Richtlinie über die Klassifizierung und den Schutz der Dokumente in der Gemeindeverwaltung der Stadt Freiburg (vom 23. September 2025)

Der Gemeinderat der Stadt Freiburg

gestützt auf:

- das Gesetz über den Datenschutz (DSchG; SGF 17.1);
- das Reglement über die Sicherheit der Personendaten (DSR; SGF 17.15);
- die Verordnung über die Informationssicherheit (ISV; SGF 17.15),

erlässt folgende Bestimmungen:

Erläuterungen

Die Stadt Freiburg bearbeitet ein grosses Volumen an Dokumenten, die Informationen aller Art enthalten, darunter auch besonders schützenswerte Personendaten (Bürger:innen, Gemeindepersonal, Verträge, Sozial- und Gesundheitsdaten). Kraft kantonaler Datenschutzgesetzgebung muss sie im Rahmen ihres öffentlichen Auftrags die Sicherheit dieser Informationen gewährleisten.

Diese Richtlinie legt ein Klassierungssystem für Dokumente fest, das für alle Mitarbeitenden und Partner der Stadt gilt. Sie ist eine Säule der Governance der Informationssicherheit und Teil der internen Dokumentenmanagementpolitik.

Erstes Kapitel: Allgemeine Bestimmungen

Geltungsbereich

Art. 1 Diese Richtlinie gilt für alle Dokumente, unabhängig von ihrem Format (Papier, digital, DMS, E-Mail) und für alle Mitarbeitenden, für die Mitglieder des Gemeinderats sowie für die Leistungserbringer und

Partner, die Zugriff auf das Informationssystem der Stadt haben.

Zweck

Art. 2 Diese Richtlinie bezweckt:

a) die Einführung einer klaren und einheitlichen Klassifizierungs- und Datenschutzstrategie für die Dokumente der Stadt Freiburg;
b) die Gewährleistung der Vertraulichkeit, der Integrität und der Verfügbarkeit der Informationen;
c) die Erfüllung der gesetzlichen Vorgaben des Kantons;
d) die Reduktion der Gefahr von Datenlecks, des unbefugten Zugriffs und des Kontrollverlusts;
e) die Stärkung des Vertrauens der Bürgerinnen und Bürger in Bezug auf den Datenschutz.

Klassifizierung der Dokumente und obligatorische Sicherheitsmassnahmen

Art. 3 [1] Die Klassifizierung der Dokumente wird gemäss Anhang festgelegt, der ein fester Bestandteil dieser Richtlinie ist.

[2] Folgende Sicherheitsmassnahmen sind obligatorisch:

- systematische Verschlüsselung schützenswerter Daten (C3);
- strenge Zugangskontrolle gestützt auf das Prinzip der geringsten Privilegien (Least Privilege Principle);
- starke Authentifizierung (MFA) für jeglichen Zugriff auf kritische Systeme;
- ins DMS und in den E-Mail-Dienst integrierte Verhinderung von Datenverlust (DLP);
- regelmässiges Logging und Audit, um die Rückverfolgbarkeit sicherzustellen;
- sichere Backups und regelmässige Wiederherstellungstests;

- Verwaltung des externen Zugangs (Leistungserbringer, gemeindeübergreifende Partner) mit eigenen Vertragsklauseln.

Bearbeitung der Personendaten

Art. 4 [1] Personendaten sind gemäss den rechtlichen Vorgaben zu bearbeiten.

[2] Bei der Bearbeitung von Personendaten und besonders schützenswerten Daten müssen die Sicherheitsziele der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Rückverfolgbarkeit gewährleistet sein.

Governance und Verantwortung

Art. 5 [1] Die bzw. der Sicherheitsbeauftragte stellt die Umsetzung der Richtlinie sicher, überwacht die Audits und kümmert sich um die Sicherheitsvorfälle.

[2] Die Fachverantwortlichen weisen den erstellten oder erhaltenen Dokumenten die richtige Klassifizierung zu.

[3] Die Mitarbeitenden wenden die Klassifizierungsregeln an und melden jede Abweichung.

Lebenszyklus und Änderungsmanagement

Art. 6 [1] Die Zuweisung der Stufe geschieht automatisch oder manuell bei der Erstellung oder beim Import des Dokuments.

[2] Die Klassifizierung bleibt über den gesamten Lebenszyklus erhalten (Abfrage, Änderung, Archivierung).

[3] Die Neuklassifizierung eines Dokuments ist möglich, wenn sich der Inhalt weiterentwickelt (z. B. von Stufe C1 auf C3).

[4] Stufenänderungen müssen von der für das Dokument verantwortlichen Person und von der bzw. dem Sicherheitsbeauftragten genehmigt werden.

[5] Die Rückverfolgbarkeit ist durch das Logging sicherzustellen.

Konkrete Anwendung

Art. 7 [1] Das Klassifizierungsmodell ist mit einem automatischen Schutz für den ganzen Lebenszyklus ins DMS integriert.

[2] Ein nicht erlaubter Versand wird im E-Mail-Dienst blockiert und ein automatischer Schutz wird eingeführt.

[3] Die Berechtigungen der Dokumentenflüsse werden ohne Auswirkung auf die Effizienz der Dienststellen kontrolliert.

Schulung und Sensibilisierung

Art. 8 [1] Für alle Mitarbeitenden wird eine obligatorische Einführung in die Klassifizierung der Dokumente eingeführt.

[2] Jedes Jahr werden Auffrischungskurse organisiert.

[3] Bei Änderungen des Rechtsrahmens werden zusätzliche Auffrischungskurse organisiert.

[4] Es werden Sensibilisierungskampagnen (Workshops, E-Learnings, Phishingtests) organisiert.

Inkrafttreten

Art. 9 Diese Richtlinie tritt mit ihrer Genehmigung durch den Gemeinderat in Kraft.

Verabschiedet vom Gemeinderat am 23. September 2025

Im Namen des Gemeinderats der Stadt Freiburg

Der Stadtammann: Der Stadtschreiber:

Thierry Steiert David Stulz