# Informatiksicherheitsverordnung

(vom 17. Dezember 1997)[1]

## I. Allgemeine Bestimmungen

Geltungsbereich

§ 1. Diese Verordnung gilt für die kantonale Verwaltung, die Bezirksverwaltungen und die unselbständigen Anstalten.

Sie gilt auch für Gemeinden, soweit sie gemeinsam mit den vorgenannten Stellen Informatiksysteme oder -anwendungen betreiben oder mit ihnen Daten austauschen.

Grundsatz

§ 2. Informatiksysteme und -anwendungen sind durch angemessene organisatorische und technische Massnahmen vor äussern Einwirkungen und vor unbefugtem Zugriff zu schützen.

Begriffe

§ 3. Die folgenden Ausdrücke bedeuten:

a) Informatiksysteme: Geräte und Einrichtungen sowie die dazugehörende Infrastruktur und Betriebssoftware, die zur elektronischen Bearbeitung von Daten eingesetzt werden.
b) Informatikanwendungen: Programme, welche die Nutzung von Informatiksystemen für die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen, einschliesslich der dabei bearbeiteten Daten.
c) Daten: Alle digitalen Informationen, die mit Informatiksystemen bearbeitet werden.

Verantwortlichkeiten

§ 4. Die Amtsstellen beurteilen die Risiken, legen die Sicherheitsstufen fest und ermitteln die Schutzziele. Sie beantragen die Sicherheitsmassnahmen für ihre Informatiksysteme und -anwendungen.

Die vorgesetzte Direktion oder die Staatskanzlei legt die Sicherheitsmassnahmen fest und kontrolliert deren Umsetzung und Einhaltung durch die Amtsstellen.

Die Gemeinden regeln die Verantwortlichkeiten selbst.

Unterstützung

§ 5. Die Informatikfachstellen, insbesondere das Amt für Informatikdienste, die Abteilung für Informatikplanung, die Informatikverantwortlichen der Direktionen, die betrieblichen Sicherheitsbeauftragten, die Informatikrevision der Finanzkontrolle sowie die oder der Beauftragte für den Datenschutz beraten die Amtsstellen bei der Risikobeurteilung, der Festlegung der Sicherheitsstufen, der Ermittlung der Schutzziele sowie bei der Bestimmung, Umsetzung und Überprüfung der Sicherheitsmassnahmen.

## II. Sicherheitsstufen und Schutzziele

Risikobeurteilung

§ 6. Die Amtsstellen prüfen für ihre Informatiksysteme und -anwendungen je einzeln die Gefährdung insbesondere durch unvorsichtiges oder böswilliges Verhalten von Mitarbeitenden und Aussenstehenden, technische Mängel an Geräten und Gebäuden sowie durch Feuer und Elementarereignisse.

Sie berücksichtigen die Eintretenswahrscheinlichkeit und beurteilen die möglichen Negativfolgen.

Negativfolgen

§ 7. Die Negativfolgen gelten als klein, wenn der Ausfall des Informatiksystems oder der -anwendung oder der Verlust oder das unbefugte Bearbeiten von Daten nur zu geringen Schäden führen, keine Persönlichkeitsrechte gefährden, die Einhaltung gesetzlicher und vertraglicher Pflichten nicht einschränken und die Aufgabenerfüllung höchstens geringfügig beeinträchtigen kann.

Mittlere Negativfolgen liegen vor, wenn der Ausfall des Informatiksystems oder der -anwendung oder der Verlust oder das unbefugte Bearbeiten von Daten zu grösseren, aber überblickbaren Schäden führen, Persönlichkeitsrechte gefährden, die Einhaltung gesetzlicher und vertraglicher Pflichten einschränken oder die Erfüllung wesentlicher Aufgaben beeinträchtigen kann.

Die Negativfolgen gelten als gross, wenn der Ausfall des Informatiksystems oder der -anwendung oder der Verlust oder das unbefugte Bearbeiten von Daten zu grossen Schäden führen, Persönlichkeitsrechte in hohem Masse gefährden, die Einhaltung gesetzlicher oder vertraglicher Pflichten stark einschränken oder die Erfüllung wesentlicher Aufgaben verunmöglichen kann.

Sicherheitsstufen

§ 8. Bei kleinen Negativfolgen gehören Informatiksysteme und -anwendungen zur Sicherheitsstufe 1. Ein Grundschutz ist zu gewährleisten.

Bei mittleren Negativfolgen gehören Informatiksysteme und -anwendungen zur Sicherheitsstufe 2. Ein mittlerer Schutz ist zu gewährleisten.

Bei grossen Negativfolgen gehören Informatiksysteme und -anwendungen zur Sicherheitsstufe 3. Ein hoher Schutz ist zu gewährleisten.

Schutzziele

§ 9. Entsprechend der Art und Grösse der Negativfolgen legen die Amtsstellen im Rahmen der Sicherheitsstufen Schutzziele fest bezüglich

a) Verhinderung einer unbefugten Kenntnisnahme von Daten (Vertraulichkeit),

b) Verhinderung einer unbefugten Veränderung von Daten oder Zugriffsrechten (Integrität und Authentizität) und
c) höchstzulässiger Dauer eines Ausfalls der Informatiksysteme und -anwendungen (Verfügbarkeit).

## III. Umsetzung der Sicherheitsmassnahmen

Massnahmenplan

§ 10. Die Amtsstellen erstellen einen Plan der organisatorischen und technischen Massnahmen, um für ihre Informatiksysteme und -anwendungen die ermittelten Schutzziele zu erreichen.

Sie berücksichtigen dabei den Grundsatz der Verhältnismässigkeit, den Stand der Technik und die verfügbaren Mittel.

Die Massnahmen können der Verkleinerung des Risikos dienen (Zutrittskontrollen, Zugriffsschutz, Verschlüsselung usw.) oder der Milderung der Folgen (Alarmsysteme, Protokollierung, Sicherungskopien, Ausweichsysteme usw.).

Zu den einzelnen Massnahmen wird angegeben,

a) wie sie die Risiken oder die möglichen Negativfolgen verringern;
b) was sie kosten;
c) in welchen Schritten und Fristen sie umgesetzt werden sollen.

Umsetzung

§ 11. Die Sicherheitsmassnahmen und der Zeitplan ihrer Umsetzung werden im Entscheid über die Neu- oder Ersatzbeschaffung von Informatiksystemen und -anwendungen festgelegt.

Sind Amtsstellen für Beschaffungen zuständig, bleibt die Zustimmung gemäss § 4 Abs. 2 vorbehalten.

Instruktion des Personals

§ 12. Die Amtsstellen informieren die Mitarbeitenden über die Sicherheitsmassnahmen, die sie zu beachten haben.

Sie sorgen für die nötige Ausbildung.

## IV. Datenbearbeitung ausserhalb der Amtsstelle

Zusammenarbeit mehrerer Amtsstellen

§ 13. Wenn eine Amtsstelle Daten durch andere Amtsstellen bearbeiten lässt oder sie mit diesen austauscht, werden die Sicherheitsstufen und -massnahmen sowie die Verantwortlichkeiten bei der Umsetzung gemeinsam festgelegt.

Dasselbe gilt bei einer Zusammenarbeit mit zürcherischen Gemeinden.

Zusammenarbeit mit Dritten

§ 14. Wenn eine Amtsstelle Daten durch Stellen, welche dieser Verordnung nicht unterstehen, bearbeiten lässt, wird im Zusammenarbeitsvertrag vereinbart, welche Massnahmen der Beauftragte zu treffen hat und wie ihre Einhaltung kontrolliert wird.

Datenaustausch über öffentliche Netze

§ 15. Der Datenaustausch über öffentliche Netze ist nur über gesicherte Zugangspunkte zulässig.

Als öffentlich gelten alle Netze ausserhalb des kantonsinternen Netzes (KZH-Netz), insbesondere Anschlüsse an das Netz der Kantonsverwaltungen (KOMBV-KTV), Informationsverbreitung über Internet und Verbindungen zu Herstellern und Dienstleistungsanbietern.

Der Zugriff von aussen auf das kantonsinterne Netz muss über die vom Netzwerkbetreiber bereitgestellten gesicherten Netzwerkübergänge erfolgen. Der Netzwerkbetreiber kann Ausnahmen bewilligen.

Informatikarbeitsplätze ausserhalb der Verwaltung

§ 16. Die Zulässigkeit der Bearbeitung von Daten ausserhalb der Amtsräume und der Verwendung von Programmen der Verwaltung auf privaten Geräten wird im Massnahmenplan geregelt.

## V. Überprüfung der Sicherheitsmassnahmen

Amtsinterne Überprüfung

§ 17. Die Amtsstellen überprüfen periodisch die Einhaltung und die Angemessenheit der Sicherheitsmassnahmen.

Ändern Aufgaben, Organisation oder eingesetzte Informatiksysteme oder -anwendungen einer Amtsstelle, überprüft sie die Sicherheitsstufen und Schutzziele sowie die Angemessenheit der Sicherheitsmassnahmen.

Kontrolle

§ 18. Die Amtsstellen lassen nach den Weisungen der vorgesetzten Direktion bzw. der Staatskanzlei die Sicherheitsmassnahmen periodisch durch unabhängige interne oder externe Stellen überprüfen.

Die Finanzkontrolle und die oder der Beauftragte für den Datenschutz können in die Berichte Einsicht nehmen.

## VI. Schlussbestimmungen

Richtlinien der AGIK

§ 19. Die Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation (AGIK) erlässt Richtlinien über die Konkretisierung der Schutzziele und legt Mindestanforderungen an die Sicherheitsmassnahmen pro Sicherheitsstufe fest.

Vor ihrem Entscheid holt sie die Stellungnahmen der oder des Beauftragten für den Datenschutz und der Finanzkontrolle ein.

Übergangsbestimmung

§ 20. Für bestehende Informatiksysteme und -anwendungen haben die Amtsstellen innerhalb von zwei Jahren nach Inkrafttreten dieser Verordnung die Risiken zu beurteilen und die Sicherheitsstufen, Schutzziele, Sicherheitsmassnahmen sowie den Zeitplan ihrer Umsetzung festzulegen.

Einfache und kostengünstige Sicherheitsmassnahmen, vor allem solche organisatorischer Art, sind nach Möglichkeit schon vorher umzusetzen.

Inkrafttreten

§ 21. Diese Verordnung tritt am 1. April 1998 in Kraft.

[1] OS 54, 481.