Merkblätter zur Datensicherheit

Datenschutzbeauftragter des Kantons Zug

Kanton Zug

Die vier Merkblätter

Datenschutzbeauftragter des Kantons Zug
Regierungsgebäude
Postfach 156
6301 Zug

Telefon 041 728 31 87

www.datenschutz-zug.ch

Einleitung

Warum diese Broschüre?
Die Medien berichten fast täglich über Hackerangriffe, Softwarefehler oder Datendiebstahl. Dies zeigt klar, dass die Nutzung der heutigen Informations- und Kommunikationstechnologien mit Risiken und Gefahren verbunden ist.
Die Verwaltung bearbeitet viele sehr sensible Daten über Zugerinnen und Zuger. Diese haben einen Anspruch darauf, dass Sie mit ihren Daten in jeder Hinsicht sicher umgehen. Die vorliegende Broschüre enthält vier Merkblätter, die Sie dabei unterstützen. Es wird aufgezeigt, was Sie konkret tun müssen, damit Ihre Datenbearbeitungen sicher sind und Schäden vermieden werden.

Neben dem Merkblatt zu den grundlegenden Hinweisen werden die folgenden Themen speziell behandelt: der sichere Umgang mit Passwörtern, E-Mail und mobilen Geräten.

eLearning
Auf unserer Website steht Ihnen ergänzend auch eine Schulung über den Inhalt der vorliegenden Merkblätter zur Verfügung. Für das Durcharbeiten benötigen Sie etwa eine Stunde. Dieses eLearning endet mit einem kurzen Abschlusstest. Bei Bestehen erhalten Sie eine schriftliche Bestätigung.

Für wen gelten die Hinweise?
Verwaltung des Kantons
Diese Hinweise gelten umfassend und verpflichtend für alle Mitarbeitenden der kantonalen Verwaltung.

Gemeinden und Institutionen mit Leistungsvereinbarung
Da einzelne Hinweise von technischen Gegebenheiten abhängig sind, gelten die Merkblätter für die Mitarbeitenden von Gemeinden (Einwohner-, Bürger-, Kirch- und Korporationsgemeinden) und von Institutionen, denen in Leistungsvereinbarungen öffentliche Aufgaben übertragen sind, sinngemäss.

Unternehmen und Privatpersonen
Grundsätzlich sind diese Merkblätter auch für Unternehmen und Privatpersonen nützlich.

Ihre Verantwortung
Bearbeiten Sie Daten, so sind Sie in Ihrem Bereich für die Einhaltung von Datenschutz und Datensicherheit verantwortlich. Entsteht ein Schaden, weil Sie die Sicherheitsvorgaben nicht eingehalten haben, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden. Aber seien Sie beruhigt: Die vorliegenden Merkblätter enthalten alle Informationen, die Sie für sicheres Arbeiten benötigen. Sie müssen sie nur beherzigen.

Rechtsgrundlagen
Gestützt auf das Datenschutzgesetz des Kantons Zug[1)] hat der Regierungsrat die Datensicherheitsverordnung[2)] erlassen. Diese sieht vor, dass der Datenschutzbeauftragte Merkblätter für die Instruktion aller Mitarbeitenden zur Verfügung stellt.

Haben Sie Fragen? Die Datenschutzstelle steht Ihnen gerne zur Verfügung.

[1)] § 7 DSG, BGS 157.1.
[2)] DSV, BGS 157.12.

Merkblatt «Der sichere Umgang mit Daten»

Kurz und bündig
Hier finden Sie die grundlegenden Hinweise zum sicheren Umgang mit Daten in der öffentlichen Verwaltung.

Schutz gegen Zugriff Unberechtigter
So schützen Sie Ihre Daten am Arbeitsplatz:

Bei Abwesenheit vom Arbeitsplatz

- Aktivieren Sie die Bildschirmsperre mit Passwortschutz auch bei nur kurzem Verlassen Ihres Arbeitsplatzes, wird doch ein unbenutzter PC-Arbeitsplatz *automatisch* erst nach 20 Minuten gesperrt. So sperren Sie Ihren PC: Drücken Sie entweder gleichzeitig die drei Tasten «Ctrl», «Alt» und «Del» und bestätigen Sie mit «Enter/Eingabe» oder noch einfacher: Drücken Sie gleichzeitig die beiden Tasten «Windows-Taste» und «L».
- Ist bei Ihnen eine Smartcard im Einsatz, müssen Sie diese bei Abwesenheit vom Arbeitsplatz entfernen und mitnehmen.
- Bewahren Sie Unterlagen (Papiere, Dossiers, elektronische Datenträger), die besonders schützenswerte Personendaten enthalten, abgeschlossen auf.

Bei Arbeitsschluss

- Schalten Sie Ihren PC nie via Schalter an einer Steckerleiste ab, sondern melden Sie Ihren Computer mittels «Herunterfahren» vom Netzwerk ab und schalten Sie den Bildschirm aus. Dadurch wird der Speicher aufgeräumt und Ihr PC arbeitet nach dem erneuten Start zuverlässig.
- Sämtliche Unterlagen oder Datenträger, die Personendaten enthalten, müssen Sie verschlossen aufbewahren.

Weitergabe, Speichern und Löschen von Daten
Vorweg: Es ist aus Sicherheitsgründen verboten, Personendaten oder vertrauliche Sachdaten in Cloud-Diensten (wie etwa Dropbox/Amazon, iCloud/Apple, SkyDrive/Microsoft, Google Drive/Google) zu speichern oder auf diese Weise zu übermitteln. Cloud-Dienste speichern Daten unter Umständen in beliebigen Ländern ab, die Daten können durch Dritte gelesen, verändert, gelöscht oder auch durch ausländische Behörden beschlagnahmt werden.

Weitergabe von Daten

Verwenden Sie zur Weitergabe von Daten grundsätzlich neue Datenträger (USB-Sticks, CD-ROM, DVD). Beim AIO erhalten Sie USB-Sticks, welche die Daten verschlüsselt abspeichern.

Speichern von Daten

Auf dem C-Laufwerk dürfen Sie keinerlei Daten abspeichern. Dieses Laufwerk steht ausschliesslich für Systemdateien und Programme zur Verfügung. Speichern Sie Daten an dem Ort im Netzwerk ab, der Ihnen durch Ihren Arbeitgeber bzw. das AIO zur Verfügung gestellt wird. In aller Regel somit auf dem O-Laufwerk bzw. in der Fachanwendung. Damit ist sichergestellt, dass nur Berechtigte Zugang zu Ihren Daten haben und dass die Daten durch das AIO regelmässig gesichert werden.

Löschen von Daten

Wenn Sie Ihren PC oder ein anderes Gerät (Laptop/Notebook, mobiles Telefon, externe USB-Harddisk etc.) ihrem Arbeitgeber bzw. dem AIO zurückgeben, sorgt der Servicedesk dafür, dass die Daten unwiderruflich gelöscht werden.

Entsorgen von elektronischen Datenträgern

Stellen Sie Datenträger (CD-ROM, DVD, Datenbänder, USB-Sticks, Festplatten etc.) dem AIO-Servicedesk zur sicheren Löschung bzw. fachgerechten Entsorgung zu.

Entsorgen von Papierakten

Unterlagen in Papierform, die Sie nicht mehr benötigen und die Personendaten enthalten, müssen Sie im Aktenvernichter schreddern.
Auf Papierakten, die Sie zur Entsorgung in die graue Kunststoffbox geben, haben – auf dem Weg zum zentralen Aktenvernichter – verschiedene Personen Zugriff. Geben Sie daher nur Papierunterlagen, die keine Personendaten enthalten, in die graue Kunststoffbox.

Schutz vor Verlust

Mobile Datenträger

Daten auf mobilen Datenträgern (USB-Stick, CD-ROM etc., aber auch Dokumente in Papierform) sind erhöhten Gefahren und Risiken ausgesetzt, da sie leicht verloren gehen oder entwendet werden können. Entsprechend müssen Sie die erforderlichen Massnahmen ergreifen:

- Sichern Sie den Datenträger (bzw. Ordner/Dateien) mit einem starken Passwort.
- Schliessen Sie mobile Geräte bei Nichtgebrauch an einem sicheren Ort ein (falls im Auto: nicht sichtbar).
- Wenn Sie mobile Datenträger an Dritte zustellen müssen, wählen Sie die angemessene Zustellungsart (persönliche Übergabe, Bote, eingeschriebene Briefpost etc.).

Viren und Schadsoftware (Malware)

Viren, Würmer, trojanische Pferde oder dergleichen sind kleine Programme, die Computersysteme befallen und Daten oder Programme zerstören, verändern oder andere gravierende Schäden anrichten können. Sie werden insbesondere über E-Mails und deren Anhänge, über Dateien (z.B. Spiele, Bildschirmschoner, Freeware etc.), die vom Internet heruntergeladen werden, oder durch Speichermedien wie USB-Sticks und CD-ROM/DVD eingeschleppt. Bereits der Besuch von entsprechend präparierten Websites kann Schadprogramme auf Ihr Gerät laden.

Sie schützen sich vor Viren, indem Sie

- nur E-Mails öffnen, die Ihnen absolut vertrauenswürdig erscheinen. Anhänge zu E-Mails sind grundsätzlich nur dann zu öffnen, wenn Sie den Anhang erwartet haben (alles Nähere dazu im Merkblatt «E-Mail»);
- USB-Sticks und CD-ROM/DVD vor dem Gebrauch immer mit dem Virenschutzprogramm prüfen;
- nur vertrauenswürdige Websites besuchen (s. dazu die Hinweise im Abschnitt «Internet» auf Seite 4);
- nur vom AIO (bzw. Ihrem IT-Fachanwendungsdienstleister) zur Verfügung gestellte, rechtmässig lizenzierte Software verwenden (die Installation privater Software ist verboten);
- bei der Nutzung von privaten Geräten ein Virenschutzprogramm installieren, das Sie laufend aktualisieren.

Vorgehen bei Auftreten von Viren

- Nehmen Sie keine eigenen Reparaturversuche vor, sondern informieren Sie umgehend den AIO-Servicedesk per Telefon.
- Fahren Sie bei Nichterreichbarkeit des AIO-Servicedesks das Gerät herunter.

Und vergessen Sie nicht

- Auch Wasser, Feuer und Diebstahl sind Gefahrenquellen. Schützen Sie deshalb Geräte, Datenträger und Papierdokumente entsprechend.
- Von Ihnen erkannte Mängel oder Sicherheitslücken müssen behoben werden. Melden Sie diese dem AIO-Servicedesk und/oder Ihrem Vorgesetzten.

Kommunikation über Netze

Hinweise zu externen Netzen

Bei der Kommunikation über externe Netze müssen Sie Folgendes beachten:

- Unverschlüsselte Informationen sind bei der Benutzung eines öffentlichen Netzes (z.B. Hotspot eines Service-Providers) einseh- bzw. abhörbar. Personendaten dürfen Sie über solche Datenkanäle nicht unverschlüsselt weitergeben.
- Aus Sicherheitsgründen dürfen Sie mobile Geräte nicht gleichzeitig an das interne Netzwerk des Kantons und an ein externes Netz (z.B. WLAN Kantonsschule Zug) anschliessen. Damit stellen Sie sicher, dass unkontrollierbare und ungesicherte Zugriffe auf die kantonale Informatikinfrastruktur ausgeschlossen sind.
- Die Synchronisation von Outlook mit externen webbasierten Kalendern (z.B. Google oder Office 365) ist nicht zulässig.

Internet

Das Internet ist ein offenes Netzwerk. Alle darin publizierten Informationen sind für jedermann weltweit zugänglich und kopierbar. Zunehmend ergeben sich Gefahren durch Schadprogramme, die in Websites versteckt eingebaut sind. Besuchen Sie daher nur vertrauenswürdige Websites und seien Sie zurückhaltend und vorsichtig, was Sie anklicken.

Eine Website ist möglicherweise *nicht* vertrauenswürdig, wenn eine der folgenden Bedingungen zutrifft:

- Eine unbekannte Person hat Ihnen einen Link auf die Website per E-Mail geschickt.
- Erhalten Sie einen «gekürzten Link» (wie etwa http://bit.ly/13VO6fz), dürfen Sie ihn nicht anklicken, da Sie nicht sehen, wohin der Link führt (unter www.longurl.org können Sie jedoch den gekürzten Link wieder in seiner vollständigen Länge sehen).
- Die Website enthält fragwürdige oder illegale Inhalte.
- Auf der Website werden Angebote gemacht, die zu gut sind, um wahr zu sein.
- Sie werden durch eine Lockvogeltaktik zu der Site gelockt, wobei die tatsächlich angebotene Information nicht dem entspricht, was Sie eigentlich erwartet haben.
- Sie werden aufgefordert, zu Ihrer Identifizierung Ihre Kreditkartennummer anzugeben oder persönliche Daten preiszugeben, die nicht notwendig scheinen.

Intranet bzw. internes Netzwerk

Das Intranet ist ein Netzwerk für einen bestimmten Personenkreis. Die Übertragung *innerhalb des kantonalen Netzwerks* gilt grundsätzlich als sicher. Sie dürfen somit über das *kantonale Netzwerk* Personendaten (auch besonders schützenswerte) unverschlüsselt versenden.

Datenspuren

In Dateien

Bedenken Sie, dass Dokumente, die Sie mit Office-Programmen (Word, Excel, PowerPoint etc.) erstellen, automatisch eine ganze Reihe versteckter Informationen enthalten: Verfassername, Erstelldatum, alles Nähere zu sämtlichen Änderungen, Angaben zu weiteren Bearbeitenden etc. Wenn Sie ein solches Dokument weitergeben, müssen Sie all diese Informationen zur Datei wie folgt entfernen: Im Reiter «Datei» unter «Informationen» «Auf Probleme überprüfen» anklicken und dort «Dokument prüfen». Die versteckten Informationen müssen Sie anschliessend entsprechend entfernen.

Noch besser ist es, wenn Sie das fragliche Dokument als PDF abspeichern und dem Adressaten dieses zustellen.

Beim Surfen

Auf dem eigenen Gerät:

- Cookies: kurze Textfiles, die Ihnen Dritte ohne Ihr Zutun zustellen und die auf Ihrem PC gespeichert werden. Sie enthalten meist Angaben zu Ihrer Internet-Nutzung.
- Im Zwischenspeicher, dem sogenannten «Cache», werden auf Ihrem Gerät die durch Sie besuchten Websites und weitere Informationen gespeichert.
- History: speichert in einer Liste alle Websites, die Sie besucht haben.
- Funktion «Auto-Vervollständigen»: speichert frühere Eingaben zu besuchten Websites und schlägt diese vor, wenn die gleichen Angaben neu eingegeben werden.

Auf den kantonalen und anderen Servern:

- Protokollierungen: enthalten Informationen über alle Aktivitäten, die Sie auf Ihrem Gerät ausgeführt haben. Diese sind auf den beteiligten Servern gespeichert und enthalten unter anderem etwa die (IP-)Adresse Ihres Geräts, den Zeitpunkt und die besuchten Sites etc. Sie haben keine Möglichkeit, diese Angaben zu löschen.
- Datenspuren zeigen auch auf, wenn Sie Ihre Geräte für private Zwecke nutzen. Surfen zu privaten Zwecken ist Mitarbeitenden der kantonalen Verwaltung gestattet, sofern es sich um eine nur geringfügige Nutzung handelt (analog zur Nutzung des geschäftlichen Telefons).

Weitergabe von Informationen über Sie an Dritte

Die meisten Betreiber von Websites geben zu Marketingzwecken umgehend Daten über Sie an Drittfirmen weiter. Beispielsweise welche Websites Sie unmittelbar vorher besucht haben sowie viele Angaben zu Ihrem Computer und dessen System bzw. Konfiguration.

Löschen Sie Cookies, Cache, Verlauf und Auto-Vervollständigen des Browsers regelmässig auf Ihrem Gerät. Im Internet-Explorer[1] gehen Sie wie folgt vor: Reiter «Extras»/Zahnradsymbol «Internetoptionen» anklicken, Reiter «Allgemein» wählen, unter «Browserverlauf» auf «Löschen» klicken, alle Optionen mit Häkchen versehen und auf «Löschen» klicken.

Rechtsgrundlagen

Die wichtigsten Rechtsgrundlagen im Bereich Datenschutz/Datensicherheit sind:

- Datenschutzgesetz des Kantons Zug (BGS 157.1)
- Datensicherheitsverordnung (BGS 157.12)
- Verordnung über die Benutzung von elektronischen Kommunikationsmitteln im Arbeitsverhältnis (E-Mail und Abruf von Webseiten) (BGS 154.28)
- Weisung des Regierungsrates zur Überprüfung der Datensicherheit (Stand vom 13. April 2010)
- Personalgesetz (BGS 154.21) und Personalverordnung (BGS 154.211)
- Strafgesetzbuch (SR 311.0)

Zusätzliche Hinweise finden Sie hier

Datenschutzbeauftragter des Kantons Zug

Neben vielen Informationen zum Zuger Datenschutz steht Ihnen auch unser Newsletter zur Verfügung – abonnieren Sie diesen und Sie sind in Sachen Datenschutz und Datensicherheit auf dem Laufenden:
www.datenschutz-zug.ch

Datenschutzbeauftragter des Kantons Zürich

Auf der Website des Zürcher Datenschutzbeauftragten finden Sie ein nützliches Lernprogramm zum Datenschutz, umfassende Informationen zur Datensicherheit, ein Tool zur Grobanalyse getroffener Massnahmen für Datenschutz und Informatiksicherheit («Review-Tool») sowie ein Programm zur Überprüfung der Qualität von Passwörtern («Passwort-Check»):
www.datenschutz.ch

Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

www.edoeb.admin.ch

[1] Falls Sie den Firefox im Einsatz haben: Wählen Sie den Menüpunkt «Extras» (oder bei neueren Versionen «Chronik») und wählen Sie «Neueste Chronik löschen», wählen Sie «Alles löschen» und klicken Sie auf «Jetzt löschen».

Merkblatt «Passwort»

Passwort: Schutz vor dem Zugriff Unberechtigter

Passwörter müssen sicherstellen, dass nur Berechtigte Zugriff auf ein System oder auf bestimmte Anwendungen und deren Daten haben. Damit wird verhindert, dass Daten von Unberechtigten eingesehen, kopiert, verändert oder gelöscht werden können.

Das Passwort ist der Schlüssel zu einer Tür. Es ist daher das zentrale Objekt der Begierde von Angreifern. Sobald ein Passwort an eine unberechtigte Person gelangt ist, hat es seine Schutzwirkung verloren. Die Daten sind dann gefährdet, der Datenschutz ist verletzt.

Für den Schutz Ihrer Passwörter sind nur Sie alleine verantwortlich. Entsteht ein Schaden durch nicht korrekten Umgang mit Ihren Passwörtern, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden.

Ein gutes – oder: «starkes» – Passwort

Ein PC-Passwort muss mindestens 8 Zeichen haben und es muss zusätzlich 3 der 4 folgenden Bedingungen erfüllen:
- min. einen Grossbuchstaben
- min. einen Kleinbuchstaben
- min. eine Zahl
- min. ein Sonderzeichen (! ? + - _ % &)

Das Passwort darf nicht einfach zu erratende Bestandteile wie Name/Vorname, E-Mail-Adresse, Telefonnummer, Geburtsdaten oder Auto-Kennzeichen enthalten. Nicht erlaubt sind Passwörter, die mehr als 3 aufeinanderfolgende Gross- oder Kleinbuchstaben bzw. Zahlen beinhalten (unzulässig somit: ABCD, bcde oder 4567).
Erfinden Sie ein Passwort, das Sie sich gut merken können, andere aber nicht erraten können: Sonn**EN00schein, fRan?ziska57 oder erfinden Sie einen Satz, den Sie nicht so schnell vergessen und setzen Sie den Anfang der einzelnen Wörter zu einem Passwort zusammen:
Der Satz «Wir fahren 2 Mal im Jahr nach Zermatt in die Ferien!» ergibt das starke Passwort «Wf2MiJnZidF!».

Ergänzende Hinweise bezüglich Passwörter zu Fachanwendungen

Für Passwörter von gewissen Fachanwendungen gelten die folgenden Einschränkungen:
- Keine Umlaute wie ääüéàè verwenden (weil diese bei Webanwendungen teilweise nicht akzeptiert werden oder auf der internationalen Tastatur nicht eingegeben werden können).
- Leerzeichen sind nicht erlaubt (können bei Webanwendungen oder in Fachanwendungen zu Login-Fehlern führen).
- Gewisse Fachanwendungen erlauben ein maximal 8 Zeichen langes Passwort.

Bei Fragen dazu können Sie sich an die Verantwortlichen der entsprechenden Fachanwendung wenden.

Umgang mit dem Passwort
- Halten Sie Ihr Passwort unter allen Umständen geheim. Lassen Sie sich bei der Eingabe eines Passwortes nicht beobachten.
- Ändern Sie das Passwort nach spätestens 90 Tagen, falls Sie durch das System nicht früher aufgefordert werden, Ihr Passwort zu ändern.
- Bei Verdacht auf Missbrauch müssen Sie Ihr Passwort sofort ändern und den Vorfall dem AIO-Servicedesk und Ihrer vorgesetzten Stelle melden.
- Verwenden Sie für verschiedene Anwendungen verschiedene Passwörter.
- Ein Passwort, das Sie für Webanwendungen oder für Fachanwendungen nutzen, dürfen Sie nicht auch für das Login Ihres PC verwenden.
- Passwörter dürfen Sie nicht an andere Mitarbeitende oder Dritte weitergeben, auch nicht an Ihre Stellvertretung. Mitarbeitende des AIO oder externe IT-Dienstleister werden Sie übrigens nie nach Ihrem Passwort fragen.
- Verwenden Sie privat andere Passwörter als am Arbeitsplatz.

Wichtige zusätzliche Informationen zum Passwort

Hier können Sie überprüfen, wie gut Ihr Passwort ist («Passwort-Check»); Sie finden zudem weitere Hinweise zum Passwort:
www.datenschutz.ch

Merkblatt «E-Mail»

Die Kommunikation per E-Mail ist kaum mehr aus unserer Arbeitswelt wegzudenken. Sie ist rasch, einfach und billig. Leider ist sie aber nicht in jedem Fall sicher.

Entsteht ein Schaden, weil Sie die Sicherheitsvorgaben bezüglich E-Mail nicht eingehalten haben, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden. Folgendes müssen Sie deshalb beachten:

Eile mit Weile!
E-Mail ist ein sehr «schnelles Medium» – ein Klick und Ihre Nachricht ist unwiderruflich weg! Immer wieder gelangen vertrauliche Mitteilungen in der Hast an einen ganz falschen Adressaten. Eine häufige Fehlerquelle liegt darin, dass Outlook Ihnen beim Eintippen der Adresse gleich Vorschläge macht. Überprüfen Sie deshalb stets sorgfältig – auch und gerade in hektischen Situationen –, ob Sie den richtigen Empfänger eingegeben (falls es mehrere sind, ob tatsächlich alle Informationen an alle diese Personen zu senden sind) und ob Sie die richtigen Dokumente beigelegt haben.

Der Adressat ist nicht immer der (einzige) Empfänger
Wenn Sie vertrauliche Daten per E-Mail übermitteln, müssen Sie stets bedenken, dass allenfalls das Sekretariat oder die Stellvertretung des Adressaten über eine Zugriffsberechtigung verfügt. Falls Drittpersonen keine Kenntnis der Daten erhalten dürfen, müssen Sie mit dem Adressaten Rücksprache nehmen oder einen anderen Kommunikationsweg wählen – etwa die «Persönliche/Vertrauliche» Briefpost.

Versand innerhalb des verwaltungseigenen Netzes
Das Versenden von E-Mails innerhalb des Netzwerks des Kantons gilt grundsätzlich als sicher. Ist der Empfänger ebenfalls am verwaltungseigenen Netz angeschlossen, dürfen Sie grundsätzlich auch besonders schützenswerte Personendaten unverschlüsselt übermitteln.

Endet die Adresse auf «@zg.ch», erfolgt die Zustellung intern, ohne dass das eigene Netz verlassen wird. Im folgenden Beispiel dürfen Sie Daten somit unverschlüsselt übermitteln:
peter.muster@zg.ch an max.beispiel@zg.ch

Der Versand zwischen kantonalen Stellen und solchen der Einwohnergemeinden ist nur dann sicher, wenn die E-Mail-Adresse auf «@*gemeindename*[1].ch» endet:
max.beispiel@zg.ch an peter.muster@huenenberg.ch

Nicht sicher ist der Versand hingegen etwa hier:
peter.muster@zg.ch an max.beispiel@schulen-huenenberg.ch (Grund: diese Adresse endet *nicht* auf «@*gemeindename*.ch»).

Versand via Internet
Unverschlüsselte E-Mail-Kommunikation via Internet – somit ausserhalb des verwaltungseigenen Netzes – gilt als weniger vertraulich als der Versand einer Postkarte. Auf dem Übertragungsweg sind E-Mails an vielen Orten für Dritte direkt einsehbar, werden kopiert und können verändert oder gelöscht werden. Deshalb dürfen Sie als Mitarbeitende der kantonalen Verwaltung keinerlei Personendaten *unverschlüsselt* per E-Mail über das Internet versenden.

Reine Sachinformationen – somit Informationen, die *keinerlei* Bezug zu einer Person haben – dürfen Sie unverschlüsselt per E-Mail verschicken. So etwa die Bekanntgabe von Öffnungszeiten oder der Hinweis auf Gesetzesbestimmungen.

Personendaten hingegen dürfen Sie über das Internet nur verschicken, wenn sie *korrekt verschlüsselt* sind. Ist die direkte Verschlüsselung von E-Mails und Anhängen in Ihrem E-Mail-System nicht möglich, können Sie Office-Dokumente, PDF oder WinZip-Ordner vor dem Versand mit einem Passwort verschlüsseln. Wichtig ist, dass Sie ein sicheres Passwort verwenden und dass Sie dieses dem Adressaten nicht per E-Mail, sondern via Telefon oder SMS mitteilen.

[1] Darunter fallen auch die Stadt Zug (@stadtzug.ch) und die Gemeinde Risch (@rischrotkreuz.ch).

So verschlüsseln Sie Dokumente

1. Einzelne oder mehrere beliebige Dokumente können Sie mit dem Programm WinZip wie folgt verschlüsseln:

Bei den Programmen finden Sie unter «Werkzeuge» das Programm WinZip. Öffnen Sie es, fügen Sie die zu verschlüsselnden Dokumente ein und sichern Sie den Ordner wie folgt:
Reiter «Extras» → «Archiv verschlüsseln». Bedenken Sie, dass der *Name* des WinZip-Ordners und die *Namen* der enthaltenen Dokumente für Dritte sichtbar sind (nicht aber der *Inhalt*). Der Dokumentenname darf daher nicht einen Hinweis auf den Inhalt des Dokuments geben (der Name des Dokuments darf somit nicht lauten «fristlose_Entlassung_Müller.doc», sondern etwa «HR_27NOV2013»).

2. Office-Dokumente (Word, Excel, PowerPoint)

Reiter «Datei» → «Informationen» → «Dokument schützen» → «Mit Kennwort verschlüsseln».

3. PDF

So speichern Sie ein Office-Dokument (Word, Excel, PowerPoint) als verschlüsseltes PDF ab:
Reiter «Datei» → «Speichern unter» → «Dateityp» als PDF auswählen → «Optionen» → «Dokument mit einem Kennwort verschlüsseln» ankreuzen.

Wenn Sie obige Sicherheitsmassnahmen einhalten, haben Sie grosse Gewähr, dass nur der berechtigte Adressat Kenntnis vom Inhalt erhält. Wenn es sich jedoch um ein Dokument mit vertraulichem Inhalt handelt, ist der Versand per Briefpost oder die persönliche Übergabe der elektronischen Zustellung vorzuziehen.

Ein ergänzender Hinweis, falls Sie die Anwendung «Web-Mail» des AIO nutzen:

Diese Anwendung verschlüsselt den Datenverkehr *zwischen dem Web-Mail Nutzenden und dem AIO*. Dadurch entspricht der Zugang auf das eigene E-Mail-Konto demjenigen an Ihrem Arbeitsplatz im Büro. Die vorstehenden Hinweise bezüglich des Versendens von E-Mails sind ebenfalls zu beachten.

Nachdem Sie sich beim Web-Mail abgemeldet haben, müssen Sie die temporär gespeicherten Dokumente und Informationen beim Internet-Explorer[1)] wie folgt löschen: unter «Extras»/Zahnradsymbol «Internetoptionen» anklicken, Reiter «Allgemein» wählen, unter «Browserverlauf» auf «Löschen» klicken, alle Optionen mit Häkchen versehen und auf «Löschen» klicken.

Erhalt von E-Mails

E-Mails können Schadprogramme enthalten und deshalb Risiken und Gefahren für Ihre IT-Umgebung, Ihren Computer oder Ihre Daten darstellen. Beachten Sie deshalb Folgendes:

- E-Mails von zweifelhafter Herkunft müssen Sie *ungeöffnet* löschen.
- *Ungeöffnet* löschen müssen Sie auch Beilagen und Bilder von zweifelhafter Herkunft.
- Bei verwaltungsexternen Anfragen per E-Mail haben Sie grundsätzlich *keinerlei* Gewissheit über die Identität des Absenders, da der Sender die Informationen über seine Identität problemlos beliebig selber definieren kann. Im Zweifelsfall müssen Sie beim angegebenen Absender telefonisch nachfragen.
- Selbst wenn Ihnen der verwaltungsexterne Absender bekannt ist, müssen Sie bezüglich Beilagen vorsichtig sein, da dessen System bzw. dessen Infrastruktur durch Schadprogramme infiziert sein kann.

Vorgehen bei Abwesenheit

- Sie müssen Absender von E-Mails mit einer automatischen Antwort über Ihre Abwesenheit informieren und angeben, an wen man sich während Ihrer Abwesenheit wenden kann.
- Das automatische Um- oder Weiterleiten sowohl an externe wie auch an interne E-Mail-Adressen ist nicht gestattet. Soll Ihr Outlook-Kalender oder Ihr Post-Eingang bei Abwesenheit durch Ihre Stellvertretung geführt werden, darf dies nur nach *vorgängiger* Absprache zwischen Ihnen und Ihrer Stellvertretung über die Outlook-Freigabefunktionen auf genau bezeichnete Ordner geschehen.

[1)] Falls Sie den Firefox im Einsatz haben: Wählen Sie den Menüpunkt «Extras» (oder bei neueren Versionen «Chronik») und wählen Sie «Neueste Chronik löschen», wählen Sie «Alles löschen» und klicken Sie auf «Jetzt löschen».

Merkblatt «Mobile Geräte»

Vorweg
Arbeiten Sie mit mobilen Geräten, sind Sie für den korrekten Umgang mit den Kommunikationsmitteln persönlich verantwortlich. Für Papierunterlagen ausserhalb des Büros gilt das Folgende übrigens sinngemäss. Entsteht ein Schaden durch nicht korrekten Umgang mit Ihren mobilen Geräten, können Sie allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden.

Mobile Geräte
Mobile Geräte sind Laptops/Notebooks, Mobiltelefone/Smartphones, iPads, USB-Sticks (und andere mobile Speichermedien) sowie alle anderen mobilen technischen Geräte, auf denen geschäftliche Informationen bzw. Personendaten verarbeitet oder abgespeichert werden.

Sicherheitsmassnahmen
Für mobile Geräte müssen Sie grundsätzlich dieselben Sicherheitsbestimmungen einhalten wie für feste Arbeitsstationen. Die Gefahr von Verlust oder Diebstahl ist bei tragbaren Geräten jedoch besonders gross, da diese leicht verloren gehen oder entwendet werden können. Deshalb müssen Sie zusätzlich die folgenden Sicherheitsmassnahmen ergreifen:

- Absolut zentral ist, dass Sie Ihr Gerät durch ein starkes Passwort schützen (s. dazu das separate Merkblatt «Passwort»).
- Sie müssen den Passwortschutz so einstellen, dass er bei Notebooks nach zehn Minuten und bei Smartphones und ähnlichen mobilen Geräten zusammen mit der Bildschirmsperre automatisch spätestens nach fünf Minuten einsetzt.
- Von mobilen Geräten dürfen Sie Personendaten, besonders schützenswerte Personendaten oder Persönlichkeitsprofile nicht auf externe private Geräte abspeichern.
- Mobile Geräte verfügen über diverse Möglichkeiten zur drahtlosen Kommunikation (WLAN, Bluetooth, Infrarot, GSM etc.). Arbeiten Sie gerade nicht mit dem mobilen Gerät, müssen Sie die vorhandenen Funktechnologien *ausschalten*. Vermeiden Sie wenn immer möglich die Nutzung von öffentlichen «Hotspots», seien Sie jedenfalls besonders vorsichtig.
- Ihr mobiles Gerät muss grundsätzlich mindestens einmal pro Woche mit dem Internet verbunden sein, damit der Virenschutz automatisch aktualisiert wird. Den Virenschutz bzw. die automatische Aktualisierung des Virenschutzes dürfen Sie in keinem Fall ausschalten.
- Bei Verlust oder Diebstahl eines mobilen Geräts müssen Sie umgehend den Servicedesk des AIO informieren, damit dieser die erforderlichen Schutzmassnahmen (Sperrung Ihres Accounts usw.) ergreifen kann.

SMS und E-Mail
Da die Nachrichtenübermittlung unverschlüsselt erfolgt, dürfen Sie auf diesem Weg keine Personendaten versenden. Dem Empfänger von SMS-Nachrichten muss bewusst sein, dass der Absender seine Identität beliebig fälschen kann. Haben Sie Zweifel bezüglich der Echtheit des Absenders, müssen Sie durch telefonische Rückfrage Klarheit schaffen.
Unverschlüsselter E-Mail-Versand via Internet darf keine Personendaten enthalten. Hinweise zur Verschlüsselung von Dokumenten finden Sie im Merkblatt «E-Mail».

Falls Sie die Anwendung «Web-Mail» oder «VPN/VDI» des AIO nutzen:
Diese Anwendungen verschlüsseln den Datenverkehr zwischen *Ihrem Gerät* und *dem AIO*. Dadurch entspricht der Zugang auf das eigene E-Mail-Konto demjenigen an Ihrem Arbeitsplatz im Büro. Die Hinweise im Merkblatt «E-Mail» müssen Sie auch für den Versand von Personendaten via Web-Mail bzw. VPN/VDI einhalten.

Vertrauliches gehört nicht an die Öffentlichkeit
Wenn Sie in der Öffentlichkeit mit mobilen Geräten arbeiten, müssen Sie verhindern, dass Unberechtigte auf den Bildschirm Ihres Laptops sehen, Zugang zu Ihrem Gerät erhalten oder Ihre Mobiltelefongespräche mithören können. Die gleichen Vorgaben müssen Sie einhalten, wenn Sie zu Hause geschäftliche Daten bearbeiten.