen, unlesbar gemacht werden. Informationen auf mobilen Endgeräten wie Notebooks, und USB-Speichermedien geraten nicht in falsche Hände, wenn das Gerät verloren oder gestohlen wird und die darauf gespeicherten Daten verschlüsselt sind. Gleiches gilt für die elektronische Übertragung von Daten, z.B. beim E-Mail-Versand.

Neben der Nutzung spezieller Verschlüsselungssoftware wie z.B. *GNU Privacy Guard for Windows (Gpg4Win)* kommt hierfür auch die Nutzung von Datenkompressionsprogrammen (Packern) in Frage, die neben der Komprimierung auch die Verschlüsselung von Daten ermöglichen.

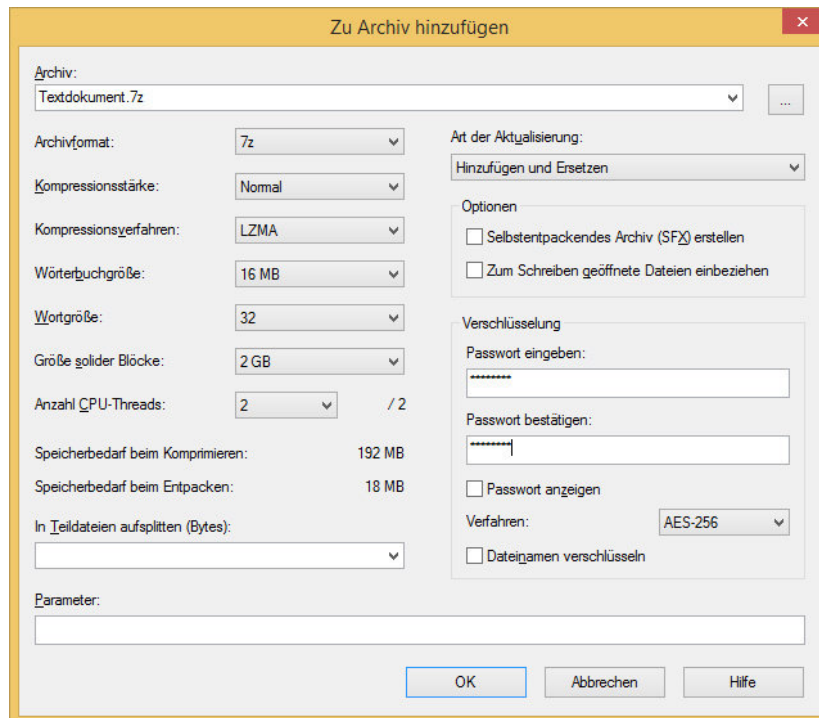
Im Folgenden wird diese Möglichkeit am Beispiel von 7-Zip, einem bereits auf allen Rechnern im Bildungsnetz installierten Programm erklärt, das kostenlos unter <http://7-zip.org> erhältlich ist.

Dateien Packen

Um eine Datei oder ein Verzeichnis zu packen und dabei zu verschlüsseln klicken Sie mit der rechten Maustaste auf die zu verschlüsselnde Datei. Nun öffnet sich ein Kontextmenü. In dem Kontextmenü wählen Sie unter „7-Zip“ den Punkt „Add to archive“ mittels eines Linksklicks aus.

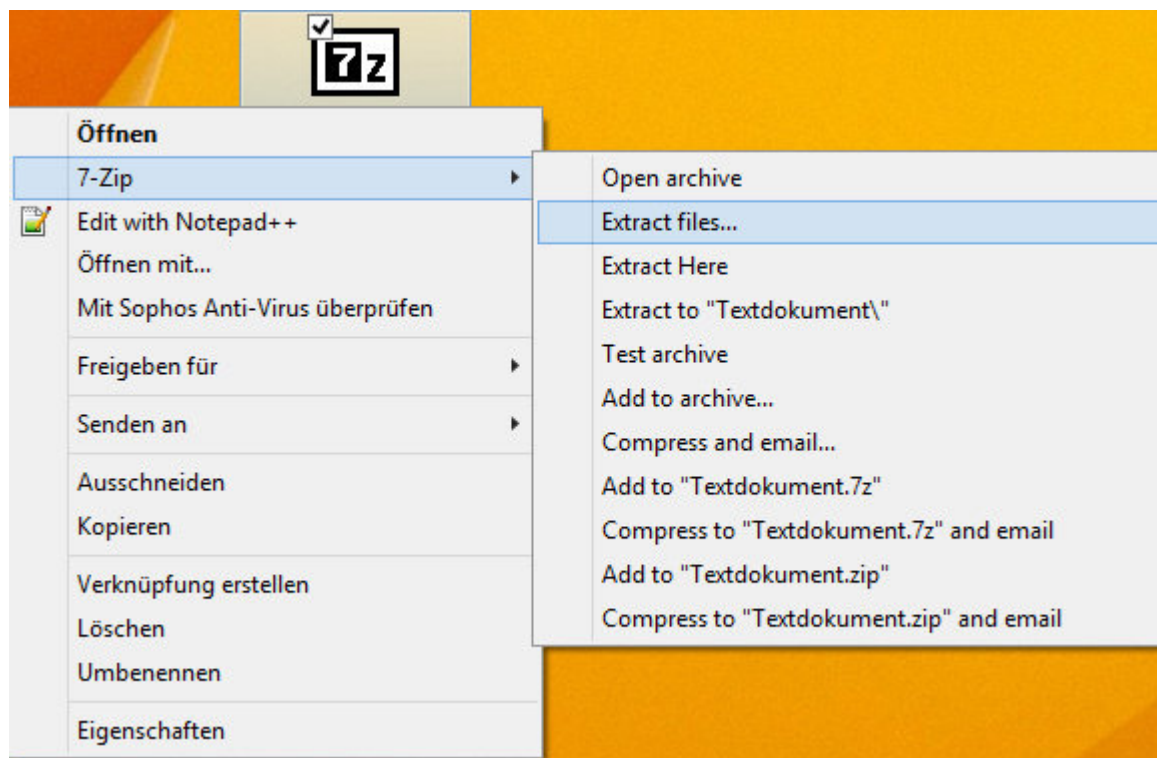


Es öffnet sich nun ein neues Fenster. Dort gibt es im unteren rechten Bereich die Möglichkeit ein Passwort für die Verschlüsselung der Datei einzugeben. Nachdem das Passwort eingegeben wurde, wird mit einem Linksklick auf den Button „OK“ die .zip Datei erzeugt.

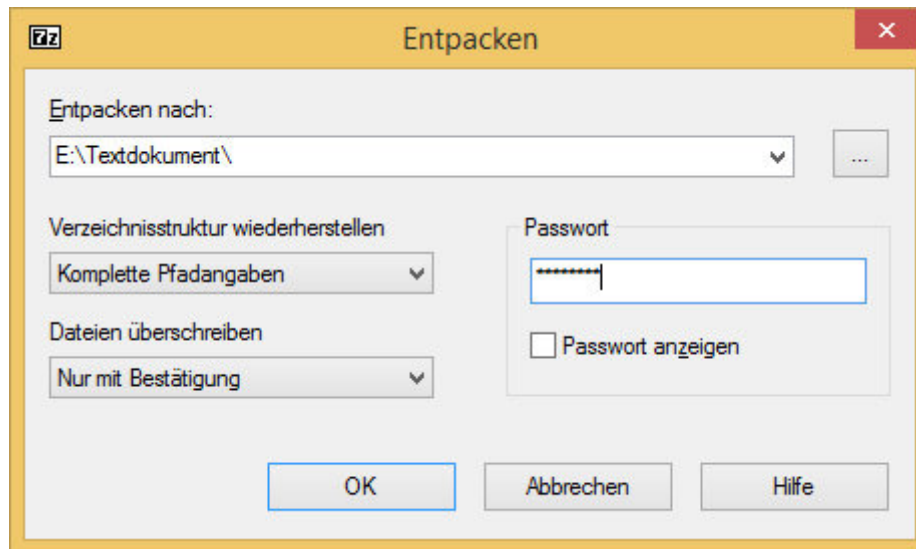


Dateien Entpacken

Zum entpacken einer .zip Datei klicken Sie mit der rechten Maustaste auf die zu entpackende Datei. In dem nun geöffneten Kontextmenü wird der unter „7-Zip“ zu findende Eintrag „Extract files“ mittels eines Linksklicks ausgewählt.



Nun öffnet sich ein neues Fenster welches zur Eingabe des zur Verschlüsselung genutzten Passwortes auffordert. Nach der Eingabe des Passwortes und des Bestätigen mittels „OK“ ist die Datei Entpackt und entschlüsselt am unter „Entpacken nach“ eingebenden Pfad zu finden.



Dieses Verfahren kann sowohl zur sicheren Ablage von Dateien auf Datenträgern, als auch zur sicheren Übertragung z.B. per E-Mail (verschlüsselter Anhang) genutzt werden. Hierbei empfiehlt sich dann die Übermittlung des Passworts an den Empfänger der Nachricht auf eine andere Weise, z.B. per Telefon.