Berufsgeheimnis und Mail-Verschlüsselung

Warum (angestellte und selbständig erwerbende) medizinische Fachpersonen[1] zwingend ihre E-Mails verschlüsseln sollten.

Baar, 17. August 2026

Artikel von Lukas Fässler, Rechtsanwalt & Informatikexperte, FSDZ Rechtsanwälte & Notariat AG, VR-Mitglied HIN AG

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Risiken beim Versand unverschlüsselter E-Mails

Die allgemeine **Risikosituation** bei der **Verwendung von E-Mails** ist mittlerweile allen hinlänglich bekannt. Die Kenntnisse über diese Risiken gehören heute schon zum fachlichen Grundwissen von Gesundheitsfachpersonen, welche mit Personendaten und insbesondere den besonders schützenswerten Personendaten[2] arbeiten und solche Informationen via E-Mail Dritten (Patientinnen, andere Gesundheitsfachpersonen, Spitäler, Apotheken, Behörden etc.) per elektronische Post (E-Mail Service) zustellen.

Die unverschlüsselte elektronische Post birgt erhebliche Gefahren in sich, da sie keinerlei Vertraulichkeit gewährleistet.

Absender- und Empfängerinformationen sowie der Inhalt der Nachricht werden im Klartext über das Internet transportiert. Dabei werden die E-Mails von Server zu Server geschickt und können mehrfach zwischengespeichert werden. Auf jedem dieser Server kann die Nachricht von einem Administrator oder Angreifer gelesen werden. Auch die Bedrohung durch Abgreifen des E-Mailverkehrs durch unbeteiligte Dritte (Spionage, Cyberkriminalität etc.) ist bekannt. Unter strengen Voraussetzungen nehmen staatliche Stellen zudem selber auch Überwachungen des E-Mail-Verkehrs zu Strafverfolgungszwecken vor.

Rechtsfolgen

Ein unangemessener Umgang mit E-Mailnachrichten, welche Personendaten oder besonders schützenswerte Personendaten oder gar Geschäfts- und Geheimnisdaten des Arbeitgebers (insgesamt als «Geheimnisdaten» bezeichnet) beinhalten, kann dazu führen, dass

- **Betriebs- und Geschäftsgeheimnisse** (wie Konzepte, Ideen, geistige Werke, Produktionsdaten etc.) offenbart werden. Die finanziellen Folgen und der Imageverlust bedrohen das betroffene Unternehmen in seiner Existenz und Fortbestand.

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

---

1 Art. 2 Abs. 1 EPDG
Diese Bestimmung definiert den Begriff der «Gesundheitsfachperson» als eine nach eidgenössischem oder kantonalem Recht anerkannte Fachperson, die Behandlungen im Gesundheitsbereich durchführt, anordnet oder Heilmittel sowie andere Produkte im Zusammenhang mit einer Behandlung abgibt. Dies ist grundlegend für den Fall, um festzustellen, auf welche Personen die spezifischen Pflichten zur IT-Sicherheit und Vertraulichkeit im Gesundheitswesen anwendbar sind.

2 Art. 5 lit. c DSG
Zu den besonders schützenswerten Personendaten gehören insbesondere alle Informationen über die Gesundheit und Intimsphäre (Daten über den körperlichen, geistigen oder seelischen Zustand) oder genetische Daten sowie eindeutig identifizierende biometrische Daten.

- Die **Verletzung von Geheimhaltungspflichten** und **Persönlichkeitsrechten** kann
    - **privatrechtlich** zu arbeitsrechtlichen Konsequenzen sowie Schadenersatz- und Genugtuungszahlungen,
    - **strafrechtlich** zu Busse oder Gefängnis und
    - **standesrechtlich** zu einschneidenden Disziplinarmassnahmen
    - **aufsichtsrechtlichen** Zusatzmassnahmen führen

Compliance und Governance – Verantwortung bis zu den einzelnen Mitarbeitenden

Es gehört zur rechtlichen Verantwortung der Geschäftsleitung und des Verwaltungsrates (Stiftungs- oder Spitalrates) einer Unternehmung (Spital, Arztpraxis, Apotheke etc.), die Anforderungen an die IT-Sicherheit zu kennen und die **notwendigen technischen und organisatorischen Massnahmen** festzulegen sowie deren Umsetzung periodisch zu überprüfen. Sie sind verantwortlich für Organisation und Kontrolle der Informationssicherheit.

Die **arbeitsrechtliche Sorgfaltspflicht** (nach Schweizer Recht geregelt in Art. 321e des Obligationenrechts, OR) verpflichtet Arbeitnehmende, die zugewiesene Arbeit gewissenhaft auszuführen, die Interessen der Arbeitgebenden zu wahren und Maschinen, Materialien sowie Arbeitsgeräte fachgerecht zu bedienen und zu schützen. Die Mitarbeitenden haben somit trotz allenfalls versäumter Weisungen der Arbeitgebenden in Bezug auf die Kommunikation mit anvertrauten Patientendaten die ihnen übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen der Arbeitgebenden in guten Treuen zu wahren. Dazu zählt auf jeden Fall auch die Sorgfalt beim Einsatz von E-Mails.

Wir haben also eine durchgängige Kaskade aller an der Bearbeitung von Personendaten und besonders schützenswerten Personendaten Beteiligten zur Kenntnis zu nehmen. **Jede Person ist und bleibt für ihren Tätigkeitsbereich und damit auch für die Nutzung, den Einsatz und die Weiterleitung von E-Mails verantwortlich.**

Technische Herausforderungen – einfache Handhabung

Niemand von uns will sich in der Verrichtung der täglichen Arbeiten (so auch beim Einsatz von E-Mails) jedes Mal die Frage stellen müssen, verletze ich jetzt damit die Rechte von Betroffenen. Daher ist ein pragmatischer Ansatz der richtige. **Er sieht den generellen Einsatz von Verschlüsselungs-Technik für jeden E-Mail-Benutzer standardmässig vor**. Dadurch muss der Mitarbeitende nicht mehr in jedem Einzelfall mühsam entscheiden, ob er jetzt verschlüsselt oder nicht.

Dafür sind einfach anwendbare Services gefordert, wie sie HIN anbietet. HIN verschlüsselt E-Mails an HIN Mitglieder sowie an Personen, die nicht HIN Mitglied sind (Patientinnen, Partner im In- und Ausland), so dass sie von Dritten weder eingesehen noch verändert werden können. HIN Mitglieder wahren mit verschlüsselten E-Mails den Datenschutz und das Berufsgeheimnis sowie sämtliche Geheimhaltungspflichten. **Für die Nutzung von HIN Mail benötigen Sie als Gesundheitsfachperson eine** HIN Mitgliedschaft. Ihre Patientinnen oder Kunden können jedoch ohne HIN Mitgliedschaft direkt vom Verschlüsselungsservice ohne (finanziellen oder technischen) Zusatzaufwand profitieren.

Die rechtliche Pflicht zur Verschlüsselung von E-Mails

Der unverschlüsselte E-Mail-Versand mit Personendaten oder Geheimnisdaten kann einen Verstoss gegen die Verpflichtung zur vertraulichen Behandlung von personenbezogenen oder dem Geschäftsgeheimnis unterstellten Informationen darstellen. Diese Verpflichtung ergibt sich aus vertraglichen Vereinbarungen (z.B. Anstellungsvertrag) und aus gesetzlichen Vorschriften (z.B. Datenschutzgesetzgebung).

a) Vertragliche Vereinbarungen

Bei Geschäftsbeziehungen, die von einem besonderen Vertrauensverhältnis geprägt sind (wie bei Gesundheitsfachpersonen, Apothekerinnen, Anwälten, Treuhänderinnen etc.) ist eine Geheimhaltungspflicht stillschweigend, d.h. ohne schriftliche oder mündliche Abmachung, zu beachten. Der im Auftragsverhältnis tätige beratende Person hat nach Art. 398 OR eine Reihe von Treuepflichten gegenüber der auftraggebende Person (Patientin oder Klient). Dazu zählen insbesondere die **Diskretions- und Geheimhaltungspflichten.** Bereits die fahrlässige Nichtbeachtung der Vertraulichkeit stellt im Auftragsverhältnis eine Vertragsverletzung dar. Die Verletzung vertraglicher Geheimhaltungspflichten hat je nach Ausgestaltung des Vertrages unterschiedliche Rechtsfolgen. Im Vordergrund stehen Schadenersatzverpflichtungen, Konventionalstrafen und die Auflösung des Vertragsverhältnisses.

b) Gesetzliche Pflichten

Der Schutz der Privat- und Geheimsphäre wird in Art. 13 der Bundesverfassung geregelt. Er hält fest, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs und Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat.

Dieser Schutzanspruch wird auf Gesetzesstufe mehrfach konkretisiert.

- Gemäss Art. 28 ff. ZGB kann eine Person, die in ihrer Persönlichkeit widerrechtlich verletzt wird, gegen jede und jeden, der an der Verletzung mitwirkt, das Gericht anrufen. Der **verfassungsmässig garantierte Schutz der Persönlichkeit** ist bei unverschlüsselten, personenbezogenen E-Mails nicht gewährleistet.
- Weiter kann die im Obligationenrecht (OR) verankerte auftrags- und arbeitsrechtliche **Treuepflicht zur Verschwiegenheit** verpflichten.
- Bei Berufsgeheimnisträger wie Ärzteinnen, anderen Gesundheitsfachpersonen jeder Ausprägung, Rechtsanwälten, Apothekerinnen etc. spielt das **Vertrauensverhältnis** in der Geschäftsbeziehung eine übergeordnete Rolle. Deshalb werden sie **gesetzlich unter Strafandrohung zur Geheimhaltung verpflichtet**.
    - Das **Strafgesetzbuch (StGB)** kennt eine ganze Reihe von Geheimschutzregeln, welche entsprechende Massnahmen zur Sicherstellung der Vertraulichkeit von Informationen fordern
        - das **Amtsgeheimnis** (Art. 320 StGB),
        - die bereits angesprochenen **Berufsgeheimnisse** (Art. 321 und Art. 321bis StGB),
        - **Fabrikations- und Geschäftsgeheimnisse** (Art. 162 und Art. 273 StGB) sowie
        - die Pflicht zur **Wahrung politischer und militärischer Geheimnisse** (Art. 267, Art. 272 und Art. 274 StGB).
    - Im neuen, seit 1.9.2023 in Kraft stehenden Datenschutzgesetz des Bundes sowie jener der Kantone wird die **Verletzung der beruflichen Schweigepflicht** (Art. 35 DSG) zusätzlich besonders geregelt und geahndet. Die Art. 61 ff. DSG (Bund) sehen
        - bei **vorsätzlicher Verletzung von Sorgfaltspflichten** sowie
        - bei **vorsätzlicher Verletzung der beruflichen Schweigepflicht**

      hohe Geldbussen bis CHF 250´000 vor. Dabei ist zu beachten, dass ein Eventualvorsatz genügt[3].

[3] Eventualvorsatz liegt vor, wenn eine Person eine Tat oder einen Schaden für möglich hält und diesen billigend in Kauf nimmt. Der Täter will den Erfolg zwar nicht direkt, findet sich aber mit ihm ab, falls er passiert.

Wer es im medizinische Fachbereich in der heutigen Zeit in Kauf nimmt, dass die von der eigenen Person oder von Mitarbeitenden bearbeiteten Personendaten oder besonders schützenswerten Personendaten unverschlüsselt an Dritte per Mail-Services weitergegeben werden, handelt eventualvorsätzlich.

- Zudem kommen **besondere Bestimmungen** in Bezug auf die **IT-Sicherheit und Vertraulichkeit** zum Tragen, insbesondere in den Arztpraxen, den Spitälern oder den Apotheken. Bestimmung dazu finden sich im Datenschutzrecht.
  - **Art. 8 Abs. 1 und 2 DSG**: Die verantwortliche Person und die auftragsbearbeitende Person sind verpflichtet, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten, um Verletzungen der Datensicherheit zu vermeiden. Dies betrifft direkt die Anforderungen an die IT-Sicherheit im Gesundheitswesen.
  - **Art. 30 Abs. 2 DSG**: Hier wird festgelegt, dass eine Persönlichkeitsverletzung insbesondere dann vorliegt, wenn Personendaten entgegen den Grundsätzen der Datensicherheit bearbeitet werden oder wenn besonders schützenswerte Personendaten (wie Gesundheitsdaten) unbefugt Dritten bekanntgegeben werden.
  - **Art. 2 Abs. 1 DSV**: Die Verordnung konkretisiert die Ziele der technischen und organisatorischen Massnahmen. Diese müssen sicherstellen, dass Daten ihrem Schutzbedarf entsprechend vertraulich (nur Berechtigten zugänglich), verfügbar, integer (nicht unberechtigt verändert) und nachvollziehbar bearbeitet werden.
  - **Art. 3 Abs. 1 DSV**: Diese Bestimmung präzisiert die Massnahmen zur Gewährleistung der Vertraulichkeit. Sie fordert spezifische Kontrollen: die Zugriffskontrolle (nur notwendige Daten für berechtigte Personen), die Zugangskontrolle (physischer Zugang zu Anlagen) und die Benutzerkontrolle (Verhinderung unbefugter Nutzung von IT-Systemen).
  - **Gesundheitsgesetz**: Gemäss § 16 Abs. 1 sind Personen im Gesundheitswesen sowie ihre Hilfspersonen über Geheimnisse und Wahrnehmungen aus ihrer Tätigkeit zu schweigen (Berufsgeheimnis). § 16 Abs. 2 regelt die Ausnahmen (z. B. Einwilligung des Patienten), während § 17 spezifische Meldepflichten und -rechte (z. B. bei erheblicher Gefährdung der Bevölkerung) definiert, die das Berufsgeheimnis durchbrechen können.
  - **Gesetz zur Erhaltung und Förderung der Gesundheit**: Art. 47 verpflichtet Gesundheitsfachpersonen und Mitarbeitende von Gesundheitsinstitutionen zur Verschwiegenheit über Tatsachen, die ihnen in ihrer beruflichen Stellung anvertraut wurden. Art. 47 Abs. 2 und 3 regeln die Befreiung vom Berufsgeheimnis, einschliesslich der Vermutung einer Einwilligung für medizinisch notwendige Auskünfte an beteiligte Gesundheitsfachpersonen.
  - **Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen**: Die Bestimmungen fordern in Art. 17, dass Personendaten durch angemessene organisatorische und technische Massnahmen gesichert werden müssen, wobei sich die Angemessenheit nach dem Stand der Technik und dem Risiko einer Persönlichkeitsverletzung richtet. Art. 14 Abs. 2 schränkt die Bearbeitung besonders schützenswerter Personendaten auf gesetzliche Grundlagen, die Erfüllung klar umschriebener Aufgaben oder

die ausdrückliche Einwilligung ein. Art. 19 fordert zudem Datensparsamkeit sowie die Nutzung von Anonymisierung und Pseudonymisierung.

- **Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen**: § 4 konkretisiert die technischen Massnahmen bei elektronischer Bearbeitung, darunter Zugangskontrolle, Datenträgerkontrolle, Transportkontrolle, Bekanntgabekontrolle, Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle sowie Eingabekontrolle und Wiederherstellung. § 7 definiert besonders schützenswerte Personendaten (inkl. Gesundheits- und genetischer Daten), und § 6c definiert Verletzungen der Datensicherheit als solche, die zum unbefugten Zugang führen.

- **Kantonale administrative Massnahmen der Gesundheitsbehörden** wie temporärer oder permanenter **Entzug der Betriebsbewilligung** (vgl. dazu den Fall Genf unter Gerichte A/2899/2015 / ATA 967/2016- Kanton GE; https://entscheidsuche.ch/docs/GE_Gerichte//GE_CJ_013_A-2899-2015_2016-11-15.pdf)

Zusammenfassung

Die rechtlichen Anforderungen an Gesundheitsfachpersonen ergeben sich aus einem Zusammenspiel von allgemeinem Datenschutzrecht, berufsrechtlichen Schweigepflichten und spezifischen technischen Vorgaben.

→ Wenn die Person als **Gesundheitsfachperson** im Sinne von Art. 2 Abs. 1 EPDG tätig ist: Gilt eine **kumulative Verpflichtung** aus dem allgemeinen Datenschutzrecht (DSG), dem Berufsgeheimnis (kantonal/bundesweit) und – sofern anwendbar – spezifischen kantonalen Gesundheitsgesetzen.

→ Wenn die **Datenbearbeitung elektronisch erfolgt**: müssen **zwingend technische und organisatorische Massnahmen (TOM) implementiert** werden, die über allgemeine Sorgfaltspflichten hinausgehen und spezifische Kontrollen (Zugriff, Zugang, Benutzende) umfassen.

Unverschlüsselten E-Mail-Nachrichten fehlt es an der Vertraulichkeit. Ein unverschlüsselter E-Mail-Versand wird dem jeweils vorliegenden besonderen Vertrauensverhältnis und den Geheimhaltungspflichten **von Personen, die dem Berufsgeheimnis unterstehen**, nicht gerecht. Der unverschlüsselte E-Mail-Versand von personenbezogenen Informationen kann zudem die Persönlichkeitsrechte der betroffenen Personen und Unternehmungen verletzen. Das Gesetz verlangt angemessene technische und organisatorische Massnahmen zur Datensicherheit.

Auf der Basis der heute bestehenden Verschlüsselungsverfahren können die Kommunikationsteilnehmende ihre Mitteilungen einfach und zuverlässig verschlüsseln, womit das Einsehen der E-Mails auf dem Weg zum Empfänger verunmöglicht wird.

Die Verschlüsselung sensibler E-Mail-Nachrichten gewährleistet Vertraulichkeit und Integrität der übermittelten Informationen**. Für Personen, die dem Berufsgeheimnis unterstehen, sowie für alle, die sensible E-Mails versenden, ist der Einsatz geeigneter Verschlüsselungslösungen unerlässlich**. Andernfalls drohen Schadenersatzforderungen, Bussen, Gefängnis, Disziplinarstrafen und Reputationsverlust.

Es ist so einfach, als Gesundheitsfachperson gesetzeskonforme Nachrichten zu versenden. Anstatt alles selber sicherzustellen, bietet der HIN Mail Service (https://www.hin.ch/de/index.cfm) **die integrierte Lösung für alle diese Anforderungen.**