Digital
Stadt Bern

# Konzept zur Klassifizierung von elektronischen Daten in der Stadtverwaltung Bern

(Klassifizierungskonzept)

**Stadt Bern**, Präsidialdirektion, Personal, Finanzen & Digitale Entwicklung, Junkerngasse 47, 3011 Bern, bern.ch/digital

**Herausgeberin:** Konferenz Digital Stadt Bern (KDSB) ● **Bern, 15. September 2023**

# Inhalt

# 1 Einleitung

## 1.1 Allgemeines

Das Konzept zur Klassifizierung von elektronischen Daten in der Stadtverwaltung Bern *Klassifizierungskonzept* legt den Rahmen für die Klassifizierung von elektronischen Daten in der Stadtverwaltung Bern fest.

Das Klassifizierungskonzept dient den Direktionen und Verwaltungseinheiten als Orientierungshilfe im Umgang mit elektronischen Daten hinsichtlich der rechtlichen Anforderungen, des Wertes, der Kritikalität und der Empfindlichkeit gegenüber Offenlegung oder Änderung. Insbesondere beim Schutz von vertrauenswürdigen Daten vor unbefugten Zugriff muss die Klassifizierung klar geregelt sein, auf lesbaren Dokumenten deutlich sichtbar und maschinenlesbar angegeben werden, damit der nötige Zugriffsschutz bei digitalen Systemen sinnvoll und sicher umgesetzt werden kann.

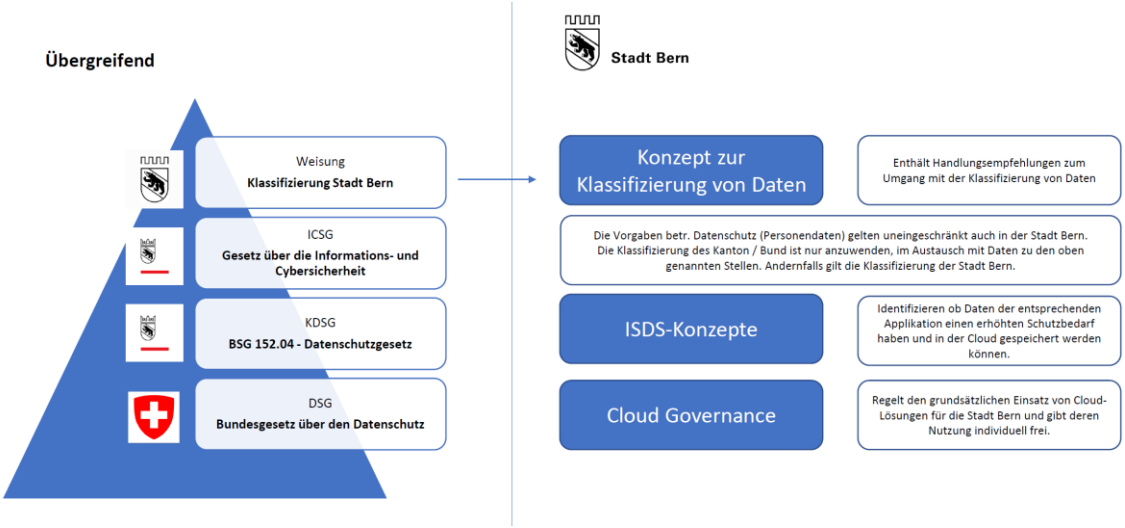


***Abbildung**: Einbettung des Konzeptes zur Klassifizierung von elektronischen Daten*

Bis heute gibt es keine Vorschriften zur Klassifizierung von Daten und Dokumenten in der Stadtverwaltung Bern. Mit der *Cloudstrategie* der Stadt Bern auf Basis einer hybriden Informatik werden die Anforderungen zum Schutz des Amts- und Berufsgeheimnisses beim Speichern und Bearbeiten von Daten auf (ausländischen) Cloud-Infrastrukturen noch relevanter. Das Klassifizierungskonzept hilft diese Lücke zu schliessen und enthält Handlungsempfehlungen zur systematischen Nachbesserung der fehlenden Klassifizierung.

Die *Cloud Governance*, welche die Restrisiken bei Nutzung einer Cloudlösung regelt, ist nicht Bestandteil der Klassifizierungsweisung, Jedoch bildet die Klassifizierungsweisung die Grundlage für die Nutzung von (ausländischen) Cloudlösungen.

Die kantonalen und städtischen Datenschutzbestimmungen sind bei der Bearbeitung von schützenswerten Personendaten in jedem Fall zu berücksichtigen.

Die Abteilungsleitungen[1] oder die von Ihnen bestimmten Personen sind als Dateneigner*innen für die korrekte Klassifizierung unter Berücksichtigung des Berufs- und Amtsgeheimnisses verantwortlich. Für zentral genutzte Infrastrukturen wie z.B. SAP oder Microsoft 365 erfolgt die technische Klassifizierung inkl. der dazu notwendigen Schutzstufen im Auftrag der Konferenz Digital Stadt Bern (KDSB) zentral durch die ICT Security der Informatikdienste.

In der Umsetzung werden zentral verschiedene Schulungsformate und -unterlagen angeboten (Einführungskurs in die Klassifizierung, Refresherkurse, Self-Learning usw.). Diese richten sich gleichermassen an Vorgesetzte, Projektmitarbeitende und Mitarbeitende. Die Sensibilisierung und Ausbildung der Mitarbeitenden soll künftig integraler Bestandteil des Onboardings sein.

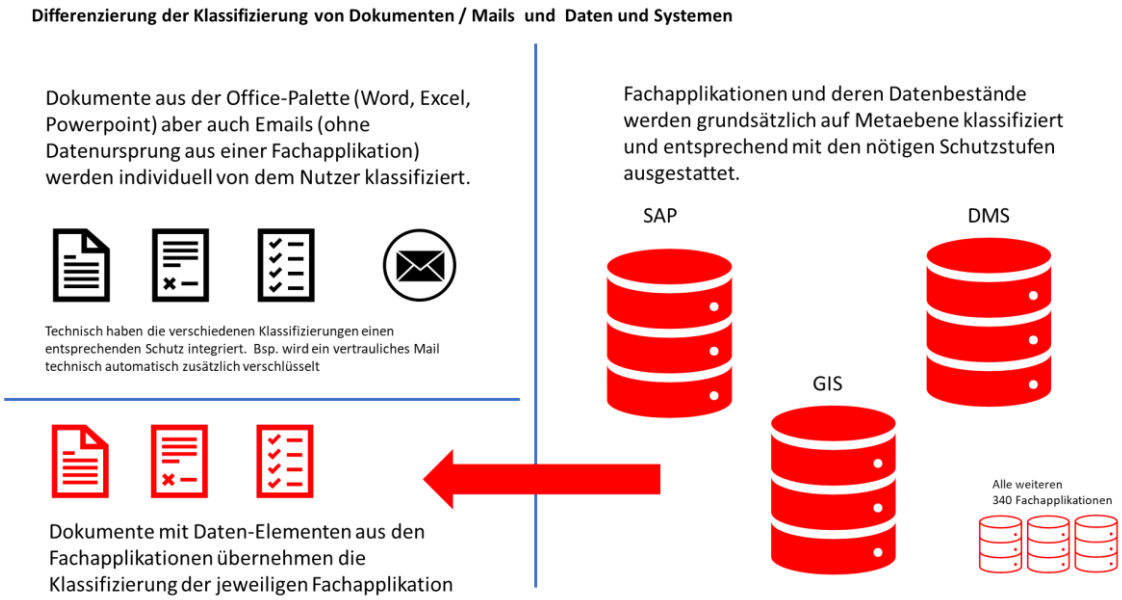


***Abbildung**: Differenzierung der Klassifizierung bei Dokumenten und Systemen*

Im Kanton Bern gilt das Öffentlichkeitsprinzip. Nach Artikel 17 Absatz 3 der Kantonsverfassung (BSG 101.1) und die Artikel 27ff des Informationsgesetzes (BSG 107.1) hat jede Person ein Recht auf Einsicht in amtliche Akten, soweit keine überwiegenden öffentlichen oder privaten Schutzinteressen bestehen. **Die vorliegende Weisung regelt nicht das Recht zur Akteneinsicht. Diese wird in jedem Falle von Juristinnen und Juristen der Stadtverwaltung beurteilt.** Eine systematische Klassifizierung und die fachlich korrekte Handhabung, Kennzeichnung und Aufbewahrung hilft aber auch bei der Beurteilung der inhaltlichen Kriterien für eine mögliche Akteneinsicht.

[1] Abteilungsleiter*innen und Werkdirektor*innen gemäss Personalreglement der Stadt Bern.

Zahlreiche gesetzliche Regelungen schränken den Umgang mit Daten ein, welche an die Stadtverwaltung geliefert oder intern generiert werden. Falls unberechtigte Personen klassifizierte (interne, vertrauliche oder geheime) Informationen lesen, verändern, bearbeiten oder entwenden, kann für die Stadt Bern ein finanzieller Schaden oder ein Imageverlust entstehen.

## 1.2 Zuständigkeiten

Die Abteilungsleitungen sind für die Klassifizierung ihrer Daten verantwortlich. D.h. sie haben die **Datenhoheit** inne. Sie können ergänzende, konkretisierende Regelungen veranlassen, jedoch immer unter Einhaltung der übergeordneten Bestimmungen. Sie sind verantwortlich, dass die Erbringenden von ICT-Leistungen (Informatikdienste, GIS-Kompetenzzentrum und externe Liefernde) die nötigen technischen Massnahmen entsprechend der Klassifizierung treffen können. Neben der systematisch und klar erkennbar vorgenommen Klassifizierung gehören hierzu auch Information, Dokumentation, Controlling und betriebliche Bildung auf Ebene der Mitarbeitenden. Insgesamt gilt es die *Corporate Governance* um das *Datenmanagement* zu erweitern und eine *neue Datenkultur* zu leben.

Die Abteilungsleitungen sind als Dateneigner*innen verantwortlich für die **Umsetzung des Datenkonzepts**. Dies gilt namentlich für den mit der Klassifizierungsweisung verbindlich geregelten Bereich der Vertraulichkeit. Sie legen die Klassifizierung der Vertraulichkeit für alle von Ihnen verantworteten Datensätze fest.

Die **Umsetzung** erfolgt stadtweit im Rahmen der Einführung der *Neuen digitalen Zusammenarbeit* mit Microsoft 365 | Teams, SAP Hana und bei den rund 300 Fachapplikationen im Rahmen von Ersatzanschaffungen auf Basis des städtischen Datenmanagementsystems (DMS). Die Umsetzung der Klassifizierung soll einhergehen mit der schrittweisen Harmonisierung aller Datensätze nach dem Prinzip von *OnceOnly*. Damit wird die performante Datengrundlage u.a. als Voraussetzung für das künftige Bevölkerungsportal geschaffen.

## 1.3 Weisung über die Klassifizierung von elektronischen Daten

Die von der Konferenz Digital Stadt Bern am 3. März 2023 erlassene Klassifizierungsweisung legt fest, wie elektronische Daten hinsichtlich ihrer *Vertraulichkeit* zu klassifizieren sind und wie mit entsprechend klassifizierten elektronischen Daten umzugehen ist. Sie dient damit dem Schutz von elektronischen Daten und bietet Gewähr dafür, dass nur berechtigte Personen und Systeme Zugriff auf diese haben. Die im Klassifizierungskonzept ebenfalls behandelten Themenfelder der *Datenintegrität* und der *Datenverfügbarkeit* sind nicht Gegenstand der Klassifizierungsweisung.

## 1.4 Definition Daten

Als elektronische Daten im Sinne der Klassifizierungsweisung gelten alle Daten der Stadtverwaltung Bern, die auf elektronischen (z.B. Memory Stick), digitalen (z.B. Cloud) oder anderen Sicherungsmedien gespeichert sind. Dazu gehören sowohl strukturiert erfasste Daten (z.B. html, Excel, Datenbanken) als auch technisch unstrukturierter Inhalt in Dokumenten (z.B. Word, PDF). Ebenso gehören Daten auf allen Arten von Datenträgern und Speichermedien, Daten in Fachapplikationen und an technischen Schnittstellen zur Verfügung gestellte Daten dazu. Im Folgenden wird nur der Begriff (elektronische) *Daten* benutzt, mitgemeint sind dabei alle Formen von gespeicherten elektronischen Informationen (als Dokumente, Unterlagen und Informationen). Nicht dazu gehören Daten in Papierform.[2]

## 1.5 Umsetzungsplanung

Die Klassifizierungsweisung tritt per 15. August 2023 in Kraft und sieht sehr lange Umsetzungsfristen vor, damit sich die Dienststellen fundiert mit der Datenhaltung, -bearbeitung und -steuerung auseinandersetzen können.

1. Die inhaltliche und technische Umsetzung im Bereich der Bürokommunikation erfolgt mit der Einführung von Microsoft 365 | Teams und im Bereich der Ressourcensteuerung mit SAP HANA spätestens bis 31. Dezember 2024.

   Die Operationalisierung erfolgt stadtweit im Rahmen der Einführung der *Neuen digitalen Zusammenarbeit NDZ*, welche namentlich auch Schulungen zu Datenmanagement und Governancefragen für Vorgesetzte umfasst.

2. Für alle übrigen Daten erfolgt die Klassifizierung auf Metaebene spätestens bis *31. Dezember 2025*.[3]

3. Die technische Umsetzung in den Fachapplikationen erfolgt grundsätzlich auf Basis des städtischen Datenmanagementsystems DMS im Rahmen von Ersatzbeschaffungen (*Life Cycle Management*) spätestens bis 31. Dezember 2028.

   Die Operationalisierung erfolgt bei den rund 300 Fachapplikationen im Rahmen von Ersatzanschaffungen und auf Basis der Grundlagen für das neu von den Informatikdiensten beschaffte städtische Datenmanagementsystems DMS. Die Umsetzung der Klassifizierung soll einhergehen mit der schrittweisen Harmonisierung aller Datensätze nach dem Prinzip von *OnceOnly*.

Bei der Datenharmonisierung und der Klassifizierung bei Fachapplikationen sollen die Dienststellen durch das *Fachorgan Daten* der Konferenz Digital Stadt Bern (KDSB) und durch ein eigens dafür lanciertes städtisches Projekt *Data Excellence* unterstützt werden.

[2] Es besteht keine generelle städtische Weisung für die Klassifizierung von Papierakten.

[3] Anhand des Dateninventars.

# 2 Ziele und Gültigkeit

## 2.1 Klassifizierungskonzept

Der Zweck des Klassifizierungskonzept ist die Festlegung der Prinzipien und Grundregeln für die Klassifizierung von elektronischen Daten der Stadtverwaltung Bern, so dass die elektronischen Daten auf einem angemessenen Niveau geschützt und nur den dafür vorgesehenen Personen und Systemen zugänglich gemacht werden.

Die in diesem Konzept festgelegten Regelungen bieten die Grundlage, damit Vorgaben der Stadt und des Kantons Bern im Umgang mit Daten in der Stadtverwaltung korrekt umgesetzt werden. Sie umfassen dabei Klassifizierungsstufen in den Bereichen Vertraulichkeit, Integrität und Verfügbarkeit der Daten:

- **Vertraulichkeit**: Darunter versteht man, dass Daten nur von den Personen verändert oder eingesehen werden dürfen, die dazu auch berechtigt sind.

- **Integrität:** Unter der Integrität von Daten versteht man die Nachvollziehbarkeit von vorgenommenen Änderungen an diesen.

- **Verfügbarkeit**: Die gespeicherten Daten müssen in einem grösstmöglichen zeitlichen Rahmen verfügbar sein, wenn die nutzenden Personen Zugriff darauf benötigen.

## 2.2 Klassifizierungsweisung: Klassifizierung der Vertraulichkeit

Die Weisung über die Klassifizierung von elektronischen Daten (Klassifizierungsweisung) legt verbindlich fest, wie elektronische Daten hinsichtlich **Vertraulichkeit** zu klassifizieren sind und wie mit den entsprechend klassifizierten elektronischen Daten umzugehen ist. Sie dient damit dem Schutz von elektronischen Daten und bietet Gewähr dafür, dass nur berechtigte Personen und Systeme Zugriff auf diese haben:

- Die Vertraulichkeitsklassifizierung von Daten ist für alle Mitarbeitenden der Stadtverwaltung – und wo durch die Mitarbeit in Projekten, Arbeitsgruppen oder Kommissionen – auch externe Partner der Stadt Bern verbindlich. Sie richtet sich ebenso an alle Liefernde, an externe Dienstleistende und Partnerunternehmen der Stadt Bern (im Umgang mit städtischen Daten). Externe Mitarbeitende müssen explizit im Rahmen der Vertraulichkeitserklärungen (Beilagen zu Verträgen) die Klassifizierungsweisung akzeptieren.

- Die Klassifizierungsweisung gilt für alle Arbeiten mit elektronischen Daten der Stadtverwaltung (siehe 1.3 *Definition elektronische Daten*).

- Die Klassifizierungsweisung betrifft nicht den Bereich der Papierdaten/Akten (siehe 1.3 *Definition elektronische Daten*).
- Für die Klassifizierung von Geodaten bestehen weiterführende Bestimmungen.
- Die Klassifizierungsrichtline wird regelmässig auf ihre Aktualität und Wirksamkeit geprüft. Die Konferenz Digital Stadt Bern (KDSB) ist für das Controlling verantwortlich.

## 2.3 Ausführungsbestimmungen

Die Konferenz Digital Stadt Bern (KDSB) regelt gestützt auf:

- Anhang I Ziffer 5 der Verordnung vom 29. November 2000 über die Kommissionen des Gemeinderats (Kommissionenverordnung; KoV; SSSB 152.211);
- die Verordnung vom 29. März 2000 betreffend die Information der Öffentlichkeit über städtische Belange (Informationsverordnung; InfV; SSSB 107.1);
- den Gemeinderatsbeschluss Nr. 2021-1098 vom 15. September 2021 zu Strategie Sourcing und Cloud Computing 2022 (Cloudstrategie),

die Ausführungsbestimmungen in Richtlinien, Weisungen und Konzepten.

Sie kann den Erlass technischer und organisatorischer Ausführungsbestimmungen wie Standards, Sicherheitsanforderungen und Prozesse an ein Fachorgan der Stadt Bern delegieren. Weiter bestimmt sie die Übergangsfristen, innerhalb derer die von diesem Konzept und seinen Ausführungsbestimmungen vorgesehenen Massnahmen erstmals ergriffen werden müssen.

# 3 Rahmenbedingungen

## 3.1 Gesetzliche Grundlagen

- Öffentlichkeitsprinzip Kanton Bern: Artikel 17 Absatz 3 der Verfassung des Kantons Bern vom 06. Juni 1993 (KV; BSG 101.1) besagt, dass jede Person ein Recht auf Einsicht in sämtliche Akten hat, soweit keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen.
- Gesetz vom 02. November 1993 über die Information der Bevölkerung (Informationsgesetz; IG; BSG 107.1).
- Verordnung vom 26. Oktober 1994 über die Information der Bevölkerung (Informationsverordnung; IV; BSG 107.111).
- Verordnung vom 29. März 2000 betreffend die Information der Öffentlichkeit über städtische Belange (Informationsverordnung; InfV; SSSB Nr. 107.1).
- Datenschutzgesetz vom 19. Februar 1986 (KDSG; BSG 152.04).
- Datenschutzverordnung vom 22. Oktober 2008 (DSV; BSG 152.040.1).
- Direktionsverordnung vom 03. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV; BSG 152.040.2).
- Gesetz vom 31. März 2009 über die Archivierung (ArchG; BSG 108.1).
- Verordnung vom 04. November 2009 über die Archivierung (ArchV; BSG 108.111).
- Verordnung vom 15. November 2017 über die Verwaltung und Archivierung von Unterlagen der Stadt Bern (Archivverordnung; ARCV; SSSB Nr. 421.21).
- Geoinformationsverordnung vom 03. April 2019 der Stadt Bern (StGeoIV; SSSB Nr. 152.09).

## 3.2 Schützenswerte Personendaten

Beim Umgang mit Personendaten ist immer dem Datenschutzgesetz des Kantons Bern (KDSG; BSG 152.04) Rechnung zu tragen. Als Personendaten gelten alle Angaben, welche sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Darunter können Namen, Vornamen und E-Mail-Adresse einer Person u.U. auch eine IP-Adresse fallen. Personendaten finden sich nicht nur in Verträgen (Bezeichnung der Vertragspartei), sondern auch in E-Mails (insbes. Absender), Worddateien (Metadaten), HR-Unterlagen, Logdaten (IP-Adresse) usw.

Besonders schützenswerte Personendaten sind Angaben über:

a) die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit;
b) den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand;
c) Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung;
d) polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.

## 3.3 Dateneigner*innen

Für alle erstellten Daten sind die Abteilungsleitungen als Dateneigner*innen verantwortlich. Sie sind formal für die Beurteilung definierter Informationswerte bezüglich ihrer Bedeutung für die Stadtverwaltung und für die korrekte Klassifizierung verantwortlich.

Die Dateneigner*innen sorgen dafür, dass

- die von ihnen erarbeiteten elektronischen Daten richtig klassifiziert und entsprechend geschützt werden,
- der Zugriff zu den Bearbeitungsverfahren und deren Daten nur Personen mit berechtigtem geschäftlichem Interesse erteilt wird,
- elektronische Daten mit der Klassifizierung *Vertraulich* oder *Geheim* nur einem eingeschränkten Personenkreis zur Verfügung gestellt werden,
  Mitarbeitende und externe Mitwirkende in hohem Masse über diese Weisung und Grundlagen informiert sind und diese richtig anwenden. Neben der systematisch und klar erkennbar vorgenommen Klassifizierung gehören hierzu auch standardisierte Prozesse beim Onboarding, beim Controlling und beim Qualitäts- und Risikomanagement (z.B. Aufbau Datenzirkel innerhalb Dienststelle).

# 4 Klassifizierung von elektronischen Daten

## 4.1 Verschiedene Perspektiven der Klassifizierung

Mit Hilfe der Klassifizierung der elektronischen Daten sollen die notwendigen Schutzmassnahmen abgeleitet werden, mit dem Ziel, die Kontinuität, Integrität, Vertraulichkeit sowie die Bereitstellung von Daten zu gewährleisten und die Auswirkungen von Sicherheitsvorfällen zu begrenzen.

Das Schutzniveau der Daten wird dabei in Klassifizierungsstufen für die Vertraulichkeit, Integrität und Verfügbarkeit der Daten ausgedrückt:

- **Vertraulichkeit**: Darunter versteht man, dass Daten nur von den Personen verändert oder eingesehen werden dürfen, die dazu auch berechtigt sind. Will man Daten vertraulich behandeln, muss klar festgelegt sein, wer in welcher Art und Weise Zugriff auf diese Daten hat und wie die Daten gespeichert und übertragen werden.

- **Integrität:** Unter der Integrität von Daten versteht man die Nachvollziehbarkeit von vorgenommenen Änderungen an diesen. Daten stehen immer einem gewissen Kreis von autorisierten Personen zur Verfügung. Es darf nicht möglich sein, dass Daten unerkannt bzw. unbemerkt geändert werden (verändern, löschen, einfügen, publizieren, entfernen).

- **Verfügbarkeit**: Die gespeicherten Daten müssen in einem grösstmöglichen zeitlichen Rahmen verfügbar sein, wenn die nutzenden Personen Zugriff darauf benötigen. So ist es unbedingt zu vermeiden, dass Daten verschwinden oder auf diese nicht zugegriffen werden kann, wenn sie gebraucht werden, respektive sie gemäss Öffentlichkeitsprinzip zur Verfügung stehen müssen.

## 4.2 Klassifizierung der Vertraulichkeit

Elektronische Daten müssen bezüglich der Vertraulichkeit klassifiziert werden, damit klar zugeordnet werden kann, ob und wem der Zugriff auf entsprechende Daten gewährt werden kann. Die Kategorien oder die Klassifizierung müssen dabei die Spannweite von vollständig öffentlichen Daten (öffentlich publizierte Informationen und Open Government Data) bis hin zu geschützten Daten (vertrauliche oder geheime Daten) abdecken.

Grundsätzlich sollen nur diejenigen Personen und Systeme Zugriff zu besonders geschützten Daten erhalten, welche diese unbedingt zur Erfüllung ihrer Aufgaben benötigen („need-to-know-Prinzip“). Die Klassifizierung von elektronischen Daten nach den in Kapitel 4.1 genannten Klassifizierungsstufen wird auf das erforderliche Mindestmass und wenn möglich zeitlich beschränkt. Die Dateneigner*innen bezeichnen Daten in ihrem Verantwortungsbereich, die vertraulich sind.

Für die Regelung der Zugriffe auf Daten durch Personen und andere Systeme muss grundsätzlich auf die im nachfolgenden Kapitel gezeigten allgemeinen Klassifizierungen geachtet werden. Dabei sind allenfalls auch die Informatiksysteme (und Schnittstellen), mit welchen besonders schützenswerte Daten bearbeitet, gespeichert, gelöscht, publiziert und übertragen werden, mit speziellen Sicherheitsmassnahmen umzusetzen, damit in jedem Falle sichergestellt werden kann, dass nur berechtigte Personen (oder Rollen) Zugriff auf die entsprechend klassifizierten Daten erhalten.

Das Öffentlichkeitsprinzip, der Datenschutz sowie die Geheimhaltungspflicht müssen bei allen Klassifizierungskategorien respektiert werden.

### 4.2.1 Klassifizierungsstruktur

Die elektronischen Daten werden in folgende Klassen eingeteilt:

- Öffentlich
- Intern (Default)
- Vertraulich
- Geheim

Die untenstehende Grafik illustriert die notwendigen Klassifizierungskategorien.

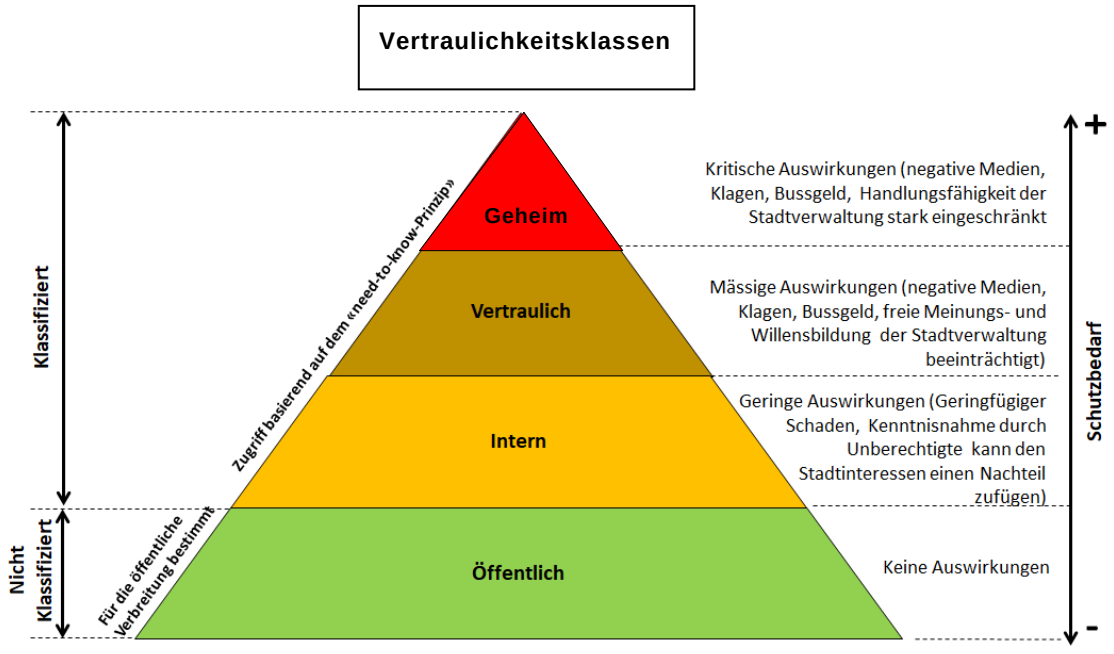


**Abbildung 1: Allgemeine Klassifizierungsstruktur**

### 4.2.2 Vertraulichkeitsklassen

Im Folgenden werden die vier Vertraulichkeitsklassen und die grundlegenden Regeln bezüglich Kennzeichnung, Weitergabe und Absicherung sowie das Schadenspotential bei unsachgemässem Umgang dargestellt.

| Klassifizierung | Beschreibung |
|---|---|
| **Öffentlich** | • Öffentliche[4] Daten sind für die Bevölkerung auch ausserhalb der Organisation zugänglich.<br>• Als öffentlich gelten alle Informationen, die vom*n der*die Dateneigner*in zur Veröffentlichung frei gegeben werden und/oder dem Öffentlichkeitsprinzip unterliegen.<br>• Diese Daten bedürfen *keiner* expliziten Kennzeichnung.<br>• Für die Handhabung offener Informationen existieren keine Einschränkungen, vorbehalten bleiben lizenzpflichtige Informationen wie beispielsweise GEO-Daten. |
| **Intern** | • Interne Daten sind für Mitarbeitende der Stadtverwaltung bestimmt. Als intern gelten alle elektronischen Daten, welche der*die Dateneigner*in nicht anderweitig klassifiziert wurden und welche nicht gemäss dem Öffentlichkeitsprinzip auch ausserhalb der Organisation zugänglich sind.<br>• Interne Daten können ohne Einschränkungen an Mitarbeitende der Stadtverwaltung übermittelt werden, sofern dienstlich benötigt.<br>• Diese Daten bedürfen *keiner* expliziten Kennzeichnung. |
| **Vertraulich** | • Daten, die für einen eingeschränkten, explizit festgelegten Empfängerkreis bestimmt.<br>• Unter vertraulichen Daten werden Informationen verstanden, deren Kenntnisnahme durch Unbefugte für die Stadtverwaltung grossen Schaden zufügen könnte (z.B. Finanzen, Rechtslage) oder jemanden in seinen persönlichen Verhältnissen verletzen könnte.<br>• Vertrauliche Daten können bestimmten, d.h. von dem*der Dateneigner*in bestimmte nutzende Person (namentlich oder Rollen) übermittelt werden, sofern dienstlich benötigt und vorher explizit als „vertraulich“ gekennzeichnet wurde.<br>• Diese Daten müssen als *vertraulich* gekennzeichnet werden.<br>• Besonders schützenswerte Personendaten[5] |
| **Geheim** | • Daten, die für einen eingeschränkten, explizit festgelegten kleinen Empfängerkreis in Verbindung mit oberster Leitung und kleiner Anzahl bestimmt.<br>• Unter geheimen Daten werden Informationen verstanden, deren Kenntnisnahme durch Unbefugte für die Stadtverwaltung erheblichen Schaden zufügen könnte. |

[4] Artikel 27 Informationsgesetz BGB 107.1

[5] Artikel 28 Informationsgesetz BSG 107.1

| Klassifizierung | Beschreibung |
|---|---|
| | • Vertrauliche Daten dürfen nur an bestimmte gemäss Dateneigner*in namentlich genannte nutzende Person übermittelt und von jedem*r Empfänger*in nur mit ausdrücklicher Einwilligung durch den*die Dateneigner*in an andere nutzende Personen weitergeleitet werden.<br>• Unabhängig davon ist der Kreis der nutzenden Personen möglichst klein zu halten.<br>• Diese Daten müssen als *geheim* gekennzeichnet werden. |

### 4.2.3 Änderung der Klassifizierung im Lebenszyklus von Daten

Daten können während des gesamten Lebenszyklus' verschiedene Klassifizierungsstufen durchlaufen. So können für die Veröffentlichung vorgesehene Informationen (z.B. Medienmitteilungen) temporär als vertraulich klassifiziert und zu behandeln sein, solange sie nicht veröffentlicht sind. Später muss die Klassifizierungsangabe entfernt werden, wenn die Daten nach Veröffentlichung nicht mehr klassifiziert sind.

Es muss jederzeit gewährleistet werden, dass die Kennzeichnung der Inhalte selbst und die Bezeichnung über die entsprechenden Klassifizierungen in den Metadaten (beschreibende Daten) nachgeführt wird. In einigen Fällen wird es sogar nötig sein, die Daten beim Wechsel der Klassifizierung auf andere Systeme zu verschieben oder entsprechende Metadaten zu vergeben (z.B. Verschiebung im Registraturplan) und es muss allenfalls mit angegeben werden wann und weshalb die Umklassifizierung geschah.

Zuständig für die Erledigung und saubere Kennzeichnung der Daten während des Lebenszyklus' von der Erstellung bis zur Ablieferung an das Stadtarchiv (elektronisches Langzeitarchiv) ist der*die jeweilige Dateneigner*in. Diese*dieser bleibt Dateneigner*in bis zur Ablieferung und muss auch in regelmässigen Abständen überprüfen, ob die Daten entlang der vorliegenden Weisung klassifiziert wurden und die notwendigen Änderungen nachgeführt sind.

### 4.2.4 Kennzeichnung von elektronischen Daten

Alle Daten, welche nicht für die Öffentlichkeit bestimmt oder intern sind, müssen eine Kennzeichnung aufweisen, welche die entsprechende Klassifizierungskategorie zeigt. Dies muss auch bei Daten in elektronischer Form, welche für den Druck optimiert wurden (z.B. Word-Dokumente oder PDF), gut sichtbar auf der Titelseite und in der Fusszeile oder in anderer geeigneter Form auf jedem Blatt eingefügt werden. Öffentliche oder interne Daten dürfen bei Bedarf die Klassifizierung «öffentlich» oder «intern» aufweisen.

Daten, die sich noch im Entwurfsstadium befinden, sind als solche mit dem Hinweis „Entwurf“ zu kennzeichnen. Zusätzlich sind diese mit einer Kennzeichnung der jeweiligen Klassifizierungsstufe zu versehen. Dokumente im Entwurfsstadium dürfen nicht die Kennzeichnung «öffentlich» aufweisen.

Sinnvollerweise werden sämtliche Vorlagen und Daten bei der Erstellung automatisch (per Default) auf die Kategorie intern gestellt: Dokumentenvorlagen (wie beispielsweise Word-Dokumente) enthalten die entsprechende Kategorie in den Metadaten, Datensätze in Datenbanken enthalten die Angaben intern per Default als Metadaten mitgeliefert. Die Benutzenden müssen so z.B. bei Veröffentlichung die Kategorie explizit auf öffentlich (nicht klassifiziert) stellen.

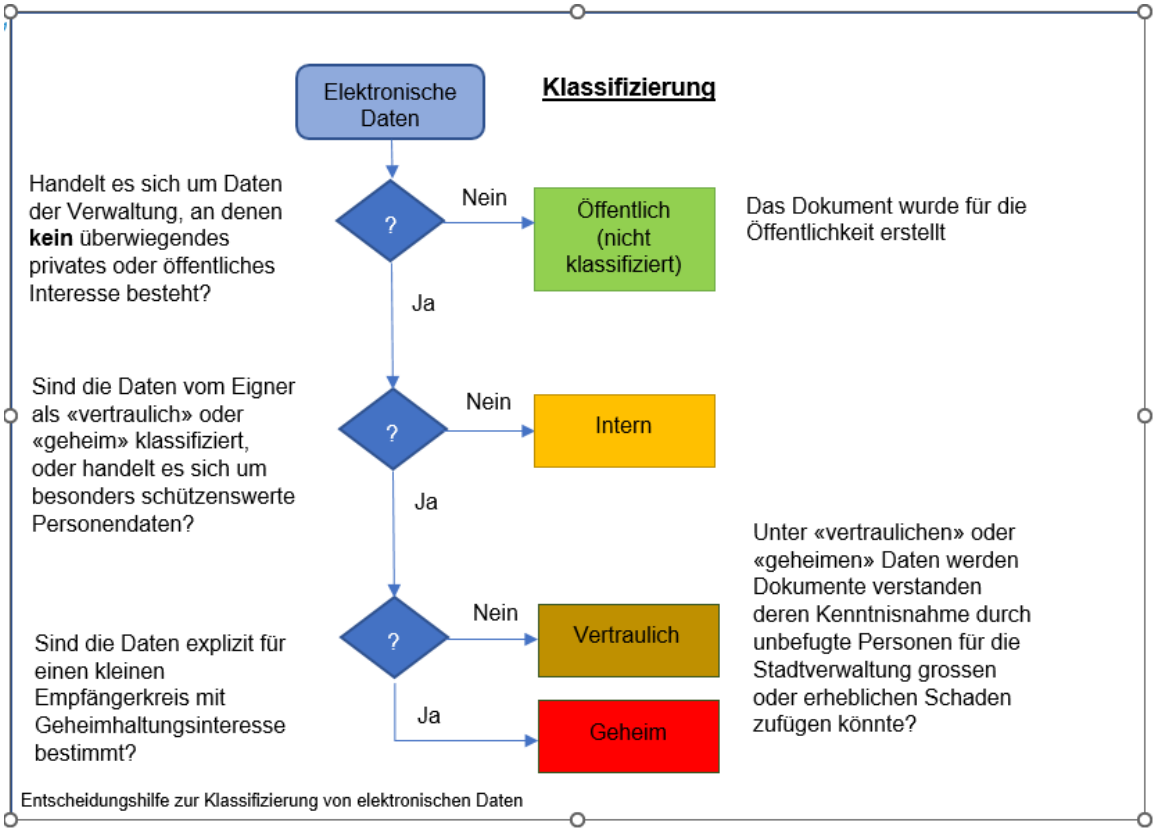


**Abbildung 2: Entscheidungshilfe zur Klassifizierung der Vertraulichkeit**

## 4.3 Klassifizierung der Integrität

Datenintegrität bezieht sich auf die Zuverlässigkeit und Vertrauenswürdigkeit von Daten während ihres gesamten Lebenszyklus. Das Schutzziel beschreibt die Anforderungen an die Richtigkeit (Korrektheit /Unversehrtheit) von Daten und damit zusammenhängend der korrekten Funktionsweise von Systemen. Integrität bedeutet gegenüber der Vertraulichkeit, dass Daten nicht unerkannt bzw. unbemerkt verändert werden dürfen. Es geht hierbei um Korrektheit der Daten und dabei um die Nachvollziehbarkeit von Datenänderungen.

Der*die Dateneigner*in ist für die Klassifizierung bezüglich Integrität der im eigenen Verantwortungsbereich vorhandenen Informationen zuständig:

| Klassifizierung | Beschreibung |
|---|---|
| **Normal** | • Bei „Normal“ ist die Richtigkeit der Daten von der Sache her sehr wichtig. Tritt aber dennoch ein Fehler auf, kann mit entsprechendem Aufwand die Integrität wiederhergestellt werden. Die Integritätsverletzung ist folglich korrigierbar.<br>• Mögliche Auswirkungen unbefugter oder unbeabsichtigter Veränderungen der Informationen sind für den*die Dateneigner*in akzeptabel. Ein sorgfältiger Umgang mit den Informationen im Tagesgeschäft, sowie die Anwendung von Grundschutzmassnahmen (wie Zugriffsschutz und Backup) werden als ausreichende Sicherheitsmassnahmen betrachtet.<br>• Gilt als Standardwert für alle Informationen, die bezüglich Integrität nicht explizit als *hoch* eingestuft sind. |
| **Hoch** | • Unbefugte oder unbeabsichtigte Veränderungen der Daten sind für den*die Dateneigner*in nicht akzeptabel. Sie müssen verhindert oder mindestens erkannt werden.<br>• Ein Fehler muss sofort erkannt werden, da die Daten unmittelbar Handlungen auslösen, die nicht mehr rückgängig gemacht werden können, die aber bei falschen Angaben fatale Folgen haben können (Beispiel Abstimmungsresultate). |

## 4.4 Klassifizierung der Verfügbarkeit

Das Schutzziel „Verfügbarkeit“ beschreibt, in welchem Umfang die Daten und Systeme bei Störungen und Ausfällen in dem vereinbarten Rahmen zur Verfügung stehen müssen und wie gross der maximale Datenverlust sein darf.

Der*die Dateneigner*in ist für die Klassifizierung bezüglich Verfügbarkeit der im eigenen Verantwortungsbereich vorhandenen Informationen zuständig:

| Klassifizierung | Beschreibung |
|---|---|
| **Normal** | • Einschränkungen beim Zugriff auf die elektronischen Daten oder ein vollständiger Verlust der Zugriffsmöglichkeiten während mindestens einem Arbeitstag ist akzeptabel.<br>• Ein Verlust der seit der letzten Datensicherung vor einem Vorfall (Incident) durchgeführten Änderungen an den Informationen ist akzeptabel.<br>• Gilt als Standardwert für alle Informationen, die bezüglich Verfügbarkeit nicht explizit als *hoch* eingestuft sind. |
| **Hoch** | • Einschränkungen beim Zugriff auf die Daten oder ein vollständiger Verlust der Zugriffsmöglichkeiten sind innerhalb von 4 Stunden akzeptabel.<br>• Ein Verlust der seit der letzten Datensicherung einem Vorfall (Incident) durchgeführten Änderungen an den Informationen ist bis maximal 4 Stunden akzeptabel oder mit zusätzlichen Massnahmen zum Schutz vor Datenverlust abzusichern (Log). |

# 5 Mögliche Risiken je Klassifizierung mit Beispielen

## 5.1 Vertraulichkeits-Risiken

| Risiko-klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| **Öffentlich** | **Unbedeutendes Risiko**<br><br>Keine weit reichenden Konsequenzen, da die Information für die Öffentlichkeit bestimmt ist.<br><br>Allenfalls können beispielsweise aus Entwürfen, qualitativ noch ungeprüften oder falsch verwendete Daten Falschaussagen abgeleitet werden (Presse). Diese liessen sich aber gut widerlegen. | **Diese Daten und Informationen sind gemäss dem Öffentlichkeitsprinzip der Bevölkerung zugänglich**.<br><br><u>Exemplarische Prüffragen:</u><br><br>- Sind die Informationen nicht den schützenswerten oder einfachen Personendaten zuzuordnen und/oder nicht nur für den verwaltungsinternen Gebrauch bestimmt?<br>- Können die Daten uneingeschränkt (z.B. im Internet) veröffentlicht werden? | - Medienmitteilungen<br>- Stadtratsunterlagen/-erlasse<br>- Open Government Data (OGD), z.B. statistische Rohdaten<br>- Stadtkalender<br>- Jahresberichte<br>- Wahl- und Abstimmungsresultate<br>- Antworten vom Gemeinderat |

| Risiko-klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| intern | **Geringes Risiko**<br><br>Eine Veröffentlichung begrenzter Mengen von sensitiven Daten kann zu einem Vertrauensverlust mit eingeschränkter kurzfristiger Belästigung, Bedrängnis oder Verlegenheit einer beteiligten Partei führen. | **Diese Daten und Informationen, die den einfachen Personendaten zuzuordnen und/oder Sachdaten, welche nur zur Erledigung der verwaltungsinternen Aufgaben bestimmt sind.**<br><br><u>Exemplarische Prüffragen:</u><br><br>- Stehen die Daten allen Mitarbeitenden oder einem grossen Kreis zu Verfügung, sind aber nicht für die Öffentlichkeit gedacht?<br>- Sind die Daten den einfachen Personendaten zuzuordnen?<br>- Sind die Sachdaten nur zur Erledigung von verwaltungsinternen Aufgaben bestimmt? | - Organisatorische Grundlagen einer Dienststelle.<br>- Einfache Personendaten wie Listen von Personen/Mitarbeitende.<br>- Projektdokumente<br>- Öffentliche Dokumente, welche noch im Entwurfsstadium sind<br>- Entwürfe für die öffentliche Kommunikation z.B. Medienmitteilungen mit Sperrfrist.<br>- Betriebshandbücher IT<br>- Interne Kommunikation<br>- Forum, in welchem man über verschiedenste Themen diskutieren kann. Nur registrierte Benutzende können Einträge erstellen. Zur Registrierung sind Vorname, Name, E-Mail-Adresse, Benutzername und Passwort anzugeben. Die Angaben werden nicht überprüft und Benutzername und Passwort können ohne Beschränkungen frei gewählt werden. |

| | | | |
|---|---|---|---|
| **vertraulich** | **Mittleres Risiko**<br><br>Schlimmstenfalls eine Veröffentlichung von sensitiven Behörden-, Unternehmens- oder Personendaten an unautorisierte Drittpersonen, wodurch ein Vertrauensverlust mit spürbaren negativen Auswirkungen auf die Ausübung der Haupttätigkeiten der betroffenen Parteien entsteht.<br><br>- Betroffen ist ein Aufgabenbereich der Stadt Bern<br>- Erheblicher finanzieller Schaden<br>- Rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen<br>- Verärgerung und Imageverlust bei Personengruppen oder Organisationen | **Diese Daten sind auf der Basis besonderer geschäftlicher oder gesetzlicher Anforderungen vertraulich zu behandeln. Der Zugriff ist auf die mit dem Geschäft betrauten Personen beschränkt. Die Dateninhaber müssen jederzeit prüfen können, welche Personen mit welchen Bearbeitungsrechten (Schreiben, Lesen, Löschen) Datenzugriff haben**.<br><br><u>Exemplarische Prüffragen:</u><br>- Kann die öffentliche Sicherheit oder die Sicherheit Einzelner wesentlich beeinträchtigt werden?<br>- Kann die freie Meinungs- und Willensbildungsprozess der öffentlichen Organe wesentlich beeinträchtigt werden?<br>- Kann die Beziehungen zu einem anderen Kanton, zum Bund oder zum Ausland beeinträchtigt werden?<br>- Kann mit diesen Daten eine Zusammenstellung ermöglicht werden, die eine Beurteilung wesentlicher Aspekte (z.B. Steuerdaten) einer natürlichen Person (Persönlichkeitsprofil) erlaubt oder die Privatsphäre verletzt?<br>- Wurden die Daten von einer anderen Behörde einer vergleichbaren Vertraulichkeitsstufe zugeordnet? | - Personal- und Bürgerdossiers<br>- Heute als *geheim* klassifizierte GRB's (Teilmenge)<br>- Gespeicherte Kundendaten z.B. im Sozialbereich, Kinderbetreuung oder Einwohnerkontrolle<br>- Angaben im Zusammenhang mit der Organisation von Verkehr- und Polizeiaufgaben<br>- Synchronisation der E-Mail-, Kalender- und Kontaktdaten mit mobilen Geräten<br>- Schützenswerte Personendaten; religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit, den seelischen, geistigen oder körperlichen Zustand, Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung<br>- Überwiegende öffentliche Interessen; der Schutz vor vorzeitige Bekanntgabe von Informationen, welche die Entscheidungsfindung oder eine Verhandlung wesentlich beeinträchtigen.<br>- Überwiegende private Interessen; der Schutz des persönlichen Geheimbereichs, der Persönlichkeitsschutz in nicht rechtskräftig abgeschlossenen Verwaltungs- und Justizverfahren, Geschäfts-, Berufs- oder Fabrikationsgeheimnisse<br>- Polizeiliche Ermittlungen, Straftaten und die dafür verhängten Strafen oder Massnahmen |

| Risiko-klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| Geheim | **Schwerwiegendes Risiko bis Existenz gefährdend**<br><br>Die Veröffentlichung von sensitiven Behörden-, Unternehmens- oder Personendaten an unautorisierte Drittpersonen, wodurch ein Vertraulichkeitsverlust mit gravierenden negativen Auswirkungen auf die Ausübung der Haupttätigkeiten der betroffenen Parteien entsteht.<br><br>- Betroffen ist die Gesamte Verwaltung.<br>- Sehr schwerer Schaden für die Geschäftszwecke und Ziele.<br>- Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen.<br>- Erheblicher Verlust von Ansehen und Vertrauen bei Bevölkerung/Politik. | **Diese Daten sind auf der Basis besonderer geschäftlicher oder gesetzlicher Anforderungen geheim zu behandeln. Der Zugriff ist auf die mit dem Geschäft betrauten Personen beschränkt. Die Dateninhaber müssen jederzeit prüfen können, welche Personen mit welchen Bearbeitungsrechten (Schreiben, Lesen, Löschen) Datenzugriff haben. Zugriffsrechte, Kopien und Löschungen sind zu protokollieren.**<br><br><u>Exemplarische Prüffragen:</u><br>- Kann die künftige Entscheidungsfindung des Gemeinderates, die öffentliche Sicherheit, die Sicherheit Einzelner, die öffentliche Versorgung schwerwiegend beeinträchtigt oder auf andere Weise gravierenden Schaden verursacht werden?<br>- Kann der freie Meinungs- und Willensbildungsprozess der öffentlichen Organe gravierend beeinträchtigt werden?<br>- Wurden die Daten von einer anderen Behörde einer vergleichbaren Geheimhaltungsstufe zugeordnet | - Daten welche die Handlungsfähigkeit des Stadtrats, die Aufgabenerfüllung des Gemeinderats, oder wesentlicher Teile davon vor schwerwiegend Beeinträchtigungen oder Gefahren schützen<br>- Daten mit börsenkursrelevanten Informationen über Unternehmen mit städtischer Beteiligung<br>- Daten zu Gemeinderatsgeschäften aufgrund von gesetzlichen oder vertraglichen Geheimhaltungspflichten<br>- Gesamtstädtisches Sicherheits- und Versorgungsdispositiv |

**Abbildung 3: Darstellung der Klassifikationsstruktur**

## 5.2 Integritäts-Risiken

| Risiko-Klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| Normal | **Geringes Risiko**<br><br>Unsachgemässe Behandlung von Daten führen zu Verlusten oder Falschinformationen. Es entstehen Kosten in der Korrektur dieser Daten.<br><br>Eine Verletzung der Nachvollziehbarkeit und der Unleugbarkeit führt zu keinem juristischen Schaden. | **Fehler im Zusammenhang mit fehlenden oder unwirksamen automatisierten Dateneingabe- und Datenannahmekontrollen, die Fehler in den Informationen verursachen.**<br><br><u>Exemplarische Prüffragen:</u><br><br>- Sind die Daten hinsichtlich Integrität kritisch?<br>- Können die Daten bei Verfälschung schwerwiegende Schäden verursachen?<br>- Ist die Nachvollziehbarkeit der Veränderungen aufgrund regulatorischer oder gesetzlicher Vorgaben zwingend? | - Stadtkalender mit falschen Einträgen<br>- Interne Protokolle, welche nicht freigegeben aber bereits publiziert wurden<br>- Imageschaden, da nicht nachgeführte und nicht aktualisierte Webinhalte |

| Risiko-Klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| **Hoch** | **Schwerwiegendes Risiko**<br><br>Unbefugte Änderung oder Zerstörung von Informationen haben schwerwiegende nachteilige Auswirkungen auf den organisatorischen Betrieb, die Stadt Bern oder Einzelpersonen. | **Schwerwiegende Fehler im Zusammenhang mit fehlenden oder unwirksamen automatisierten Dateneingabe- und Datenannahmekontrollen, die Fehler in den Informationen und der Nachvollziehbarkeit verursachen.**<br><br><u>Exemplarische Prüffragen:</u><br><br>- Sind die Daten hinsichtlich Integrität kritisch?<br>- Sind die Daten hinsichtlich Vertrauenswürdigkeit besonders schützenswert?<br>- Können die Daten bei Verfälschung schwerwiegende Schäden verursachen?<br>- Ist die Nachvollziehbarkeit der Veränderungen aufgrund regulatorischer oder gesetzlicher Vorgaben (Compliance) zwingend? | - Finanzdaten.<br>- Besonders schützenswerte Personendaten.<br>- Datenbanktransaktionen<br>- Nicht vollständige CMDB (Configuration Management Database) & Konfigurations-Repository (oder mit irreführenden Angaben)<br>- Protokolle und Beschlüsse<br>- Verfälschung von Informationen, die an die Öffentlichkeit bestimmt sind (die Herausgabe irreführender, ungenauer oder vertraulicher Informationen zur Täuschung, Irreführung oder Verschleierung von Fehlverhalten oder im Tausch gegen Vorteile oder Vergünstigungen)<br>- Verlust von Daten und damit Verlust der Nachvollziehbarkeit<br>- Manipulation des Beschaffungsprozesses durch Bevorzugung eines Bieters |

**Abbildung 4: Beispiele Integritäts-Risiken**

## 5.3 Verfügbarkeits-Risiken

| Risiko-Klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| **Normal** | **Geringes Risiko**<br><br>Ausfall von unkritischen, internen Fileshare-Systemen verhindern den Zugriff auf wichtige Arbeitsdokumente. Dadurch sind Ressourcen nicht produktiv einsetzbar und führen zu Verzögerungen.<br>**Achtung**: Verfügbarkeits-Klassen können sich terminlich verändern, wenn wichtige Vorhaben geplant und durchgeführt werden, wie beispielsweise Abschlussarbeiten oder wichtige Präsentationen vor Gemeinderatsitzungen. Eine entsprechende Kommunikation muss sichergestellt und Massnahmen getroffen werden. | **Wichtige Systeme sind nicht genügend gegen Ausfall geschützt. Die Risiken hinsichtlich Verfügbarkeit sind nicht korrekt eingeschätzt worden.**<br><br><u>Exemplarische Prüffragen:</u><br><br>- Sind die Anforderungen an die Verfügbarkeit definiert worden?<br>- Können die Systeme nach einem Ausfall in der mit den Abteilungen vereinbarten Recovery-Zeiten wiederhergestellt werden?<br>- Werden die elektronischen Daten gemäss Vereinbarung regelmässig gesichert und können diese auf Verlangen in der geforderten Zeit wiederhergestellt werden? | - Ausfall Fileshare System<br>- Irrtümliches löschen von Protokollen<br>- Datenbank-Ausfall |

| Risiko-Klasse | Schadensgrösse | Beschreibung | Beispiele |
|---|---|---|---|
| **Hoch** | **Schwerwiegendes Risiko**<br><br>Ausfall von zentralen Webservern mit wichtigen Informationen für die Bürger der Stadt. Längere Ausfallzeiten können zu Reputationsschaden oder gar juristische Auseinandersetzungen wegen Klagen aufgrund verzögerter Geschäftsprozesse. | **Elektronische Daten stehen bei wichtigen Geschäften nicht zur Verfügung oder gehen gar ganz verloren. Die Wiederherstellung und Zurverfügungstellung ist mit grossen Kosten und zeitlichen Verzögerungen verbunden, welche zu Verletzungen der Sorgfaltspflicht und Compliance führen können.**<br><br><u>Exemplarische Prüffragen:</u><br><br>- Unterliegen die elektronischen Daten dem Datenschutz oder anderen Gesetzesvorlagen<br>- Sind die Anforderungen an die Verfügbarkeit definiert worden?<br>- Braucht es für die Daten ein Business Continuity Konzept<br>- Können die Systeme nach einem Ausfall in der mit den Abteilungen vereinbarten Recovery-Zeiten wiederhergestellt werden?<br>- Werden die elektronischen Daten gemäss Vereinbarung regelmässig gesichert und können diese auf Verlangen in der geforderten Zeit wiederhergestellt werden? | - Ausfall Public Webserver<br>- Ausfall zentraler Datenbanken<br>- Nichtverfügbarkeit wichtiger Geschäftsprotokolle |

**Abbildung 5: Beispiele Verfügbarkeits-Risiken**

# Anhang

## A) Umgang und Kennzeichnung von klassifizierten elektronischen Daten

| **Klassifikation**<br>Risikograd<br>Datenart | **Öffentlich**<br>Kein oder geringes Risiko | **Intern**<br>Geringes Risiko | **Vertraulich**<br>Mittleres Risiko | **Geheim**<br>Schwerwiegend bis Existenz gefährdendes Risiko |
|---|---|---|---|---|
| Bearbeitung von digitalen Dokumenten (Word, PDF, etc.) | Kennzeichnung nicht erforderlich. | - Kennzeichnung nicht erforderlich.<br>- An Dritte/Externe nur nachschriftlicher Geheimhaltungsvereinbarung.<br>- Kopieren erlaubt. | - Kennzeichnung explizit mit „Vertraulich“ auf jeder Seite in Kopf- oder Fusszeile und auf Deckblatt.<br>- Liste der Empfänger empfohlen, namentlich aufgeführt oder Bezeichnung Gremium.<br>- Seitenangabe mit Seite von bis. | - Kennzeichnung explizit mit „Geheim“ auf jeder Seite in Kopf- oder Fusszeile und auf Deckblatt.<br>- Liste der Empfänger erforderlich, namentlich aufgeführt oder Bezeichnung Gremium.<br>- Seitenangabe mit Seite von bis. |
| Bearbeitung von strukturierten Daten-Files (z.B. Excel, XML, Datenbanken, etc.) | Kennzeichnung nicht erforderlich, wenn explizit als Open Government Data vorgesehen und publiziert, in Metadaten Angabe von möglichen Copyright-Formen bzw. gut sichtbarer | - Kennzeichnung nicht erforderlich, ausser in den Metadaten.<br>- An Dritte/Externe nur mit schriftlicher Geheimhaltungserklärung (Non Disclosure Agreement NDA)<br>- Kopieren erlaubt. | - Nur an Personenkreis mit Berechtigung zur Kenntnisnahme.<br>- An Dritte/Externe Kopie oder Zugang nur mit schriftlicher Geheimhaltungserklärung (Non Disclosure Agreement NDA)<br>- Sind Daten explizit als „Vertraulich“ “ zu kennzeichnen, | - Nur an namentlich festgelegten Personenkreis, Anlegen einer Verteilungs- oder Zugriffsliste.<br>- An Dritte keine Weitergabe; in Sonderfällen Rechtskonsulentin oder Rechtskonsulent des Gemeinderats fragen.<br>- Sind Daten explizit als „geheim“ zu kennzeichnen, so ist der Träger der Information |

| | | | | |
|---|---|---|---|---|
| | Hinweis auf erforderliche Quellenangaben. | | so ist der Träger der Information (z.B. Papierbogen, DVD, Server) deutlich erkennbar mit der Kennzeichnung „Vertraulich“ zu versehen.<br>- Es muss aufgezeigt werden können, wer namentlich Zugriff auf die Systeme oder den Datenträger hat oder haben könnte.<br>- Kopieren nur nach Rücksprache mit dem Urheber. | deutlich erkennbar mit der Kennzeichnung „geheim“ zu versehen.<br>- Es muss aufgezeigt werden können, wer namentlich Zugriff auf die Systeme oder den Datenträger hat oder haben könnte.<br>- Kopieren nicht gestattet, oder Kopierschutz, wo möglich und machbar. |
| Elektronische Übertragung | Ohne Einschränkung | Elektronische Übertragung zulässig (z.B. über internes Mail, Arbeitsräume, BernBox); wenn möglich, Verschlüsselung nutzen | - Elektronische Übertragung nur verschlüsselt erlaubt.<br>- Bei Datenträgern einschreiben, d.h. schriftliche Empfangsbestätigung vom Transportunternehmen erforderlich. | Elektronische Übertragung nur verschlüsselt erlaubt, und Zugriff kann jederzeit protokolliert und digital nachvollzogen werden. |
| Aufbewahrung | Ohne Einschränkung | - Aussenstehenden nicht zugänglich (z.B. klare Zugangsregelung zu Räumen und Ablagen und Computersystemen<br>- Bei Mitnahme Kenntnisnahme durch Unbefugte verhindern (Verschlüsselung auf Datenträgern und Geräten, Zugriff nur mit Passwort) | - Datenträger und Dokumente unter Verschluss halten (z.B. abschliessbare Schränke oder Schubladen)<br>- Verschlüsselte Aufbewahrung auf allen Arten von Datenträgern.<br>- Grundsätzlich keine Mitnahme. | - Unter Verschluss halten, vorzugsweise im Tresor<br>- Verschlüsselte Aufbewahrung auf allen Arten von Datenträgern.<br>- In der Cloud nur unter den höchstmöglichen Schutzbedingungen. |

| | | | | |
|---|---|---|---|---|
| Entsorgung / Vernichtung / Löschung | Daten, die gemäss dem Öffentlichkeitsprinzip öffentlich zur Verfügung gestellt werden sollen, dürfen nicht einfach gelöscht werden. Rücksprache allenfalls mit Stadtarchiv. | - Datenträger müssen zerstört oder definitiv gelöscht werden (vollständige Neuformatierung).<br>- Bei Datenbanken muss sichergestellt und kontrolliert werden, ob die periodische Löschung von älteren Datenbeständen erfolgt ist. | - Datenträger müssen zerstört oder definitiv gelöscht werden (vollständige Neuformatierung).<br>- Bei Datenbanken muss sichergestellt und kontrolliert werden, ob die periodische Löschung von älteren Datenbeständen erfolgt ist. | Wie bei vertraulich, jedoch unter Aufsicht und Protokollierung der Datenträgervernichtung. |

**Abbildung 6: Umgang mit klassifizierten Daten**