



Kanton Zürich  
Finanzdirektion  
**KITT Geschäftsstelle**

Rahel Aeppli  
Informatikstrategie & Projektmanagement  
Walcheplatz 1  
8090 Zürich  
Telefon +41 43 259 48 11  
rahel.aeppli@kitt.zh.ch  
www.kitt.zh.ch

# Datenklassierung

Datum 28. Mai 2015  
Status zur Prüfung  
Auftraggeber/-in FD

## **Inhalt**

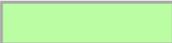
- |  |          |
|--|----------|
| <b>1. Allgemeine Informationen</b>                                 | <b>3</b> |
| <b>2. Informationseigenschaften vs. Grundschutz</b>                | <b>4</b> |
| <b>3. Klassierungskriterien und –ansprüche vs. erhöhter Schutz</b> | <b>5</b> |



## 1. **Allgemeine Informationen**

- Anhang 1 zur Verordnung über die Informationssicherheit (ISV) vom .... (z. Zt. Vs. 4.0 vom 28.05.2015)
- Genereller Vermerk: Besondere Aufmerksamkeit ist den Übergängen zwischen "Normalbetrieb", "ruhende Ablage" und "definitives Endlager" (Archiv) zu schenken.
- [1] Ausprägungen gem. Norm eCH-0039; Aus Erfahrung empfehlen wir, die Ausprägung "intern" als default zu spezifizieren. Alle Dokumente ohne Vermerk sind also nur intern, nur wenn „öffentlich“ resp. "nicht klassifiziert" drauf steht, darf das Dokument verschickt, verteilt, einem Journalisten zugänglich gemacht werden.

## 2. Informationseigenschaften vs. Grundschutz

Informationseigenschaften (Kt. ZH: IDG, ISV und IDV) vs. Grundschutz					ERSTER ENTWURF
Kriterium	Ausprägungen (als Beispiele zu verstehen; nicht abschliessend)				Sicherheitsstufe für LE Grundschutz
Verfügbarkeit	Sofort; zwingend immer 7*24h	Wartezeit max. 4 h toleriert	Wartezeit bis 48h toleriert	Wartezeit bis 1 Woche toleriert	Konfiguration redundant; Netz redundant; Client redundant; Pikettdienst; zwei Standorte
Datensicherheit (Datenexistenz)	Dokument ist existentiell wichtig	Hohe Bedeutung in Krisenfällen	Verlust kann finanzielle Konsequenzen haben	Verlust ist unangenehm	Datensicherung mehrere Generationen; mind. zwei Standorte; Standorte räumlich getrennt
Integrität (Richtigkeit, Authentizität und Nachvollziehbarkeit)	Zwingend nachweisbare Unveränderlichkeit	Mit Zusatzaufwand Integrität nachweisbar	Integrität durch Parallelog. nachweisbar (Papier / elektronische Ablage)	Integrität nicht nachweisbar	Veränderung bei Datenbank mit Audit-Trail; Dokumente werden bei jeder Aenderung als pdf weggeschrieben
Zurechenbarkeit	Zurechenbarkeit durch Beglaubigung	Zurechenbarkeit durch Visum bei jeder Transaktion	Zurechenbarkeit durch Login-trail	Zurechenbarkeit nur durch Kontext gegeben	Zurechenbarkeit wird durch DSGVO gefordert. Login-Trail ist Grundschutz
Vertraulichkeit[1]	Geheim (secret)	vertraulich (confidential)	intern (in_house)	Nicht klassifiziert (unclassified)	Passwortschutz mit (min.) User-ID und starkem Passwort; keine Gruppen-Passwörter
Personendaten	Besondere Personendaten	Personendaten	Frei verwaltungsintern	öffentlich	kein Zugriff ohne User-ID möglich; Einschränkungen nur via LB-Organisation (need to know)
Aufbewahrungsfristen	Ewig	10 Jahre	5 Jahre	1 Jahr	Standardmässig 10 Jahre nach letzter Bewegung; in DB-Systemen keine Löschungen
Löschvorgabe nach Ablauf Aufbewahrungsfrist	Darf nach Ablauf NICHT gelöscht werden	MUSS nach Ablauf gelöscht werden	Keine		keine technischen Vorkehrungen; das "physische Löschen" ist nicht realisierbar, da Datensicherung nicht mehr beeinflussbar.
Wiedervorlagedauer aus ruhender Ablage	1 Sekunde	5 Minuten	1 Stunde	1 Arbeitstag	Abhängig von Prozess-Organisation und Schlüsselssystem
Treffsicherheit bei Suche in ruhender Ablage	Genau ein Dokument	Mehrere Dokumente die zum gleichen Dossier gehören (Suche im Dossier nötig)	Ganzer Vorgang	Alles zum Stichwort ("Google-Suche")	Abhängig von Prozess-Organisation und Schlüsselssystem
 schraffiert: Empfehlung für Default-Wert  grün: im Umfang ZH-Grundschutz					Diese Anforderungen sind beispielhaft zu verstehen, sie basieren auf dem "ZH-Grundschutz", spezifiziert bezüglich der o.a. Kriterien. "Grün" ist nur erfüllt, wenn der ZH-Grundschutz (tbd) vollständig ist, eingeschlossen die o.a. Forderungen.

