

Merkblätter zur Datensicherheit  
Datenschutzbeauftragter des Kantons Zug



## **Die fünf Merkblätter**

Der sichere Umgang mit Daten	2
Passwort	5
E-Mail	6
Kundenkontakt	8
Mobile Geräte	9

Datenschutzbeauftragter des Kantons Zug  
Regierungsgebäude  
Postfach 156  
6301 Zug

Telefon 041 728 31 87  
Fax 041 728 37 01

[rene.huber@allg.zg.ch](mailto:rene.huber@allg.zg.ch)  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

# Einleitung

## Warum diese Broschüre?

Bei der Bearbeitung von Personendaten mit den modernen Informations- und Kommunikationstechnologien bestehen gewisse Risiken und Gefahren. Die öffentlichen Organe bearbeiten eine Vielzahl von teilweise sehr sensiblen Daten der Zuger Bürgerinnen und Bürger. Diese haben einen Anspruch darauf, dass mit ihren Daten in jeder Hinsicht sicher umgegangen wird. Die vorliegende Broschüre enthält fünf Merkblätter, die Sie dabei unterstützen. Darin 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 sowie die Kundenkontakte.

## Für wen gelten die Hinweise?

Diese Hinweise gelten für die ganze öffentliche Verwaltung von Kanton und Gemeinden (Einwohner-, Bürger-, Kirch- und Korporationsgemeinden) und auch für Private, denen öffentliche Aufgaben übertragen sind.

## Wie setzen Sie die Vorgaben um?

Gewisse Vorgaben können Sie sofort umsetzen, andere benötigen Anpassungen an Ihrer Infrastruktur. Wichtig ist, dass Sie dabei planmässig und schrittweise vorgehen.

Grundlegende Hinweise können nicht jeder Situation gerecht werden. Je nach Ihrer Infrastruktur müssen allenfalls besondere Lösungen gesucht werden.

## 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.

## Aktualisierung dieser Broschüre

Die Technik ist dauernd Änderungen unterworfen. Dadurch können allenfalls auch Anpassungen dieser Broschüre nötig werden. Die aktuellste Version finden Sie auf unserer Website.

## Rechtsgrundlagen

Gestützt auf das Datenschutzgesetz des Kantons Zug (§ 7 DSG, BGS 157.1) hat der Regierungsrat die Datensicherheitsverordnung (DSV, BGS 157.12) erlassen. § 7 der DSV sieht vor, dass die Zuger Datenschutzstelle Merkblätter für die Instruktion der Mitarbeitenden zur Verfügung stellt.

Wir hoffen, dass Ihnen die vorliegenden Hinweise für einen sicheren Umgang mit den Daten dienlich sind.

Sollten Sie Fragen haben, so steht Ihnen die Datenschutzstelle gerne zur Verfügung.

# Merkblatt «Der sichere Umgang mit Daten»

## Kurz und bündig

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

Die wichtigsten Rechtsgrundlagen dieser Vorgaben finden Sie am Schluss dieses Merkblattes.

## Schutz gegen Zugriff Unberechtigter

So schützen Sie Ihre Daten am Arbeitsplatz:

### Bei Abwesenheit ab 15 Min.

- Aktivieren Sie die Bildschirmsperre mit Passwortschutz (drücken Sie gleichzeitig die drei Tasten «Ctrl», «Alt» und «Del», anschliessend mit «Enter/Eingabe» bestätigen oder gleichzeitig «Windows-Taste» und «L»).
- Bewahren Sie Unterlagen (Papiere, Dossiers, elektronische Datenträger), die besonders schützenswerte Personendaten enthalten, abgeschlossen auf.

### Bei Arbeitsschluss

- Melden Sie Ihren Computer vom Netzwerk ab und schalten Sie ihn aus.
- Sämtliche Unterlagen oder Datenträger, die Personendaten enthalten, müssen Sie verschlossen aufbewahren.

## Weitergabe, Speichern und Löschen von Daten

### Weitergabe von Daten

Verwenden Sie zur Weitergabe von Daten grundsätzlich neue Datenträger (CD-ROM, DVD, Disketten).

### Speichern von Daten

Speichern Sie keine Daten auf der Hard-Disk Ihres PC (somit *nicht* im Bereich «C:» oder auf dem «Desktop» Ihres Rechners), sondern an dem Ort im Netzwerk, der Ihnen durch Ihren Arbeitgeber/IT-Dienstleister zur Verfügung gestellt wird. Damit haben nur Berechtigte Zugang zu Ihren Daten und nur so ist gewährleistet, dass die Daten durch Ihren IT-Dienstleister regelmässig gesichert werden.

## Löschen von Daten

- Wenn Sie Ihren PC oder ein anderes Gerät (Laptop, mobiles Telefon, USB-Sticks, Drucker/Kopierer etc.) abgeben oder an einen anderen Mitarbeitenden weitergeben müssen, löschen Sie alle Daten definitiv, die nicht mehr benötigt werden.
- Mit den Befehlen «Delete», «Erase», «Löschen» oder «(Quick)Format» vernichten Sie Daten nicht definitiv, diese bleiben rekonstruierbar. Erkundigen Sie sich bei Ihrem IT-Dienstleister, wie Daten unwiederherstellbar gelöscht werden können.
- Unterlagen in Papierform müssen im Aktenvernichter vernichtet werden.

## Schutz vor Verlust

### Mobile Datenträger

Daten auf mobilen Datenträgern (CD-ROM, DVD, Sticks etc., aber auch Dokumente in Papierform) sind erhöhten Gefahren und Risiken ausgesetzt, da sie leicht verlorengehen können. Entsprechend müssen Sie bei der Weitergabe die erforderlichen Massnahmen ergreifen: Sichern Sie den Datenträger (bzw. Ordner/Dateien) mit einem starken Passwort und wählen Sie die angemessene Zustellungsart (persönliche Übergabe, Bote, eingeschriebene Briefpost etc.).

## Viren

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 Anhänge, über Dateien (z.B. Spiele, Bildschirmschoner, Freeware etc.), die vom Internet heruntergeladen werden oder durch Speichermedien wie USB-Sticks, CD-ROM/DVD oder Disketten eingeschleppt.

### Sie schützen sich vor Viren, indem Sie

- an Ihrem Arbeitsplatz ein Virenschutzprogramm installieren (sofern dies nicht durch Ihren IT-Dienstleister erledigt wird)
- das Virenschutzprogramm nie deaktivieren und laufend aktualisieren

- USB-Sticks, CD-ROM/DVD und Disketten vor dem Gebrauch immer mit dem Virenschutzprogramm prüfen
- nur von Ihrem IT-Dienstleister zur Verfügung gestellte, rechtmässig lizenzierte Software verwenden.

#### Vorgehen bei Auftreten von Viren

- Computer ausschalten, keine eigenen Reparaturversuche vornehmen
- Ihren IT-Dienstleister und grundsätzlich auch Ihren Vorgesetzten informieren.

#### 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 Ihrem IT-Dienstleister und/oder Ihrem Vorgesetzten.

#### Kommunikation über Netze

##### Hinweise zu externen Netzen

Bei der Kommunikation über externe Netze ist Folgendes zu beachten:

- Unverschlüsselte Informationen sind bei der Benutzung eines öffentlichen Netzes (IT- bzw. Telefon-Netz) einseh- bzw. abhörbar. Personendaten dürfen über solche Datenkanäle nicht unverschlüsselt weiter gegeben werden.
- Wenn Sie am eigenen IT-Netz angemeldet sind, darf Ihr System nicht gleichzeitig über eine andere Verbindung beziehungsweise ein anderes Gerät (z.B. WLAN, Modem, Bluetooth, Infrarot, GSM etc.) mit einem *anderen* Netz verbunden sein.

#### 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. Einfache Vorsichtsmassnahmen ermöglichen ein sicheres Surfen:

- Schliessen Sie alle anderen Programme während Sie surfen.
- Übermitteln Sie vertrauliche Daten über sich (persönliche Daten, Kreditkartenangaben etc.) nur an vertrauenswürdige Websites und nur, wenn die Übertragung verschlüsselt erfolgt.
- Verwenden Sie zum Surfen nur ein System, auf dem lokal keine vertraulichen Daten gespeichert sind.
- Installieren Sie auf direkt mit dem Internet verbundenen Systemen eine sogenannte «Personal Firewall» (sofern dies nicht durch Ihren IT-Dienstleister erledigt wird).

#### Intranet und internes Netzwerk

Das Intranet ist ein Netzwerk für einen bestimmten Personenkreis. Ohne zusätzliche Massnahmen im Netzwerkbereich sind grundsätzlich dieselben Vorsichtsmassnahmen wie beim Internet zu treffen. Die Übertragung innerhalb des *kantonalen* Netzwerks gilt als sicher. Bei anderen Netzen müssen Sie sich über die Sicherheitsstandards des entsprechenden Netzes bei Ihrem IT-Dienstleister bzw. Ihrem Vorgesetzten erkundigen.

#### Datenspuren

##### In Dateien

Bedenken Sie, dass Dokumente, die mit Office-Programmen (Word, Excel, PowerPoint etc.) erstellt werden, automatisch eine ganze Reihe *versteckter Informationen* enthalten: Verfassername, Erstelldatum, alles Nähere zu sämtlichen Änderungen, Angaben zu weiteren Bearbeitenden etc. Wenn ein Adressat diese Angaben nicht kennen darf, ist das fragliche Dokument unter einer neuen Bezeichnung abzuspeichern oder noch besser ein PDF herzustellen.

##### Beim Surfen

Wer surft, hinterlässt Spuren auf dem eigenen PC (Cookies, Cache, Verlauf, Auto-Vervollständigen etc.) und eine ganze Reihe von Protokollierungen auf den beteiligten Servern:

- Cookie: kurzes Textfile, das auf Ihrem PC gespeichert wird und meist Angaben zu Ihrer Internet-Nutzung enthält.

- Cache: Abspeicherung besuchter Internetsites und weiterer Informationen auf Ihrem Rechner.
- History: speichert den Verlauf der besuchten Sites.
- Funktion «Auto-Vervollständigen»: speichert frühere Eingaben zu besuchten Websites und schlägt diese vor, wenn wiederum die gleichen Angaben neu eingegeben werden.
- Protokollierungen: enthalten Informationen über alle Aktivitäten, die auf der Arbeitsstation ausgeführt wurden. Diese sind auf den beteiligten Servern gespeichert und enthalten unter anderem etwa die (IP-)Adresse Ihres PC, den Zeitpunkt und die besuchten Sites etc. Sie haben keine Möglichkeit, diese Angaben zu löschen.

Datenspuren zeigen auch private Nutzung von Informatikmitteln auf. Klären Sie ab, ob und unter welchen Bedingungen Ihnen die private Nutzung von Informatikmitteln erlaubt ist. Für die Mitarbeitenden der kantonalen Verwaltung gilt: geringfügige private Nutzung des Internets ist – analog wie die Nutzung des Telefons – erlaubt.

Löschen Sie Cookies, Cache, Verlauf und Auto-Vervollständigen des Browsers regelmässig auf Ihrer Arbeitsstation (im Internet-Explorer z.B.: Extras -> Internetoptionen -> Allgemein -> Browserverlauf: «Alle löschen»).

#### 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)
- Personalgesetz (BGS 154.21) und Personalverordnung (BGS 154.211)
- Strafgesetzbuch (SR 311.0)

#### Wichtige zusätzliche Hinweise

Datenschutzbeauftragter des Kantons Zug  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

Datenschutzbeauftragter des Kantons Zürich  
Auf der Website des Zürcher Datenschutzbeauftragten finden sie ein sehr nützliches Lernprogramm zur Datensicherheit, ein weiteres zum Datenschutz, ein Tool zur Grobanalyse getroffener Massnahmen für Datenschutz und Informatik-sicherheit («Datenschutz-Review») und ein Programm zur Überprüfung der Qualität von Passwörtern («Passwort-Check»):  
[www.datenschutz.ch](http://www.datenschutz.ch)

Eidg. Datenschutz- und Öffentlichkeits-  
beauftragter (EDÖB)  
[www.edoeb.admin.ch](http://www.edoeb.admin.ch)

# 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 einen Unberechtigten 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

- besteht aus mindestens 8, besser 10 oder mehr Zeichen
- enthält Zahlen, Buchstaben und Sonderzeichen kombiniert
- hat Gross- und Kleinbuchstaben
- können Sie sich gut merken, andere aber nicht erraten, zum Beispiel Sonn\*\*EN00schein, fRan?ziska57
- besteht nicht nur aus Wörtern – auch nicht in einer Fremdsprache – oder Namen, wie sie in einem Wörterbuch zu finden sind, auch nicht nur aus Zahlen wie etwa Telefonnummern, Geburtsdaten oder Auto-Kennzeichen, da diese leicht erraten werden können.

### Wichtige Hinweise bezüglich Passwörter zu Fachanwendungen

In Abweichung der vorstehenden Regelungen gelten zurzeit bei AIO-Passwörtern die folgenden Einschränkungen:

- Das iSeries Passwort muss aus mindestens 6 und darf höchstens 10 Zeichen umfassen.
- Das Passwort muss mit einem alphabetischen Zeichen oder den Zeichen @, #, \$, \_ beginnen,

gefolgt von alphabetischen Zeichen (a–z), Zahlen (0–9) oder den Zeichen @, #, \$, \_.

- Leerzeichen sind nicht erlaubt.
- Gross-Kleinschreibung wird nicht berücksichtigt.

### Anleitung für sichere Passwörter

Bilden Sie einen Satz, den Sie sich gut merken können und setzen Sie den Anfang der einzelnen Wörter zu einem Passwort zusammen. Etwa:

- «Der Widerspruch ist es, der uns produktiv macht!» wird zum Passwort «DWiedupm!».
- «Wenn die Sonne scheint, gehe ich um 3 Uhr!» wird zu «WdSsgiu3U!».
- «Ich will jeden Tag vier Schokoladen essen!» wird zu «IwjT4Se!».

### Handhabung des Passwortes

- Halten Sie Ihr Passwort unter allen Umständen geheim. Lassen Sie sich bei der Eingabe eines Passwortes nicht beobachten.
- Ändern Sie das Passwort nach spätestens vier Monaten. Bei Verdacht auf Missbrauch *sofort* und melden Sie dies Ihrer vorgesetzten Stelle und Ihrem IT-Dienstleister.
- Verwenden Sie für verschiedene Anwendungen auch verschiedene Passwörter.
- Passwörter dürfen nicht an andere Mitarbeitende oder Dritte weitergeben werden. Auch nicht an Ihre Stellvertretung. Mitarbeitenden der Informatik oder Administratoren werden Sie übrigens nie nach Ihrem Passwort fragen. Diese Frage darf somit auch nie beantwortet werden.
- Verwenden Sie privat andere Passwörter als im Geschäft.

### 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](http://www.datenschutz.ch)

### Weitere Informationen

[www.datenschutz-zug.ch](http://www.datenschutz-zug.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 folgenden 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. 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 die richtigen Dokumente beigelegt haben.

### **Wissen Sie wirklich wer der Adressat ist?**

Wenn Sie vertrauliche Daten per E-Mail übermitteln, müssen Sie stets bedenken, dass der Empfänger allenfalls die eingehenden E-Mails an sein Sekretariat oder an seine Stellvertretung weiterleitet. Falls Drittpersonen keine Kenntnis der Daten erhalten dürfen, müssen Sie mit dem Empfänger Rücksprache nehmen oder einen anderen Kommunikationsweg wählen – etwa die «Persönliche/Vertrauliche» Briefpost.

### **Versand innerhalb des verwaltungseigenen Netzes**

Das Versenden von E-Mails innerhalb des verwaltungseigenen Netzwerkes gilt grundsätzlich als sicher. Ist somit sowohl der Absender wie auch der Empfänger am verwaltungseigenen Netz angeschlossen, dürfen grundsätzlich auch besonders schützenswerte Daten unverschlüsselt übermittelt werden.

An der E-Mail-Adresse können Sie erkennen, ob eine kantonale oder gemeindliche Stelle Teil des kantonalen Netzes ist. Endet die Adresse auf «.zg.ch», erfolgt die Zustellung über das eigene Netz. In den beiden folgenden Beispielen dürfen Daten somit unverschlüsselt übermittelt werden:  
peter.muster@huenenberg.zg.ch  
peter.muster@dbk.zg.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 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 hingegen unverschlüsselt per E-Mail verschickt werden. So etwa die Bekanntgabe von Öffnungszeiten oder der Hinweis auf Gesetzesbestimmungen.

Personendaten dürfen hingegen über das Internet verschickt werden, wenn sie korrekt *verschlüsselt* sind. Sofern Ihr E-Mail-System die Verschlüsselung von E-Mails und Anhängen nicht direkt ermöglicht, können Sie Office-Dokumente mit einem sicheren Passwort schützen und diese anschliessend per E-Mail über das Internet versenden. Wichtig dabei ist, (1) dass die Verschlüsselung korrekt vorgenommen wird, (2) ein sicheres Passwort gewählt wird und (3) dieses dem Adressaten nicht per E-Mail, sondern auf einem anderen Kommunikationsweg mitgeteilt wird. Alles Nähere dazu finden Sie im Hinweis am Ende dieses Merkblattes.

Wenn Sie jemandem ein elektronisches Dokument per E-Mail via Internet zustellen müssen und obige Sicherheitsmassnahmen einhalten, so haben Sie grosse Gewähr, dass nur der berech-

tigte Adressat Kenntnis vom Inhalt erhält. Wenn es sich jedoch um ein Dokument mit *besonders vertraulichem* Inhalt handelt, ist der Versand per Briefpost oder die persönliche Übergabe der elektronischen Zustellung vorzuziehen.

(Ergänzender Hinweis für die Nutzenden der Anwendung «Web-Mail/Web-Access» des AIO: diese Anwendung verschlüsselt *den Datenverkehr zwischen dem Web-Mail Nutzenden und dem AIO*. Dadurch entspricht der Zugang auf das eigene E-Mail-Konto demjenigen am Arbeitsplatz im Büro. Inwiefern Personendaten via Web-Mail verschickt werden dürfen, ergibt sich hingegen aus den vorstehenden Hinweisen.)

#### Erhalt von E-Mails

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

- E-Mails von zweifelhafter Herkunft sind *ungeöffnet* zu löschen.
- Ungeöffnet zu löschen sind auch Beilagen wie Bildschirmschoner (Dateien mit der Endung «.scr»), ausführbare Dateien («.exe», «.bat», «.vbs» etc.) und Bilder von zweifelhafter Herkunft.
- Bei Anfragen per E-Mail hat man 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.

#### Vorgehen bei Ferienabwesenheit

- Eingehende E-Mails dürfen Sie nicht an eine E-Mail-Adresse ausserhalb des eigenen Netzes automatisch weiterleiten. Bei automatischer *interner* Weiterleitung an Ihre Stellvertretung oder Ihr Sekretariat ist zu bedenken, dass dann auch Ihre privaten E-Mails oder vertraulichen geschäftlichen Nachrichten an Ihre Stellvertretung oder an Ihr Sekretariat zugestellt werden.
- Sie müssen Absenderinnen und Absender von E-Mails mit einer automatischen Antwort über

Ihre Ferienabwesenheit und Ihre Stellvertretung informieren.

#### Wichtige zusätzliche Informationen im Umgang mit E-Mail

##### Private Nutzung von E-Mails?

Ob Sie von Ihrem Arbeitsplatz aus private E-Mails versenden dürfen, ist eine personalrechtliche Frage. Für Mitarbeitende des Kantons ist alles Nähere dazu in der «Verordnung über die Benutzung von elektronischen Kommunikationsmitteln im Arbeitsverhältnis (E-Mail und Abruf von Webseiten)» (BGS 154.28) geregelt. Für gemeindliche Mitarbeitende ist das gemeindliche Personalrecht anwendbar. Erkundigen Sie sich diesbezüglich bei Ihrem Vorgesetzten bzw. der Personalabteilung.

##### Zur Verschlüsselung von (Office-) Dokumenten

Vgl. die Hinweise des Zuger Datenschutzbeauftragten zur Verschlüsselung von Office-Dokumenten im Beitrag «Wie kann ich Dokumente sicher per E-Mail versenden?» (in: «Schulinfo Zug, Nr. 3, 2004-05»), zugänglich auf der DSB-Homepage (Bereich «Kanton Zug/Aktuelles»).

##### Weitere Informationen

[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

## Merkblatt «Kundenkontakt»

### Kurz und bündig

Dieses Merkblatt gibt Hinweise, wie Personendaten beim Kontakt mit Externen zu schützen sind.

Für den Schutz von Personendaten in Ihrem Bereich sind ausschliesslich Sie selber verantwortlich. Entsteht ein Schaden durch nicht korrekten Umgang mit Personendaten, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden.

### Zur Identität von Anfragenden

Die Identifikation der externen Person ist absolut zentral im Kontakt mit Dritten. Es dürfen nie Daten an Personen oder Stellen herausgegeben werden, die nicht mit Sicherheit korrekt identifiziert sind.

- Werden Daten am *Telefon* bekannt gegeben, hat man sich mit entsprechenden Rückfragen Klarheit über die Identität der anrufenden Person zu verschaffen. Diese Sicherheitsmassnahmen sind dem Anrufenden mitzuteilen (vgl. etwa die telefonische Abwicklung von Bankgeschäften). Falls dies nicht möglich ist, muss man die fragliche Person/Stelle zurückrufen.
- Bei Anfragen per *E-Mail* hat man grundsätzlich keinerlei Gewissheit über die Identität des Absenders, da dieser die Informationen über seine Identität problemlos beliebig selber definieren kann.
- Bei der Datenbekanntgabe *per Fax oder SMS* hat man keinerlei Sicherheit, wer allenfalls (auch noch) Zugriff zum entsprechenden Gerät hat. Deshalb ist diese Kommunikationsart vorgängig mit dem Adressaten abzusprechen.

### Voraussetzungen der Datenbekanntgabe

- Das Amtsgeheimnis gilt grundsätzlich auch zwischen den verschiedenen Stellen *innerhalb der Verwaltung*.
- Personendaten dürfen anderen Stellen grundsätzlich nur dann bekanntgegeben werden, wenn eine entsprechende *ausdrückliche gesetzliche Grundlage* dies zulässt oder die betroffene Person der Datenbekanntgabe zugestimmt hat. Zudem ausnahmsweise, wenn ein

Organ für die Erfüllung seiner gesetzlichen Aufgaben *zwingend* auf die fraglichen Daten angewiesen ist, ohne die fraglichen Daten somit seine Arbeit schlechterdings nicht erfüllen könnte.

- An *Privatpersonen* darf ausschliesslich Auskunft über ihre *eigenen* Daten gegeben werden – grundsätzlich jedoch nie über andere Privatpersonen (wichtigste Ausnahmen: Adressauskunft bei der Einwohnerkontrolle und Anfrage bezüglich Fahrzeughalter beim Strassenverkehrsamt).

### Zum Einsichtsrecht der Betroffenen

- Jede betroffene Person hat das Recht, ihre *eigenen* Daten einzusehen und kann grundsätzlich kostenlose Kopien ihrer Daten verlangen. Es ist deshalb wichtig, dass sämtliche Unterlagen korrekt formuliert sind und geordnet aufbewahrt werden.
- Jede betroffene Person hat das Recht, falsche Daten berichtigen zu lassen.
- Die Betroffenen haben das Recht zu wissen, zu welchem Zweck und auf welcher Rechtsgrundlage Daten über sie bearbeitet und an wen sie weitergegeben werden.
- Auskünfte an Betroffene über ihre eigenen Daten müssen *speditiv* erfolgen und vollständig und richtig sein. Der anfragenden Person entstehen grundsätzlich keine Kosten. Die Beantwortung der Anfrage erfolgt in der Regel schriftlich.

### Weitere Informationen

[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

# Merkblatt «Mobile Geräte»

## Vorweg

Alle Mitarbeitende, die mit mobilen Geräten arbeiten, sind 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 dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden.

## Mobile Geräte

Mobile Geräte sind Laptops/Notebooks, PDA, Mobiltelefone/Smartphones, USB-Sticks (und andere mobile Speichermedien) sowie alle anderen mobilen technischen Geräte, auf denen geschäftliche Informationen bzw. Personendaten verarbeitet oder abgespeichert werden. Für mobile Geräte gelten grundsätzlich dieselben Sicherheitsbestimmungen wie für feste Arbeitsstationen. Absolut zentral ist der Schutz des Gerätes durch ein *starkes Passwort* (s. dazu das separate Merkblatt «Passwort»). Zusätzliche Vorschriften sind nachfolgend erwähnt. Von entsprechend gesicherten mobilen Geräten dürfen Personendaten, besonders schützenswerte Personendaten oder Persönlichkeitsprofile grundsätzlich nicht auf externe *private* stationäre Geräte abgespeichert werden.

Mobile Geräte verfügen über diverse Möglichkeiten zur drahtlosen Kommunikation (WLAN, Bluetooth, Infrarot, GSM etc.). Der Benutzende des mobilen Geräts muss bei dessen Nichtgebrauch die vorhandenen Funktechnologien ausschalten. Die Nutzung von öffentlichen «Hotspots» ist grundsätzlich zu vermeiden, mindestens ist besondere Vorsicht geboten.

Notebook/Laptop: Zur Aktualisierung des Virenschutzes muss das Gerät grundsätzlich wöchentlich an das lokale Netzwerk oder ans Internet angeschlossen werden. Der Virenschutz bzw. die automatische Aktualisierung des Virenschutzes darf nicht ausgeschaltet werden.

Der IT-Verantwortliche muss über Verlust oder Diebstahl eines mobilen Geräts *umgehend* infor-

miert werden, damit er die erforderlichen Schutzmassnahmen (Sperrung des Accounts usw.) ergreifen kann.

## Verschlüsselung

- Die Gefahr von Verlust oder Diebstahl ist bei tragbaren Geräten besonders gross. Sie müssen deshalb zwingend die erforderlichen Sicherheitsmassnahmen ergreifen.
- Der Zugang zu den Daten muss mindestens durch ein sicheres Passwort geschützt werden (s. dazu das Merkblatt «Passwort»).
- Der Passwortschutz muss bei Notebooks zusammen mit der Bildschirmsperre spätestens nach zehn Minuten einsetzen.

## SMS, MMS und E-Mail

Da die Nachrichtenübermittlung via SMS und MMS unverschlüsselt erfolgt, dürfen auf diesem Weg keine Personendaten versendet werden. Dem Empfänger von SMS- und MMS-Nachrichten muss bewusst sein, dass der Absender seine Identität beliebig fälschen kann. Bei Zweifeln an der Echtheit des Absenders muss durch telefonische Rückfrage Klarheit geschaffen werden.

Unverschlüsselter E-Mail-Versand via Internet darf *keine Personendaten* enthalten.

(Ergänzender Hinweis für die Nutzenden der Anwendung «Web-Mail/Web-Access» des AIO: diese Anwendung verschlüsselt *den Datenverkehr zwischen dem Web-Mail Nutzenden und dem AIO*. Dadurch entspricht der Zugang auf das eigene E-Mail-Konto demjenigen am Arbeitsplatz im Büro. Inwiefern Personendaten via Web-Mail verschickt werden dürfen, ist den Hinweisen im Merkblatt «E-Mail» zu entnehmen.)

## Vertrauliches gehört nicht an die Öffentlichkeit

Wer in der Öffentlichkeit mit mobilen Arbeitsgeräten arbeitet, muss verhindern, dass Unberechtigte auf den Bildschirm des Laptops sehen oder die Mobiltelefongespräche mithören können.

## Weitere Informationen

[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

