Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 3. September 2019

795. Allgemeine Informationssicherheitsrichtlinie (AISR) (Erlass)

Das Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4) verpflichtet die öffentlichen Organe unter dem Titel «Informationssicherheit», Informationen durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7 Abs. 1 IDG). Diese Massnahmen dienen den Schutzzielen Vertraulichkeit, Unversehrtheit, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit (vgl. § 7 Abs. 2 IDG). Sie richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik (§ 7 Abs. 3 IDG).

Mit Beschluss Nr. 1229/2016 ermächtigte der Regierungsrat die Direktion der Justiz und des Innern zur Durchführung einer Vernehmlassung zum Entwurf einer Verordnung über die Informationsverwaltung und -sicherheit. In der Vernehmlassung wurden Umfang und Ausgestaltung der Verordnung mehrheitlich positiv beurteilt. Zugleich bemängelten jedoch vereinzelte Teilnehmende, insbesondere der Datenschutzbeauftragte, die deutliche Verminderung der Regelungstiefe im Bereich der Informationssicherheit. Der Regierungsrat trägt beiden Rückmeldungen Rechnung: Zum einen hält er an einer übersichtlichen, auf das Wesentliche beschränkten und allgemein verständlichen Verordnungsregelung fest (vgl. RRB Nr. 794/2019). Zum anderen führt er diese Regelung mit einer Allgemeinen Informationssicherheitsrichtlinie (AISR) für die kantonale Verwaltung (d. h. die Direktionen, die Staatskanzlei, die Bezirksverwaltung und die unselbstständigen Anstalten) näher aus. Dieses zweistufige Vorgehen sorgt für verbindliche Vorgaben und gewährleistet gleichzeitig die nötige Flexibilität für Anpassungen an technische und organisatorische Änderungen.

Entsprechend der neuen Verordnung über die Informationsverwaltung und -sicherheit bezieht sich die AISR nicht nur auf die Sicherheit im Bereich der Informations- und Kommunikationstechnologie (IKT), sondern ganz allgemein auf die Informationssicherheit. Sie erstreckt sich damit über die elektronische Bearbeitung von Informationen hinaus auf die papierförmige und mündliche Bearbeitung und umfasst auch die Gebäude- und Gerätesicherheit sowie die Zuverlässigkeit des Personals. Die IKT-Sicherheit bildet jedoch eindeutig den wichtigsten Gegenstand der Richtlinie.

Die AISR legt in Anlehnung an international anerkannte Standards die Grundsätze zur Wahrung der Informationssicherheit in der kantonalen Verwaltung sowie die inhaltlichen Grundzüge der untergeordneten Regelungen fest. Sie regelt zudem den Aufbau des Informationssicherheits-Managementsystems (ISMS) und die Organisation der Informationssicherheit. Im Bereich der IKT-Sicherheit greift sie dafür in erster Linie auf das Amt für Informatik und auf die bestehende Fachgruppe IKT-Sicherheit zurück, der die IKT-Sicherheitsbeauftragten des Kantons, der Direktionen und der Staatskanzlei angehören. Die Abstimmung der Regelungen über die gesamte kantonale Verwaltung hinweg sowie zwischen dem IKT-Bereich und den übrigen Bereichen wird durch das Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) sichergestellt.

Auf der Grundlage der AISR sollen für verschiedene Regelungsbereiche Besondere Informationssicherheitsrichtlinien erlassen werden, welche die Ziele und Grundsätze der AISR mit Schlüsselanforderungen ausführen. Von den Besonderen Informationssicherheitsrichtlinien sollen diejenigen mit einem nahen Bezug zum IKT-Bereich spätestens auf Mitte 2020 und die übrigen spätestens auf Mitte 2021 in Kraft gesetzt werden. Die Richtlinien können ihrerseits Umsetzungsfristen von bis zu zwei Jahren vorsehen. Gestützt auf die AISR und die Besonderen Informationssicherheitsrichtlinien sollen sodann die nötigen Basiskonfigurationen, Verfahren und Prozesse festgelegt werden. Zusammen werden diese Regelungen das ISMS der kantonalen Verwaltung bilden. Die AISR wird damit als formeller Rahmen die wichtigsten technischen, betrieblichen und organisatorischen Massnahmen zum Schutz von Informationen in einem einzigen, einheitlichen Regelwerk zusammenführen.

Die Verantwortung für die Umsetzung dieser Regelungen wird bei den Direktionen, der Staatskanzlei, der Bezirksverwaltung und den unselbstständigen Anstalten liegen. Damit diese Umsetzung fachgerecht erfolgen kann, werden Schulungsmassnahmen, insbesondere für das höhere Kader, festgelegt werden, die in einem angemessenen Umfang obligatorisch sein werden.

Ziel dieses Regelwerks ist es, die Informationssicherheit in der gesamten kantonalen Verwaltung nachhaltig und wirtschaftlich zu verbessern und ein durchgehend risikoadäquates Sicherheitsniveau zu erreichen. Dies soll insbesondere der Gefahr entgegenwirken, dass sich Angriffe und Bedrohungen auf elektronischem Weg innerhalb der kantonalen Verwaltung ausbreiten können, und dadurch das Vertrauen in die Informationssicherheit fördern.

Gemäss RRB Nr. 392/2018 berät das SDI Anträge an den Regierungsrat, welche die Umsetzung der Strategie Digitale Verwaltung zum Gegenstand haben. Das SDI hat den Gegenstand dieses Beschlusses und des zugrunde liegenden Antrags der Finanzdirektion am 12. Dezember 2018, am 8. März 2019 und am 15. Mai 2019 vorberaten.

Auf Antrag der Finanzdirektion

b e s c h l i e s s t d e r R e g i e r u n g s r a t :

I. Es wird eine Allgemeine Informationssicherheitsrichtlinie erlassen.

II. Die Richtlinie tritt gleichzeitig mit der Verordnung über die Informationsverwaltung und -sicherheit in Kraft.

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

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli