



Merkblatt „Versand von E-Mails mit Personendaten“

1 Ziel des Merkblattes

Das Versenden von E-Mails ist aus dem Alltag nicht mehr wegzudenken. Viele E-Mails enthalten Personendaten, oft auch besonders schützenswerte. In der Regel werden E-Mails unverschlüsselt übermittelt. Bekannt ist aber, dass das unverschlüsselte Versenden einer E-Mail weniger sicher ist, als das Verschicken einer Postkarte, weil:

- Eine E-Mail mit geringem technischen Wissen abgefangen, mitgelesen oder verändert werden kann;
- E-Mails im Gegensatz zur Postkarte auch einfach nach Schlüsselbegriffen durchsucht werden können;
- Internet-Provider mit Sitz in der Schweiz verpflichtet sind, E-Mails während sechs Monaten aufzubewahren und bei Bedarf den Behörden bekannt zu geben.

Dieses Merkblatt zeigt auf, was für öffentliche Organe i.S.d. Datenschutzgesetzes¹ beim Versand von E-Mails zulässig ist. Wichtig ist dabei die Unterscheidung, ob es sich um "gewöhnliche" Personendaten² besonders schützenswerte Personendaten³ oder Persönlichkeitsprofile⁴ handelt.⁵

2 Verantwortung des öffentlichen Organs

Das öffentliche Organ (Kanton, Gemeinde⁶) ist für die datenschutzkonforme Bearbeitung der Personendaten selbst verantwortlich und für die Einhaltung der Datenschutzbestimmungen beweispflichtig. Es ist verpflichtet, organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten zu treffen.

Beim Versand von Personendaten durch sensible Einrichtungen wie Gesundheits-, Kindes- und Erwachsenenschutzbehörden oder Sozialen Diensten handelt es sich in jedem Fall um besonders schützenswerte Personendaten, da alleine die Tatsache, dass jemand Klientin/Patientin bzw. Klient/Patient bei der betreffenden Stelle ist, besonders schützenswert ist.

¹ sGS 142.1; abgekürzt DSG, in Kraft seit 25.06.2019.

² Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 1 Abs. 1 a DSG).

³ Besonders schützenswerte Angaben sind i.S.v. Art. 1 Bst. b DSG Angaben über:

- Religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten. Ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation oder einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert;
- Gesundheit, Intimsphäre und ethnische Zugehörigkeit;
- Genetische Daten;
- Biometrische Daten, die eine natürliche Person eindeutig identifizieren;
- Leistungen und Massnahmen der sozialen Hilfe;
- Strafrechtliche sowie disziplinarische Verfahren und Sanktionen;

⁴ Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt (Art. 1 Abs. 1 Bst. d DSG).

⁵ Im Zuge der Überarbeitung des DSG und Anpassung an die Richtlinie (EU) 2016/980 wurde der Begriff des Profilings (jede Art der automatisierten Bearbeitung von Personendaten; Art. 1 Abs. 1 Bst. d^{bis} DSG) neu eingeführt. Für die Bearbeitung von Profiles gemäss Art. 5 Abs. 2 DSG gelten die gleichen Bestimmungen wie für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Da der Versand eines Profilings in einer E-Mail eher unwahrscheinlich ist, beschränkt sich dieses Merkblatt auf den Versand von Personendaten, besonders schützenswerten Personendaten und Persönlichkeitsprofilen.

⁶ Gemäss Art. 2 Abs. 1^{bis} DSG sind Private dem öffentlichen Organ gleichgestellt, wenn sie Staatsaufgaben erfüllen. Infolgedessen gelten für sie die gleichen Vorgaben.



3 Grundsätze für den Versand / die Nutzung von E-Mail

- Es sollen so wenig Personendaten wie möglich verwendet werden (Datensparsamkeit).
- Eigenverantwortung: Wer Daten bearbeitet, ist für den gesetzesmässigen, zweckmässigen und verhältnismässigen Umgang und deren korrekte Weiterverarbeitung (z.B. Zugriffsberechtigung, Aktualisierung oder Löschung) verantwortlich.
- Fehlleitungen von E-Mails durch Irrtum stellen ein erhebliches Risiko dar. Die Adressen müssen sorgfältig gewählt werden. Automatismen bzw. „Komfortfunktionen“ sollen möglichst vermieden werden.
- Auf nicht kantonseigenen Informatikmitteln, insbesondere auf privaten Geräten, dürfen keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile des Kantons bearbeitet oder gespeichert werden.
- Nicht alles, was technisch möglich ist, ist auch erlaubt.
- E-Mails sollten keine Angaben über Passwörter, Konto- und/oder Kreditkartennummern oder andere Zugangsdaten wie z.B. Benutzeridentifikationen enthalten.
- Es sollten keine grossen Datenmengen verteilt/gestreut werden.
- Nur bekannte Verteiler auswählen und verwenden.
- Es muss unterschieden werden, ob eine E-Mail innerhalb von KOM SG⁷, nach ausserhalb oder an die betreffende Person selber versendet wird (siehe nachfolgend Ziff. 4 und 5).

4 Versand von nicht besonders schützenswerten Personendaten⁸

4.1 Innerhalb von KOM SG⁹

In diesem Bereich gilt der E-Mail-Verkehr als sicher, weshalb der Versand nicht besonders schützenswerter Personendaten ohne Einschränkungen zulässig ist.

4.2 An Stellen ausserhalb des KOM SG (andere Kantone, Gemeinden etc.):

Dies ist in der Regel zulässig.

4.3 An die betroffene Person

Dies ist in der Regel zulässig. Erhält die Stelle eine E-Mail von der betroffenen Person, darf sie von der stillschweigenden Einwilligung dieser Person ausgehen und die Antwort ebenfalls per E-Mail erteilen. Eine Ausnahme bilden Antworten, die besonders schützenswerte Personendaten, beispielsweise Gesundheitsdaten bzw. Persönlichkeitsprofile beinhalten.

5 Versand von besonders schützenswerten Personendaten und Persönlichkeitsprofilen

5.1 Innerhalb von KOM SG

Auch wenn dieser Bereich als sicher gilt, sollten sehr sensible Daten (z.B. psychiatrische Gutachten) nur verschlüsselt¹⁰ versandt werden. Ob die Daten als derart sensibel einzustufen sind, dass sie verschlüsselt versendet werden sollten, beurteilt sich nach dem Kontext.

⁷ <https://intranet.sg.ch/informatik/geschaeftsstellen/komsg/Seiten/default.aspx>

⁸ Siehe aber Ausführungen unter Ziff. 2.2. Abschnitt dieses Merkblattes.

⁹ Die Adresse ist im globalen Adressbuch vorhanden oder mit „EXT“ bezeichnet.

¹⁰ Wobei der Schlüssel selbstverständlich geheim zu halten ist.



5.2 An Stellen ausserhalb des KOM SG

In diesem Fall müssen die E-Mails verschlüsselt werden. Dies gilt explizit auch für alle Mitarbeitenden der kantonalen Verwaltung gemäss der Dienstanweisung über Einsatz und Verwendung der Informatikmittel.

5.3 An die betroffene Person

Diese E-Mails müssen verschlüsselt verschickt werden, auch wenn die Absenderin bzw. der Absender ihre Nachricht unverschlüsselt verschickt. Eine Ausnahme kann gemacht werden, wenn die freiwillige, ausdrückliche schriftliche Einwilligung nach angemessener Information (informierte Einwilligung) der urteilsfähigen Klientin oder des urteilsfähigen Klienten vorliegt.

6 Alternativen zum unverschlüsselten E-Mail-Versand von Personendaten

6.1 Sichere Datenübermittlung mit E-Mail:

- Abraxas Secure E-Mail Service;
- Swiss Government Zertifikat;
- Ablage auf Datenserver (durch entsprechenden Link in der Nachricht).

6.2 Verschlüsselung auf Dokumentenebene:

- Verschlüsselung von Office-Dokumenten;
- Verschlüsselung von PDF-Dokumenten;
- Verschlüsselung von ZIP-Dateien.

Hinweis: Verschlüsselungsmassnahmen auf Dokumentenebene stellen einen gewissen Schutz im Fall von Verwechslungen/Fehlleitungen dar. Das Passwort muss dabei über einen separaten Kanal (Telefon, sms) zugestellt werden. Gegen gezielte Angriffe sind diese Verschlüsselungen jedoch wirkungslos.

6.3 Anonymisierung:

Personendaten gelten dann als anonymisiert, wenn die Person nicht mehr bestimmbar ist. Unter «anonymisieren» versteht man jeglichen Vorgang, durch den die Zuordnung von Daten zu einer konkreten Person verhindert wird oder nur noch mit aussergewöhnlichem Aufwand möglich ist. Werden beispielsweise nur Initialen verwendet, kann häufig aufgrund des Kontextes auf die betroffene Person geschlossen werden. Bei der Anonymisierung muss also immer der Kontext beachtet werden.

6.4 Postversand:

Insbesondere für sehr sensible Daten zu empfehlen.

E-Learning

Der Kanton bietet über KOM SG ein E-Learning beispielsweise auch zum Thema Umgang mit E-Mail an. Bitte wenden Sie sich dafür an das Personalamt, POE: <https://www.sg.ch/politik-verwaltung/departemente-und-staatskanzlei/finanzdepartement/personalamt.html>



Nutzung von weiteren internetbasierten Kommunikationsdiensten¹¹

Die Ausführungen im Merkblatt gelten auch für die Nutzung von weiteren internetbasierten Kommunikationsdiensten wie sms, WhatsApp etc. Dabei ist zudem zu beachten, dass verschiedene Kommunikationsdienste weder schweizerischen noch europäischen Datenschutzstandards entsprechen und die Nachrichten entsprechend freizügig und im Widerspruch zu geltendem Schweizer Recht behandeln. Durch umfangreiche und schwer verständlichen Nutzer- und Datenschutzvereinbarungen werden durch die Anbieter häufig weitgehende Rechte herausbedungen. Das Niveau des tatsächlichen Schutzes bleibt letztlich vielfach intransparent.

Zu beachten ist auch, dass die Nutzung von Social Media bzw. Instant Messaging für die Übermittlung von Personendaten vermieden werden muss.

Für Fragen stehen Ihnen die folgenden Stellen gern zur Verfügung:

Kanton

Kantonale Fachstelle für Datenschutz, Tel 058 229 14 14

Gemeinden

<https://www.sg.ch/sicherheit/datenschutz/kontakt-weitere-datenschutzbehoerden/adressen-gemeindefachstellen.html>

Juli 2020

¹¹ WhatsApp, sms, etc.