

Merkblatt Datenschutz im E-Government für Gemeinden und kantonale Behörden

1. Ziele dieses Merkblattes¹

Viele Gemeinden und alle Kantone informieren die Bürger² im Internet allgemein über ihre Tätigkeiten. Auch andere Benutzer des Internets können jederzeit, rasch und weltweit auf solche Informationen zugreifen. Darüberhinaus können Personen im Internet über einen Online-Schalter Formulare ausfüllen und diese direkt elektronisch oder via E-Mail versenden. Bei anderen Online-Schaltern können Formulare elektronisch bestellt werden. **Vertrauen** der Benutzer der Cyber-Administration ist ein Schlüsselfaktor für den Erfolg von E-Government-Projekten, weil die neuen Technologien neue Herausforderungen für den Schutz der Privatsphäre darstellen. Deshalb ist dem Schutz der Privatsphäre ein hoher Stellenwert in E-Government-Projekten einzuräumen und es sind möglichst innovative Technologien zum besseren Schutz der Privatsphäre einzusetzen.

Dieses Merkblatt möchte Gemeinden und kantonalen Behörden eine Hilfe bei der datenschutzkonformen Gestaltung von E-Government-Projekten geben.³

2. Datenschutzrechtliche Grundsätze im Bereich E-Government

Im Rahmen eines E-Government-Projektes sind folgende datenschutzrechtliche Fragen zu stellen (Checkliste):

- **Sachdaten:** Werden ausschliesslich Sachdaten⁴ bearbeitet? Grundsätzlich ist die Bearbeitung von Sachdaten, dazu gehören auch korrekt anonymisierte Personendaten, problemlos zulässig (siehe aber die nachfolgende Ausnahme).
- **Amtsgeheimnis / gesetzliche Geheimhaltungspflicht:** Werden Daten – Sachdaten und/oder Personendaten - bearbeitet, welche dem Amtsgeheimnis oder einer speziellen Geheimhaltungspflicht unterstehen?
- **Rechtsgrundlage:** Liegt eine ausdrückliche Rechtsgrundlage für die Bearbeitung von (besonders schützenswerten) Personendaten im Internet vor?
- **Verhältnismässigkeit und Zweckbindung:** Werden bei der Kommunikation und bei Transaktionen nur soviel Personendaten beschafft oder bearbeitet, als für die Bearbeitung des gesetzlichen Auftrages notwendig sind oder als der Benutzer von Gesetzes wegen angeben muss? Wird die Datenmenge durch E-Government ansteigen?

¹ Dieses Merkblatt ist in Zusammenarbeit mit den Datenschutzbeauftragten des Kantons Zug und Basel-Landschaft entstanden.

² Der Einfachheit halber wird im Folgenden die weibliche Form nicht angeführt.

³ Literatur für detailliertere Ausführungen zum E-Government: „Datenschutzgerechtes E-Government, Handlungsempfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder“, abrufbar im Internet unter www.bfd.bund.de/information/eGovernment.pdf, Bund unter www.admin.ch – ausgewählte Themen E-Government, Quichet Virtuel, Vote électronique, Eidgenössischer Datenschutzbeauftragter unter www.edsb.ch/d/themen/e-government/index/htm

⁴ Abgrenzung Sachdaten/Personendaten: Gewisse Daten können auf den ersten Blick für Sachdaten gehalten werden, obwohl es sich dabei um Personendaten handelt. So sind z.B. Daten zu einzelnen, ganz bestimmten Grundstücken nicht Sachdaten, sondern Personendaten, da sie direkt dem jeweiligen Grundstückseigentümer zugeordnet werden können.

- **Transparenz:** Können die Benutzer bei jeder Aufforderung, Personendaten bekanntzugeben, frei und bewusst entscheiden, ob sie die gewünschten Daten liefern? Erhalten sie jeweils Informationen über Zweck, fakultative und notwendige Angaben, den Inhaber der Datensammlung (verantwortliche Stelle) und die Dauer der Datenaufbewahrung?
- **Auskunftsrecht:** Hat der Benutzer die Möglichkeit die ihn betreffenden Daten zu überprüfen und ihre Löschung oder Berichtigung zu verlangen?
- **Anonymer Zugang:** Haben die Benutzer die Möglichkeit, die Verfolgbarkeit (z.B. mittels IP-Nummern oder Cookies⁵) der von ihnen besuchten Websites auszuschliessen? Wird die Verwendung von Pseudonymen⁶ oder von datenschutzfreundlichen Technologien ermöglicht?
- **Datensicherheit Kommunikation Server:** Werden bei der Kommunikation und bei Transaktionen die Vertraulichkeit, Integrität und Authentifizierung der Daten durch den Einsatz angemessener Technologien zur Verschlüsselung (mindestens SSL 128bit), Firewall, Antivirenschutzprogramme, Anti-Spamfilter, Zugang nur über Passwort bei beschränktem Berechtigungskreis, gewährleistet? Ist die Datensicherheit bei Servern (Web-Server, Applikationsserver) durch angemessene organisatorische und technische Massnahmen garantiert?
- **Datenbearbeitungserklärung (Privacy Policy)⁷:** Ist eine Information für die Benutzer der Websites geplant oder vorhanden, welche über folgende Punkte informiert?
 - Welcher Rechtsgrundlage untersteht die Datenbearbeitungspraxis der Gemeinde respektive des Kantons?
 - Welche Personendaten werden gesammelt und zu welchem Zweck?
 - Welche Wahlmöglichkeit zur Bearbeitung seiner Daten stehen dem Benutzer zu?
 - Welche Rechte, insbesondere Auskunfts- und Berichtigungsrechte haben die Benutzer?
 - Welche Stelle beantwortet Fragen über die Bearbeitung von Personendaten?
 - Welche Sicherheitsmassnahmen werden zum Schutz der Privatsphäre angewendet?

3. Welche Informationen dürfen ins Internet gestellt werden?

3.1 Das Internet als Archiv für die Ewigkeit

Das Internet ist ein „Archiv für die Ewigkeit ...“. Es gibt spezialisierte Suchmaschinen, welche *Kopien* von aktuellen Websites archivieren. Informationen bleiben so selbst dann allen zugänglich, wenn die entsprechenden Dateien im eigenen Web-Auftritt gelöscht sind. Was nicht der ganzen Menschheit für immer und ewig bekannt gegeben werden soll, ist deshalb *nicht* im Internet zu publizieren (Verhältnismässigkeit). So ist es z.B. keinesfalls zwingend, dass ein lokales Publikationsorgan im Verhältnis 1:1 im Internet gestellt wird. Wer ein Baugesuch eingereicht hat, wird froh sein, wenn er nicht mit entsprechender Werbung aus der ganzen Schweiz und dem benachbarten Ausland eingedeckt wird.

⁵ „Cookies“ sind Informationen (kleine Textdateien), die vom Web-Server eines Anbieters (z.B. Kanton, Gemeinde) auf dem Rechner des Internetbenutzers gespeichert werden. Bei einem späteren Besuch der Homepage des Anbieters werden diese Daten dann zurückübermittelt, sodass feststeht, dass es sich um denselben Rechner bzw. Benutzer handelt

⁶ „Pseudonym“ kommt aus dem Griechischen und bedeutet „fälschlich so genannt“. Die Identifizierung eines Benutzers im Internet ist zwar notwendig, aber anstelle seiner wirklichen Personalien wird eine angenommene Identität (z.B. ein Kennzeichen, Zahl) verwendet

⁷ Siehe das gute Beispiel einer privacy policy der Stadt Zürich, unter www.stadt-zuerich.ch

Fazit: Was bereits in Papierform veröffentlicht wurde, kann demnach nicht automatisch auch ins Internet gestellt werden. Ob etwas im Internet veröffentlicht werden kann, ist eine Frage, die selbst bei bereits erfolgter gedruckter Publikation eigenständig und unabhängig zu prüfen ist.

3.2 Voraussetzungen

Im Internet dürfen keine Daten (Sachdaten, Personendaten) veröffentlicht werden, welche dem **Amtsgeheimnis oder anderen gesetzlichen Geheimhaltungspflichten** unterstehen (z.B. Angaben über die Finanzlage in der Gemeinde solange diese nicht definitiv ist, Liste mit säumigen Steuerzahlern, Personalgeschäft, Sozialhilfeempfänger).

Personendaten dürfen zudem nur im Internet publiziert werden, wenn eine ausdrückliche **Rechtsgrundlage**, entweder eine ausdrückliche gesetzliche Bestimmung, welche die Veröffentlichung im Internet erlaubt⁸, oder ausdrückliche Einwilligung der betroffenen Person besteht. Für die Publikation von besonders schützenswerten Personendaten ist zudem eine formell gesetzliche Grundlage nötig.

3.3 Beispiele aus der Praxis:

- **Personendaten über Behörden, Verwaltungsangestellte (Adresslisten)**
 - a) Präsentiert sich eine kantonale oder kommunale Behörde oder Verwaltungsstelle im Internet, so hat sie als Arbeitgeberin das Recht, diejenigen Behördenmitglieder und Mitarbeiter namentlich zu erwähnen, welche für die Öffentlichkeit *Ansprechpersonen* sind. Dasselbe gilt von anderen Milizgremien wie Zweckverbänden, Feuerwehr, Zivilschutz etc..

Gestützt auf eine ausdrückliche gesetzliche Grundlage oder die ausdrückliche Einwilligung der betroffenen Personen genügt es für die gesetzliche Aufgabenerfüllung, folgende Personendaten *im Internet* zu veröffentlichen: *Name, Vorname, Funktion, die geschäftliche Adresse, die geschäftliche E-Mail-Adresse⁹, die geschäftliche Fax-Nummer.*

Zusätzliche private Personendaten (private Adresse, private E-Mail-Adresse) dürfen nur nach vorgängiger ausdrücklicher Zustimmung der betroffenen Person ins Internet gestellt werden:

- Bei den *Einwohnergemeinden*:
Gemeindepräsident, Gemeindeglied, Finanzverwalter/ Staatssteuerregisterführer, Friedensrichter, Präsidenten und Aktiare der Kommissionen, AHV-Zweigstelle, Zivilstandsamt.¹⁰
- Bei den *Bürgergemeinden*:
Bürgergemeindepäsident, Bürgersreiber.¹¹

⁸ Kanton Solothurn z.B.: Regierungsratsbeschlüsse sowie Informationen, welche keine besonders schützenswerten Personendaten enthalten § 15bis der Informations- und Datenschutzverordnung (InfoDV), in Kraft seit 01.07.2004 steht noch unter Vorbehalt des Vetorechts des Kantonsrates bis 16.09.2004, Amtsblatt § 4 InfoDV, Anwaltsregister § 5 der Verordnung über das Anwaltsregister

⁹ Siehe aber die Ausführungen in Seite 7 dieses Merkblattes zu „E-Mail“

¹⁰ Siehe als Beispiel für eine kleine und mittlere Einwohnergemeinde: Die Einwohnergemeinde Steinhof unter www.steinhof-so.ch und die Einwohnergemeinde Riedholz unter www.riedholz.ch

¹¹ Siehe das Beispiel auf der Homepage der Einwohnergemeinde Riedholz

- Bei den *Kirchgemeinden*:
Präsident der Kirchgemeinde, Kirchenverwalter, Pfarrer, eventuell weitere kirchliche Mitarbeitende wie Diakon, Mitarbeitender des kirchlichen Unterrichtes.¹²
- Bei *Zweckverbänden*:
Präsident des Zweckverbandes, Aktuar des Zweckverbandes, allenfalls Delegierte der Gemeinden.

Betreffend privater Angaben über alle übrigen Personen, welche *nicht Ansprechpersonen* sind (z.B. alle übrigen Gemeinderäte, übrigen Bürgerräte und Gemeindeangestellten), wird empfohlen, auf eine Publikation solcher Angaben zu verzichten. Wird dies dennoch gewünscht (z.B. Adressliste im Internet), muss vorgängig eine ausdrückliche Einwilligung eingeholt werden.

b) In der *kantonalen Verwaltung* ist es wegen deren Grösse nicht nötig, überhaupt private Daten von Ansprechpersonen im Internet zu veröffentlichen. Wenn dies dennoch geschieht (z.B. Hobbys von Mitarbeitern eines Teams), ist vorgängig die ausdrückliche Einwilligung der betroffenen Person Voraussetzung.

c) *Fotos von Ansprechpersonen* dürfen ebenfalls nur nach vorgängiger ausdrücklicher Einwilligung der betroffenen Person im Internet veröffentlicht werden. Eine ablehnende Haltung Betroffener ist zu respektieren. Dabei muss man sich bewusst sein, dass ein Foto heute technisch problemlos manipuliert und ohne Wissen der betroffenen Person auch auf illegalen Websites abgelegt werden kann.

- **Personendaten über Bürger**

a) *Amtsblatt, Protokolle oder Beschlüsse* politischer Gremien wie Regierungsrat, Gemeinderat oder von Verwaltungsstellen enthalten häufig auch Personendaten. Sofern nicht eine ausdrückliche gesetzliche Grundlage für eine Internetpublikation vorhanden ist oder eine ausdrückliche Einwilligung der betroffenen Person vorliegt, sind diese Dokumente nur anonymisiert im Internet zu veröffentlichen.¹³ Nicht öffentliche Regierungsratsbeschlüsse oder nicht öffentliche Gemeinderatsbeschlüsse gehören nicht ins Internet.

b) Über die Homepage kann auch der Zugang zu *Datenbanken*, z.B. bei der Homepage des Kantons Solothurn zum geographischen Informationssystem (SO!GIS) oder zum Anwaltsregister des Kantons Solothurn, ermöglicht werden. Bei Datenbanken mit Zugang über ein Passwort (teilweise bei SO!GIS) ist zu beachten, dass ein sicheres Passwort gewählt wird, das regelmässig (z.B. alle 60 Tage) gewechselt wird.¹⁴ Zudem können Sie einer mangelhaften Rechte- und Benutzerverwaltung vorbeugen, indem Sie eine dafür verantwortliche Person bestimmen. Überdies sind auch hier technische Massnahmen wie Firewall, Antivirenschutzprogramm etc. zu empfehlen.

- **Internet-Auftritt von Schulen**

a) Namen und Privatadressen von *Schülern* müssen auf Grund des gesetzlichen Lehrauftrages nicht im Internet veröffentlicht werden. Zudem sprechen auch

¹² Siehe das Beispiel auf der Homepage der Einwohnergemeinde Riedholz

¹³ Siehe die Beispiele unter Fussnote 4

¹⁴ Siehe dazu die Broschüre „Der sichere Umgang mit Informations- und Kommunikationsgeräten, herausgegeben von den Schweizerischen Datenschutzbeauftragten, abrufbar auf der Homepage des kantonalen Informations- und Datenschutzbeauftragten, www.datenschutz.so - Merkblätter. Die Mitarbeitenden der Verwaltung des Kantons Solothurn müssen spätestens nach Ablauf von 60 Tagen ihr Passwort ändern, ansonsten wird ihnen der Zugang zum System verwehrt.

Sicherheitsgründe gegen eine Veröffentlichung im Internet, selbst mit Einwilligung der Betroffenen. Kinder / Jugendliche können die vorhandenen Gefahren selber zu wenig einschätzen. Gewisse zusätzliche Informationen können unter Umständen in einem passwortgeschützten Bereich, somit für einen geschlossenen Kreis, veröffentlicht werden.

b) Die Veröffentlichung von privaten Personendaten von *Lehrkräften* (private Adresse, private Telefon-Nummer, private E-Mail-Adresse) im Internet ist ebensowenig notwendig zur Erfüllung des Lehrauftrages. Es genügt auch hier die Publikation der Adresse und des Telefons der Schule. Private Personendaten dürfen auf einer Website nur publiziert werden, wenn die betroffene Lehrkraft vorher ausdrücklich zugestimmt hat. Eine Weigerung oder ein Widerruf einer erteilten Zustimmung sind zu respektieren.

- **Fotos, Videoclips, Web-Kameras**

a) Fotos mit *Portraits* dürfen nur mit ausdrücklicher Einwilligung der betroffenen Person im Internet abgelegt werden, weil Personen klar identifizierbar sind und Aufnahmen auch ohne deren Wissen für andere (rechtswidrige) Zwecke im Internet weiterverwendet werden können.

b) Oftmals werden von *Veranstaltungen* (z.B. Gemeindejubiläum, Fasnachtsumzug, Schulreise, Jahresausflug) *Fotos* oder allenfalls kurze *Videoclips* im Internet veröffentlicht. Eine ausdrückliche Einwilligung bei der Vielzahl – erst Recht von namentlich nicht bekannten - betroffenen Personen kann vorgängig aus administrativen Gründen nur sehr schwer eingeholt werden. Viele Personen auf einem Foto oder in einem Videoclip (z.B. viele Schaulustige eines Fasnachtsumzuges) sind schwerer identifizierbar als Einzelpersonen, die in einem Portrait abgebildet sind. Deshalb sollte in dieser „datenschutzrechtlichen Grauzone“ auf der Website zumindest ein Hinweis auf das jederzeitige Widerrufsrecht angebracht und einem Widerruf umgehend Folge geleistet werden (z.B. Bild, Clip ganz löschen oder die betroffene Person – falls möglich – löschen). Ausserdem ist auf die zusätzliche Angabe von Personendaten zu verzichten.

c) *Web-Kameras*, welche den Kanton oder die Gemeinde zeigen, dürfen eingesetzt werden, solange keine Personen oder Fahrzeug-Schilder etc. identifizierbar sind. Auch sollte nicht auf die Lebensgewohnheiten oder anhand der sichtbaren Wohnungsbeleuchtung auf die An- und Abwesenheit von Hausbewohnern geschlossen werden können. Kameras sind entsprechend einzustellen.

4. Was ist speziell bei der Kommunikation im Internet zu beachten?

Es besteht ein nicht unerhebliches **Risiko**, dass sich eine Person für eine andere Person ausgibt und unter deren **Identität** (Name, Vorname) mit der Behörde kommuniziert. Wie soll die kantonale oder kommunale Behörde prüfen, ob „Daniel Schmid“ auch tatsächlich „Daniel Schmid“ ist? Eine elektronische Signatur, welche eine Person eindeutig identifiziert, steht gegenwärtig technisch noch nicht zur Verfügung. Allfällige Zweifel über die Identität können daher heute nur mit einer weniger kundenfreundlichen Kommunikation (siehe nachfolgend unter „elektronische Formulare“) oder mit zusätzlichem administrativem Aufwand (z.B. direkte Kontaktaufnahme) behoben werden.

4.1 Elektronische Formulare

Im Online-Schalter sind heute verschiedene Formulare allen Personen zugänglich, z.B. Anmeldung Schule, An-, Ab- und Mutationsmeldung des Wohnsitzes, Bestellung von Formularen wie Baugesuch, Passantrag, Fristerstreckung Steuererklärung, Handlungsfähigkeitszeugnis, Heimatausweis etc..

a) Vorgängig ist zu prüfen, ob für die effiziente gesetzliche Aufgabenerfüllung das *elektronische Abrufen, Downloaden, Ausdrucken von Formularen* genügt. Dem obenerwähnten Risiko der Kommunikation unter einer falschen Identität kann damit sachgerecht begegnet werden, indem der Bürger das entsprechende Formular ausdruckt, ausfüllt und direkt der zuständigen Behörde zustellt (direkt übergeben, in den Briefkasten der Behörde einwerfen, versenden via Post). Dabei soll das System auch ein anonymisiertes Downloaden eines Bestellformulars standardmässig ermöglichen, da die Behörde zu diesem Zeitpunkt (noch) keine Daten über den Bürger benötigt.

b) Ist das elektronische Formular auch elektronisch auszufüllen, ist zu prüfen, *welche Personendaten für das Ausfüllen der Datenfelder des Formulars geeignet und erforderlich* sind. Je nach Formular müssen mehr oder weniger Datenfelder ausgefüllt werden. In der Regel genügen folgende Angaben: *Name, Vorname, Adresse, Geburtsdatum, allenfalls noch E-Mail-Adresse oder Telefonnummer*, bei weiteren Feldern ist auf den freiwilligen Eintrag hinzuweisen (z.B. mit einem *)¹⁵. Auf Datenfelder, bei welchen besonders schützenswerte Personendaten auszufüllen sind, ist falls nicht nötig (z.B. Konfession bei Anmeldung Taufe), gänzlich zu verzichten.

c) Wegen der hohen Missbrauchsgefahr (Löschungen, Fälschungen etc.) wird empfohlen, das *ausgefüllte Formular nur verschlüsselt zu übertragen (mindestens SSL 128bit)*. Im Hinblick auf die Gestaltung *sicherer Kommunikation* ist ausserdem zu bedenken, dass die SSL-Verschlüsselung im Bereich der Behörden an dem von ihnen genutzten Web-Server endet. Es kann sich daneben also ein zusätzlicher Schutzbedarf im Bereich des Web-Server-Betriebs ergeben, insbesondere wenn dieser nicht von der Behörde selbst erfolgt.

d) Die übertragenen Personendaten dürfen *nur zur Sicherstellung der Bearbeitung im Web-Server gespeichert* werden. Sobald die *Übertragung stattgefunden* hat oder im Falle einer Bestellung eines *Formulars*, sobald dieses *zugestellt* wurde, sollen die Daten auf dem Web-Server wieder *gelöscht* werden. Soweit technisch möglich, ist eine automatisierte Löschung effizienter als eine manuell vorzunehmende Löschung. Das vom Bürger ausgefüllte Formular ist automatisiert oder *rasch*-möglichst manuell *in den Applikationsserver zu übertragen* und dort zu speichern, so lange es benötigt wird (z.B. bis Mutationsänderung des Wohnsitzes im Einwohnerregister vorgenommen und eine allfällige Gebühr bezahlt wurde).

4.2 E-Mail

Viele E-Government-Lösungen beinhalten auch die Möglichkeit zum Austausch von E-Mails. Sie bieten den Vorteil, dass neben der Übermittlung des eigentlichen Inhalts auch Dateien als Attachment mit versendet werden können, die in digitaler Form längere Texte, Bilder, Töne usw. enthalten können. Ausserdem bieten sie eine schnelle Kommunikationsmöglichkeit, die unabhängig von Büroöffnungs- oder Telefonzeiten genutzt werden kann. Bei allen Vorteilen des Einsatzes von E-Mails, bestehen jedoch auch verschiedene Risiken:

¹⁵ Umgekehrt können selbstverständlich auch die obligatorisch auszufüllenden Datenfelder mit * gekennzeichnet werden, siehe etwa bei der Einwohnergemeinde Hofstetten-Flüh unter www.hofstetten-flueh.ch.

a) Behörden, die ihre E-Mail-Adresse als Kommunikationsmöglichkeit auf ihrer Website anbieten, gehen das Risiko ein, von *Spams* (unerwünschter elektronischer Werbung) überflutet zu werden. Da dieses Problem zunehmend sowohl Firmen als auch Behörden Mühe bereitet und auch mit Spamfiltern kaum vermieden werden kann, sind *möglichst wenig E-Mail-Adressen auf den Websites zu veröffentlichen*. Es empfiehlt sich bei Gemeinden nur eine E-Mail-Adresse wie z.B. „*info@behörde*“ einzurichten. Bei Kantonen entspricht dies der Veröffentlichung der E-Mail-Adresse der jeweiligen Dienststelle (z.B. info@departement, info@Amt, info@Abteilung, info@Fachstelle). E-Mail-Adressen von Mitarbeitenden sind aus diesem Grund nicht im Internet zu publizieren. Nötigenfalls kann darauf hingewiesen werden, wie sich die E-Mail-Adressen der Mitarbeitenden zusammensetzen (z.B. E-mail: vorname.name@sk.so.ch). Da E-Mail-Adressen als Text leicht durch Suchmaschinen auswertbar sind, empfiehlt es sich, die E-Mail-Adresse als Graphik auszugestalten. Diese Lösung ist zwar nicht so kundenfreundlich, da die E-Mail-Adresse neu eingegeben werden muss. Die Adresse kann jedoch nur unter erschwerten Umständen ausgewertet und für Spamzwecke gesammelt werden.

b) Da E-Mails auf verschiedenen Servern im Internet zwischengespeichert werden, ist es leicht möglich, dass E-Mails auch von *unbefugten Personen gelesen, gefälscht, gelöscht oder mit Viren und Trojanischen Pferden (ausführbare Programmcodes) versehen* werden. Daraus ergeben sich drei Forderungen für den E-Mail-Gebrauch:

- Besonders *schützenswerte Personendaten und vertrauliche Daten sind ausserhalb des verwaltungsinternen Netzes nur verschlüsselt per E-Mail zu versenden*. Behörden, welche die Möglichkeit der Kommunikation via E-Mail ermöglichen, wird empfohlen, gut sichtbar einen Hinweis auf der Website zu platzieren, dass keinerlei besonders schützenswerte Personendaten und vertrauliche Daten per E-Mail an Adressaten ausserhalb des verwaltungsinternen Netzes versendet werden, da unverschlüsselte E-Mail-Kommunikation via Internet weniger vertraulich ist als der Versand einer Postkarte. Empfohlen wird gleichzeitig auch die Bürger in Broschüren oder im mündlichen Kontakt auf dieses Risiko hinweisen. Auch die Mitarbeitenden sind immer wieder darauf aufmerksam zu machen, dass keinerlei besonders schützenswerten Personendaten und keine vertraulichen Daten (Amtsgeheimnis) unverschlüsselt via Internet an Adressaten ausserhalb des verwaltungsinternen Netzes versendet werden dürfen¹⁶. Wenn in einem E-Mail besonders schützenswerte Personendaten oder andere schutzbedürftigen Daten übermittelt werden, sind diese Daten und auch die angehängten Dateien (Attachments) zu verschlüsseln¹⁷.
- Um das Problem des Löschens oder Verlustes einer E-Mail auf ihrem elektronischen Weg zum Empfänger zu vermeiden, ist bei wichtigen E-Mails ausserdem ein Verfahren zur *Empfangsbestätigung* mit dem Empfänger vereinbart werden.
- Den *E-Mail-Empfängern* wird empfohlen einen *Virens scanner* zu benutzen, um alle eingehenden E-Mails auf Viren zu prüfen. Da neben Inhalt auch leicht der Absender eines E-Mails gefälscht werden kann, können auch E-Mails von scheinbar seriösen oder offiziellen Adressen Viren enthalten. Da täglich neue Viren ihr Unwesen

¹⁶ Für die Mitarbeitenden der Verwaltung des Kantons Solothurn gilt seit dem 01.07.2003 die Weisung über die Benutzung der Informatiksysteme und –anwendungen in der kantonalen Verwaltung (siehe Beschluss des solothurnischen Regierungsrates Nr. 2003/1296, RRB, § 11 bezüglich Nutzung der Mäildienste)

¹⁷ Anmerkung: Mit Lese-/Schreibschutz angehängte Office-Dokumente können zwar "versteckt" werden, so dass der Empfänger es nur mittels eines separat (telefonisch) mitgeteilten Passwortes öffnen kann. Allerdings entspricht dieser Schutz nicht den Anforderungen an eine sichere Datenübermittlung wie bei der Verschlüsselung, Quelle Datenschutzbeauftragter des Kantons Zürich, www.datenschutz.ch – Themen – Datenübermittlung per E-Mail: Leseschutz und Schreibschutz

treiben, ist es sehr wichtig, dass das Virens Scanner-Programm regelmässig upgedatet wird.

- Im Hinblick auf die Gestaltung *sicherer Kommunikation* kann sich auch hier wie bei den „elektronischen Formularen“ ein zusätzlicher Schutzbedarf im Bereich des Web-Server-Betriebs ergeben, insbesondere wenn dieser nicht von der Behörde selbst erfolgt. Ferner gilt es, auch die Kommunikationswege zwischen den Sachbearbeitern der E-Mails innerhalb der Behörde und dem Web-Server in die Sicherheitsüberlegungen mit einzubeziehen.

Der Beauftragte für Information und Datenschutz des Kantons Solothurn

Daniel Schmid / 27.08.2004