Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 26. Februar 2014

231. Informatiksicherheitsverordnung, Totalrevision, Konzept

A. Ausgangslage

Mit Beschluss Nr. 1955/2008 legte der Regierungsrat die vom Kantonalen IT-Team (KITT) erarbeitete Informatikstrategie als verbindliche Arbeitsgrundlage für die Direktionen des Regierungsrates, die Staatskanzlei und die unselbstständigen Anstalten fest. Das KITT wurde mit der Umsetzung der Informatikstrategie beauftragt. Zusammen mit der Informatikstrategie hat das KITT einen Umsetzungsplan vorgelegt, der die mittelfristigen Vorhaben für die Zielerreichung beschreibt. Dies umfasst die vier voneinander unabhängigen Umsetzungseinheiten Strategische Ausrichtung (UE1), Informatiksicherheit (UE2), Datenmanagement (UE3) und Portal (UE4).

Die Informatiksicherheit (UE2) ist am 13. Oktober 2011 durch das KITT genehmigt worden. Sie umfasst die Erarbeitung einer IT-Sicherheitsorganisation, das Erstellen eines Musterkonzeptes mit Richtlinien für den Aufbau eines Management-Systems für die Informatiksicherheit (ISMS) und die Überarbeitung der Informatiksicherheitsverordnung (ISV). Das Ziel ist eine nachhaltige und flächendeckende Verbesserung der Informatiksicherheit in der kantonalen Verwaltung.

Die ISV gilt nicht nur für die kantonale Verwaltung, sondern auch für die Gemeinden, soweit sie mit der kantonalen Verwaltung, den Bezirksverwaltungen und den unselbstständigen Anstalten gemeinsam Informatiksysteme oder -anwendungen betreiben oder mit ihnen Daten austauschen (Beispiel LEUnet).

Die ISV, die 1997 erlassen wurde, ist vollständig zu überarbeiten. Die Gründe sind vielfältig:

- Sie beruht noch auf dem alten Datenschutzgesetz vom 6. Juni 1993. Das heute geltende Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG) macht neue Vorgaben für die Informatiksicherheit.
- Es sind die Bestimmungen des 1999 erlassenen Gesetzes über die Auslagerung von Informatikdienstleistungen zu berücksichtigen, das ebenfalls Einfluss auf die Informatiksicherheit hat.
- Der Regierungsrat hat dem KITT bei der Umsetzung der Informatikstrategie den Auftrag erteilt, Verantwortlichkeiten und Organisation der Informatiksicherheit klar zu regeln. In der geltenden ISV fehlen solche Regelungen weitgehend.

– Der Geltungsbereich der ISV ist zu eng gezogen; ob die festgelegte Geltung auch für Gemeinden einer näheren Begutachtung standhält, ist fraglich.
– Seit 1997 haben sich die Kenntnisse und Erfahrungen über einige der zu regelnden Gebiete stark gefestigt. So ist etwa der Regelungsbereich der Risikoerkennung, -bewertung und -bewältigung neu zu definieren.
– In der Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 sind Bereiche definiert, die sachgerechter in die ISV bzw. in die Personalgesetzgebung gehören. Betreffend den Personalbereich, ist nach Vorliegen der totalrevidierten ISV eine Überarbeitung der Regelungen zu prüfen. Langfristig soll damit die Internet-Verordnung ersetzt werden können.

B. Ziel der neuen Informatiksicherheitsverordnung

Die ISV soll insbesondere auf dem Hintergrund folgender Ansprüche revidiert werden:
– Es soll eine neue Grundlage für alle informatiksicherheitsrelevanten Regelungen im Kanton geschaffen werden.
– Der Geltungsbereich soll klar umschrieben werden. Betroffene Körperschaften (Gemeinden, Spitäler, Hochschulen, Gerichte usw.) sind in den Überarbeitungsprozess einzubeziehen.
– Die mit der Informatiksicherheit zusammenhängenden Regeln aus der Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 sind in eine neue ISV zu integrieren.
– Die wichtigsten Vorgaben aus dem Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 sind zu berücksichtigen.

C. Struktur und inhaltliche Eckpunkte der neuen Informatiksicherheitsverordnung

Die neue ISV gliedert sich in folgende vier Hauptpunkte:

a) Allgemeine Bestimmungen

Unter den allgemeinen Bestimmungen sind Geltungsbereich und Grundsätze der Informatiksicherheit zu definieren.

b) Organisation der Informatiksicherheit

Unter der Organisation sind die Kompetenzen und die Verantwortung kantonsweit festzuhalten und die möglichen Ansprechstellen bezüglich IT-sicherheitsrelevanter Fragen festzulegen. Zudem ist die Koordination mit den weiteren Körperschaften (z. B. Gemeinden, Spitäler) zu regeln.

c) Informatiksicherheits-Management

Zum Informatiksicherheits-Management gehören insbesondere folgende Gesichtspunkte:

- Werte-Management (Umgang mit Daten und Dokumenten; Verantwortung, Klassierung);
- Risiko-Management (Ermittlung des Schutzbedarfs, Auditierung von Leistungserbringern, Verantwortung des Auftraggebers usw.);
- Umgang mit persönlichen Daten und Daten der öffentlichen Hand;
- Sicherheit beim Personal (vor, während, nach der Anstellung);
- Physische und umgebungsbezogene Sicherheit (z. B. Zutritt durch internes und externes Personal, Schutz gegen externe Umgebungsrisiken usw.);
- Kommunikations- und Betriebssicherheit (z. B. Dokumentation, Change Management, Service-Dienstleistungen Dritte, Netzwerk-Sicherheit, Datensicherung, Cloud-Sicherheit);
- Sicherheitstechnische Gesichtspunkte von Social Media, Internet-Angeboten usw.;
- Zugriffskontrolle (auf Netz, Betriebssystem, Applikationen, Daten, Mobile Geräte und Telearbeit);
- Systemerwerb, -entwicklung und -wartung; eingeschlossen Fragen der Abgrenzung Privatbeschaffung, Beschaffung durch das öffentliche Organ (BYOD);
- Management von Vorfällen bezüglich Informatiksicherheit (mit Schwergewicht auf technische Gesichtspunkte);
- Sicherstellung des Geschäftsbetriebs (z. B. Notfallkonzept);
- Einhaltung der Verpflichtungen von Policies, Standards und Technik.

d) Informatiksicherheits-Controlling

Dieser Bereich soll insbesondere folgende Fragen beantworten: Wer überprüft die Sicherheitsmassnahmen, die Zuordnung sowie die Wahrnehmung von Verantwortung und Kompetenzen?

D. Erforderliche Mittel

Externe Mittel

Zur Unterstützung der juristischen Arbeiten soll auf externe Unterstützung zugegriffen werden. Die externen Kosten werden auf rund Fr. 20 000 geschätzt und sind im Budget der KITT-Geschäftsstelle eingestellt.

E. Zeitplan

Nach § 10 der KITT-Verordnung vom 14. Dezember 2005 holt der KITT-Vorsitzende bei Vorhaben von grösserer Tragweite und solchen, die der Genehmigung des Regierungsrates bedürfen, vor der Beschlussfassung eine Stellungnahme der Generalsekretärenkonferenz ein. Diese hat von der beabsichtigten Überarbeitung der Informatiksicherheitsverordnung zustimmend Kenntnis genommen.

Nach der Verabschiedung des vorliegenden Konzeptes durch den Regierungsrat soll bis zum 4. Quartal 2014 ein Verordnungsentwurf ausgearbeitet werden, zu dem im 1. Quartal 2015 ein Vernehmlassungsverfahren durchzuführen sein wird. Der überarbeitete Verordnungsentwurf soll im 2. Quartal 2015 vorliegen, sodass der Regierungsrat die neue ISV im 3. Quartal 2015 verabschieden kann.

F. Projektorganisation für die Erarbeitung der neuen Informatiksicherheitsverordnung

Der Verordnungsentwurf für die neue ISV wird unter der Federführung der Finanzdirektion ausgearbeitet. Die Projektleitung liegt bei der KITT-Geschäftsstelle. In der Arbeitsgruppe sollen Fachleute aus Gemeinden, Spitälern, Universität und Fachhochschulen, Gerichten, des Datenschutzbeauftragten und dem KITT vertreten sein.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Finanzdirektion wird beauftragt, dem Regierungsrat bis Ende 4. Quartal 2014 auf der Grundlage des vorliegenden Konzepts einen Entwurf für eine revidierte Informatiksicherheitsverordnung (Vernehmlassungsvorlage) zu unterbreiten.

II. Mitteilung an die Direktionen des Regierungsrates und die Staatskanzlei.

Vor dem Regierungsrat
Der Staatsschreiber:

Husi