



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la
protection des données et de la médiation APrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz
und Mediation ÖDSMB

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08

www.fr.ch/oedsmb

—

Ref: MS/al 2024-PrD-323

T. direkt: +41 26 305 59 73

E-Mail: secretariatatprdm@fr.ch

Freiburg, 3. September 2024

Merkblatt zur Kommunikation von Personendaten und besonders schützenswerten Personendate per E-Mail

I. Grundlagen

Die vorliegenden Weisungen werden gestützt auf die Beratungsbefugnis des Datenschutzbeauftragten erlassen (Art. 54 Abs. 1 Bst. d des Datenschutzgesetzes vom 12. Oktober 2023; nachfolgend: DSchG; RSF 17.1). Diese als Richtlinien zu betrachtenden Anweisungen sollen den zuständigen Stellen als Leitfaden dienen, wenn sie personenbezogene und besonders schützenswerte Personendaten per E-Mail weitergeben. Auch Gemeindebehörden können sich auf diese Anweisungen beziehen.

II. Allgemeines

Bevor öffentliche Organe Personendaten verarbeiten, müssen sie Folgendes berücksichtigen:

1. Personendaten werden definiert als alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 4 Abs. 1 lit. a DSchG).
2. Daten, die keine Personendaten sind, unterliegen keinen Beschränkungen im Sinne des DSchG (Art. 1 DSchG *e contrario*).
3. Das öffentliche Organ, das Personendaten verarbeitet, muss geeignete organisatorische und technische Maßnahmen gegen eine unbefugte Datenverarbeitung treffen (Art. 40 DSchG).
4. Das öffentliche Organ, das besonders schützenswerte Personendaten im Sinne von Art. 4 Abs. 1 lit. c DSchG verarbeitet, muss alle notwendigen Vorkehrungen treffen, um das erhöhte Risiko einer Beeinträchtigung, das mit der Verarbeitung solcher Daten einhergeht, zu verhindern (Art. 11 DSchG).

III. Die Weitergabe von Personendaten und Daten mit erhöhter Geheimhaltungspflicht

Die Vertraulichkeit und Integrität von Personendaten und besonders schützenswerten Personendaten muss bei der elektronischen Übermittlung gewährleistet sein (Art. 3 Abs. 1 und 17 Abs. 1 lit. a und b des Reglements über die Sicherheit von Personendaten vom 29. Juni 1999; im Folgenden: DZV; RSF 17.15).

IV. Die Weitergabe von besonders schützenswerten Personendaten

Es ist von entscheidender Bedeutung sicherzustellen, dass vertrauliche Informationen angemessen geschützt werden.

E-Mail gilt grundsätzlich nicht als sicheres Übertragungsmedium.

Besonders schützenswerte Personendaten und vertrauliche Informationen sollten daher nicht per E-Mail übermittelt werden. Falls dieser Kommunikationskanal trotzdem genutzt werden soll, sind die Vertraulichkeit und Integrität der übertragenen Daten und Dokumente zu gewährleisten.

Die Voraussetzungen für einen datenschutzkonforme Nutzung von E-Mail für besonders schützenswerte Personendaten Daten und vertrauliche Dokumente sind:

1. Sicherstellung der Identifikation der Kommunikationspartner (SenderIn und EmpfängerIn)
2. Nachweis der Identität des Absenders (proof of origin)
3. Sichere Transportverbindung
4. Verschlüsselung der Inhalte der E-Mail wie auch der Anhänge
5. Sicherstellung der Integrität der Daten und Dokumente
6. Klare Regelung zu Einsatz und Konfiguration von privaten Geräten (falls diese erlaubt sein sollen)

Für die konkrete Umsetzung dieser Anforderungen bestehen technische Möglichkeiten.¹

1. Sicherstellung der Identifikation der KommunikationspartnerInnen (SenderIn und EmpfängerIn)

Die internen Kommunikationspartner nutzen ihre persönliche ID (xxx.xxx@fr.ch) und ein, den Passwortrichtlinien entsprechendes, Passwort. Für externe Kommunikationspartner soll eine starke Authentifizierung eingesetzt werden. Bsp: SMS. Diese Massnahme hilft u.a. dabei, dass eine versehentlich an eine falsche Adresse gesendete E-Mail, vom Empfänger/von der Empfängerin nicht geöffnet werden kann.

2. Nachweis der Identität des Absenders oder der Absenderin

Die Vortäuschung eines vermeintlich vertrauenswürdigen AbsendersIn ist heute ein grosses Risiko (Fake-E-Mails). Für vertrauliche und sensible Inhalte und Anhänge ist es wichtig, den Absender oder die Absenderin eindeutig identifizieren zu können. Dies erfolgt i.d.R. über eine digitale Unterschrift des Absenders oder der Absenderin.

¹ Bsp: <https://www.bit.admin.ch/fr/swiss-government-pki-fr>; <https://www.bit.admin.ch/de/sg-pki-swiss-government-pki-trust-service-provider-tsp-d>

3. Sichere Transportverbindung

Die Transportverbindung muss als end-to-end-Verbindung verschlüsselt sein; d.h. von Client zu Client.

4. Verschlüsselung der Inhalte der E-Mail wie auch der Anhänge

Die vertraulichen Inhalte müssen verschlüsselt übertragen und abgelegt werden. Die reine Transportverschlüsselung ist nicht ausreichend, da die Mails beim Empfänger oder bei der Empfängerin wie SenderIn ansonsten unverschlüsselt abgelegt sind.

5. Sicherstellung der Integrität der Daten und Dokumente

Die vertraulichen und sensiblen Inhalte der Daten und Dokumente dürfen nicht verändert werden. Der Empfänger oder die Empfängerin muss nachprüfen können, dass er oder sie die Originaldaten erhält.

6. Klare Regelung zu Einsatz und Konfiguration von privaten Geräten (falls diese erlaubt sein sollen)

Es muss klar definiert sein, wie die geschäftlichen Mails inkl. ihrer Anhänge auf privaten Geräten gehandhabt werden dürfen. Insbesondere die Löschung der Daten und die Vermischung von privaten und geschäftlichen Daten bergen hohe Risiken für den Datenschutz und die Informationssicherheit.

Alternative Übertragungskanäle: Als Alternative zu E-Mail zum Austausch von vertraulichen Dokumenten und Daten können Portale eingesetzt werden, sofern diese die Sicherheitsanforderungen erfüllen.

V. Der Zugang zu Personendaten und besonders schützenswerten Personendaten (E-Mail weiterleiten)

Im Zusammenhang mit der Nutzung von E-Mail müssen sich die BenutzerInnen im Klaren sein, dass sie vertrauliche und sensible Daten bearbeiten und somit eine besondere Sorgfaltspflicht geboten ist. Das Weiterleiten an eigene private Mailadressen ist nicht erlaubt, ebenso das Weitersenden an Personen, die nicht autorisiert sind, um diese Daten zu bearbeiten.