

Verordnung über die Informationsverwaltung und -sicherheit

(vom 3. September 2019)

Der Regierungsrat beschliesst:

I. Es wird eine Verordnung über die Informationsverwaltung und -sicherheit erlassen.

II. Die Archivverordnung vom 9. Dezember 1998 wird geändert.

III. Die Informatiksicherheitsverordnung vom 17. Dezember 1997 wird aufgehoben.

IV. Die neue Verordnung und die Verordnungsänderung treten am 1. Januar 2020 in Kraft. Die Informatiksicherheitsverordnung vom 17. Dezember 1997 wird auf dieses Datum aufgehoben. Wird ein Rechtsmittel ergriffen, wird über die Inkraftsetzung und die Aufhebung erneut entschieden.

V. Gegen die neue Verordnung und die Verordnungsänderung sowie Dispositiv III und IV kann innert 30 Tagen, von der Veröffentlichung an gerechnet, beim Verwaltungsgericht des Kantons Zürich Beschwerde erhoben werden. Die Beschwerdeschrift muss einen Antrag und dessen Begründung enthalten.

VI. Veröffentlichung dieses Beschlusses, der Verordnung, der Verordnungsänderung und der Begründung im Amtsblatt.

Im Namen des Regierungsrates

Die Präsidentin:	Die Staatsschreiberin:
Carmen Walker Späh	Kathrin Arioli

Verordnung über die Informationsverwaltung und -sicherheit (IVSV)

(vom 3. September 2019)

Der Regierungsrat,

gestützt auf §§ 5 Abs. 4 und 13 Abs. 2 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG),

beschliesst:

A. Geltungsbereich

§ 1. Diese Verordnung regelt die Verwaltung und den Schutz von Informationen der öffentlichen Organe von Kanton und Gemeinden.

B. Ordnungssystem und Dossiers

Ordnungs-
system

§ 2. Das öffentliche Organ verwaltet seine Geschäftsfälle mit einem Ordnungssystem, das eine eindeutige Zuordnung und eine zielgerichtete Suche von Informationen ermöglicht.

Dossiers

§ 3. ¹ Das öffentliche Organ legt alle für die Bearbeitung und die Nachvollziehbarkeit eines Geschäftsfalls notwendigen Informationen in einem Dossier ab.

² Auf Informationen, die aus technischen, organisatorischen oder rechtlichen Gründen gesondert abgelegt werden, wird im Dossier verwiesen.

Federführung

§ 4. ¹ Das öffentliche Organ bezeichnet für jeden Geschäftsfall eine federführende Stelle.

² Diese ist für die Vollständigkeit des Dossiers verantwortlich.

Metadaten

§ 5. ¹ Dossiers werden mit Informationen versehen, die für die Bearbeitung und die Zuordnung eines Geschäftsfalls sowie für den Schutz der dazugehörigen Informationen nötig sind (Metadaten).

² Sie enthalten insbesondere folgende Metadaten:

- a. Titel des Geschäftsfalls,
- b. Eröffnungs- und Abschlussdatum,
- c. federführende Stelle.

§ 6. ¹ Ist ein Geschäftsfall beendet, überprüft die federführende Stelle die Vollständigkeit des Dossiers und schliesst es ab. Dossierabschluss

² Sie kann Informationen, die für die Nachvollziehbarkeit des Geschäftsfalls nicht notwendig sind, entfernen.

C. Informationsträger

§ 7. ¹ Das öffentliche Organ legt fest, in welcher Form es seine Dossiers führt. Es führt die Dossiers in elektronischer Form, soweit dies möglich und wirtschaftlich ist. Im Übrigen führt es die Dossiers in physischer Form oder aus besonderen Gründen in gemischter Form. Wahl des Informations-trägers

² Es legt zudem fest:

- a. für Dossiers in elektronischer Form: den Umgang mit physischen Informationen, insbesondere solchen, die zur Wahrung der Rechtswirksamkeit oder zu Beweis Zwecken im Original aufbewahrt werden müssen,
- b. für Dossiers in physischer Form: den Umgang mit elektronischen Informationen.

³ Führt das öffentliche Organ seine Dossiers nicht ausschliesslich in elektronischer Form, erstattet es der vorgesetzten Stelle oder der Aufsichtsbehörde jährlich Bericht über die Gründe.

§ 8. ¹ Führt ein öffentliches Organ neue technische Mittel, insbesondere neue Informationsverwaltungssysteme, ein, stellt es sicher, dass die vorhandenen Informationen und Metadaten weiter verwendet werden können. Technische Mittel

² Es verwendet technische Mittel, welche die Übertragung der verwalteten Informationen in archivtaugliche Formate ermöglichen.

D. Anbietungspflicht und Archivierung

§ 9. ¹ Das öffentliche Organ sondert Dossiers aus, wenn Anbietungspflicht

- a. ihre Aufbewahrungsfrist abgelaufen ist,
- b. die entsprechende öffentliche Aufgabe dahingefallen ist.

² Es bietet die ausgesonderten Dossiers zusammen mit den dazugehörigen Metadaten dem zuständigen Archiv an und liefert die vom Archiv ausgewählten Dossiers ab.

³ Es vernichtet oder löscht unwiederbringlich:

- a. die vom Archiv nicht übernommenen Dossiers,
- b. Doppel der dem Archiv abgelieferten Informationen.

⁴ Archivwürdige Dossiers, die das Archiv aus Kapazitätsgründen nicht sofort übernehmen kann, bewahrt das öffentliche Organ weiter auf.

Übrige Pflichten des öffentlichen Organs	§ 10. Das öffentliche Organ
	a. gewährt dem Archiv Zugang zu seinen Informationen, soweit dies für dessen Aufgabenerfüllung notwendig ist,
	b. hört das Archiv bei Projekten zur elektronischen Informationsverwaltung an.
Weisungsrecht	§ 11. Das Archiv kann für die Anbietung und die Übernahme von Informationen Weisungen erlassen.

E. Informationssicherheit

Zuständigkeit	§ 12. ¹ Die federführende Stelle beurteilt die Risiken und den Schutzbedarf für die von ihr verwalteten Informationen. Sie weist diese einer der vom Regierungsrat festgelegten Schutzstufen zu.
	² Das öffentliche Organ legt gestützt darauf in einem Plan angemessene Massnahmen zum Schutz der Informationen fest. Es gibt dazu die Wirkung, die Kosten und die Termine an.
Massnahmen	§ 13. Zur Erreichung der Schutzziele gemäss § 7 Abs. 2 IDG prüft das öffentliche Organ insbesondere folgende Massnahmen:
	a. für das Schutzziel Vertraulichkeit: die Definition und Vergabe restriktiver Berechtigungen, die Verschlüsselung sowie die Anonymisierung bei der Übermittlung,
	b. für das Schutzziel Unversehrtheit: die Verwendung alterungsbeständiger Informationsträger und deren sichere Aufbewahrung,
	c. für das Schutzziel Verfügbarkeit: den Aufbau von Redundanzen sowie die Umsetzung von Vorsorgemassnahmen für Notfälle und Krisenlagen,
	d. für das Schutzziel Zurechenbarkeit: die Verwendung digitaler Zertifikate und Signaturen,

- e. für das Schutzziel Nachvollziehbarkeit: die Protokollierung und Überwachung von Zugriffen und Änderungen,
- f. für alle Schutzziele: Personensicherheitsprüfungen sowie die Sensibilisierung der Mitarbeitenden im sicheren Umgang mit Informationen.

F. Qualitätssicherung

§ 14. ¹ Das öffentliche Organ stellt die Einhaltung dieser Verordnung durch seine Verwaltungseinheiten sicher. Überprüfung

² Es überprüft regelmässig die Einhaltung der Verordnung und die Zweckmässigkeit der getroffenen Massnahmen zum Schutz der Informationen. Werden die Schutzziele gemäss § 7 Abs. 2 IDG nicht mehr erreicht, passt es die Massnahmen an.

³ Es dokumentiert die Ergebnisse der Überprüfung und die Anpassung der Massnahmen.

§ 15. Beauftragt das öffentliche Organ Dritte mit der Informationsbearbeitung, sorgt es dafür, dass die Vorgaben dieser Verordnung eingehalten werden. Informationsbearbeitung durch Dritte

Archivverordnung

(Änderung vom 3. September 2019)

Der Regierungsrat beschliesst:

Die Archivverordnung vom 9. Dezember 1998 wird wie folgt geändert:

Titel nach § 6:

II. Ablieferungspflicht für Amtsdruckschriften

§§ 7–10 werden aufgehoben.

Marginalie zu § 10 a wird aufgehoben.

§§ 15 und 16 werden aufgehoben.

Begründung

1. Ausgangslage

Mit Beschluss Nr. 1189/2012 beauftragte der Regierungsrat die Staatskanzlei, im Rahmen eines direktionsübergreifenden Projekts in Zusammenarbeit mit den Direktionen und namentlich mit dem Staatsarchiv abzuklären, ob und in welcher Form Regelungen für die Schriftgutverwaltung und insbesondere für elektronisch geführte Akten geschaffen werden sollen. Die auf dieser Grundlage gebildete direktionsübergreifende Arbeitsgruppe kam zum Schluss, es sei entsprechender Regelungsbedarf vorhanden, und empfahl dem Regierungsrat unter anderem, die Schriftgutverwaltung nach dem anerkannten Regelungsrahmen des Standards ISO-Norm 15489 mit dafür geeigneten Regelungen zu gestalten.

Der Regierungsrat beauftragte daraufhin mit Beschluss Nr. 538/2014 das Staatsarchiv, einen Entwurf für konkrete Regelungen zur Schriftgutverwaltung zu erarbeiten und mit Blick auf den Übergang zur elektronischen Aktenführung eine dafür geeignete Regelungsform vorzuschlagen. Die Arbeitsgruppe mit Vertretungen des Staatsarchivs und

der Staatskanzlei erarbeitete in der Folge einen Entwurf für Regelungen über die Informationsverwaltung *in der kantonalen Verwaltung* und unterbreitete diesen am 23. April 2015 den Direktionen und der Staatskanzlei, dem Datenschutzbeauftragten sowie dem Kantonalen IT-Team (KITT) zur Vernehmlassung. Den Teilnehmenden der Vernehmlassung wurde gleichzeitig die Frage nach der geeigneten Regelungsebene gestellt (Gesetz, Verordnung, Richtlinie, Empfehlung).

Parallel zur Erarbeitung von Regelungen zur Informationsverwaltung fand die Überarbeitung der Informatiksicherheitsverordnung (LS 170.8) statt. Mit Beschluss Nr. 231/2014 beauftragte der Regierungsrat die Finanzdirektion, einen Entwurf für eine revidierte Informatiksicherheitsverordnung zu erarbeiten. Die Projektleitung lag bei der KITT-Geschäftsstelle. Die Arbeitsgruppe bestand aus Vertretungen der Gemeinden, Spitäler, Universität, Fachhochschulen und Gerichte sowie des Datenschutzbeauftragten, der Finanzkontrolle und des KITT. Die erarbeitete Vorlage wurde in Anlehnung an die Terminologie beim Bund nicht mehr Informatiksicherheitsverordnung, sondern Informationssicherheitsverordnung genannt. Auf der Grundlage von RRB Nr. 400/2015 wurde dieser Entwurf am 1. Juni 2015 den öffentlichen Organen von Kanton und Gemeinden zur Vernehmlassung vorgelegt.

Die Resultate der beiden Vernehmlassungen (Regelungen Informationsverwaltung und Informationssicherheitsverordnung) lagen im Herbst 2015 praktisch gleichzeitig vor. Die entsprechenden Auswertungen zeigten in beiden Fällen die Notwendigkeit einer Straffung sowie einer verstärkten Abstimmung oder einer Zusammenlegung der beiden Regelungsvorhaben.

Entsprechend erteilte die Vorsteherin der Direktion der Justiz und des Innern mit Zustimmung der Finanzdirektion und der Staatskanzlei dem Staatsarchiv den Auftrag, einen gemeinsamen Regelungsentwurf zu den Themen Informationsverwaltung und Informationssicherheit zu formulieren und gleichzeitig abzuklären, inwieweit spezifischer Regelungsbedarf zu Informatiksicherheit Teil dieses Entwurfs sein oder separat geregelt werden solle.

2. Regelungsbedarf

Im April 2016 nahm eine Arbeitsgruppe, in der die Generalsekretariate der Direktion der Justiz und des Innern sowie der Finanzdirektion, die Staatskanzlei, das Staatsarchiv und die KITT-Geschäftsstelle vertreten waren, die Arbeit auf und überprüfte sämtliche ursprünglich zur Regelung vorgeschlagenen Punkte noch einmal gründlich auf ihre Regelungswürdigkeit. Auf dieser Grundlage entschied sich die Arbeits-

gruppe dafür, einen gemeinsamen Erlass zur Informationsverwaltung und zur Informationssicherheit auf der Stufe Verordnung vorzuschlagen, der für alle öffentlichen Organe von Kanton und Gemeinden gültig sein soll.

Dabei handelt es sich im Wesentlichen um Ausführungsbestimmungen zu den §§ 5 und 7 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4), die den öffentlichen Organen insbesondere vorschreiben, ihre Informationen so zu verwalten, dass das Verwaltungshandeln nachvollziehbar und die Rechenschaftsfähigkeit gewährleistet ist, sowie ihre Informationen durch angemessene organisatorische und technische Massnahmen zu schützen. Die verwendeten Begriffe sind auf die Bestimmungen des IDG abgestimmt.

Auch wenn sich jedes Organ selber so organisieren könnte, dass die erwähnten Anforderungen erfüllt sind, ist die Festlegung der Prinzipien einer ordnungsgemässen und effizienten Informationsverwaltung und -sicherheit aus mehreren Gründen sinnvoll:

1. Ein einheitliches Verständnis in zentralen Fragen unterstützt die organisationsübergreifende Zusammenarbeit.
2. Der Austausch von Unterlagen, insbesondere bei der elektronischen Informationsverwaltung, wird erleichtert.
3. Bereits vorhandenes Wissen und bewährte Methoden können auf einfache Art weitergegeben werden.

Bei einem Teil der vorgeschlagenen Regelungspunkte handelt es sich nicht um neues Recht, sondern um eine Überführung und Modernisierung bereits geltender Bestimmungen. So regelt bisher der zweite Abschnitt der Archivverordnung (LS 170.61) unter dem Titel «Grundsätze für die Aktenablage der öffentlichen Organe» vorwiegend Punkte, die nicht die Archivierung, sondern die Informationsverwaltung in den öffentlichen Organen betreffen. Entsprechend gehören solche Regelungen (§§ 7–10 Archivverordnung) thematisch nicht in das Archivrecht und sollen deshalb in die neue Verordnung übergeführt werden. Ebenso soll mit Rechten der Archive verfahren werden, die bereits vor der Ablieferung der Informationen an das zuständige Archiv in die Informationsverwaltung der öffentlichen Organe eingreifen (§§ 15 und 16 Archivverordnung).

Auf diese Weise können die Regelungen über den Umgang öffentlicher Organe mit Informationen von jenen über die Archivierung klarer getrennt werden. Die Verwaltung und der Schutz von Informationen zu laufenden und zu abgeschlossenen Geschäftsfällen während der Aufbewahrungsfrist werden in der Verordnung über die Informationsverwaltung und -sicherheit geregelt, die Archivierung von Informationen in der Archivverordnung.

Mit der Verordnung über die Informationsverwaltung und -sicherheit (IVSV) soll nicht ein umfassendes technisches Regelwerk für Fachpersonen geschaffen werden. Das Ziel ist vielmehr eine übersichtliche, auf das Wesentliche beschränkte und allgemein verständliche Regelung, die für die Mitarbeitenden des Kantons und der Gemeinden gleichermaßen akzeptabel und praktikabel sein soll. Technische Details können so in verwaltungsinternen Weisungen und Richtlinien geregelt werden. Dieser offene Regelungsansatz ermöglicht es, die rechtlichen und tatsächlichen Unterschiede zwischen den verschiedenen öffentlichen Organen zu berücksichtigen und die Regeln zur Informationsverwaltung und -sicherheit jeweils auf das konkrete Umfeld abzustimmen. Die öffentlichen Organe sollen die dafür nötige Organisationsfreiheit behalten (z.B. bei der Bezeichnung der zuständigen Stellen und Personen, der Zusammenarbeit untereinander und der Klassifizierung von Informationen). Es soll ihnen zudem freistehen, für ihren eigenen Bereich strengere Regeln aufzustellen. Dieser offene Ansatz ermöglicht es auch, bei Bedarf rasch auf Entwicklungen im technischen Bereich, in der Bedrohungslage oder im Datenschutzrecht zu reagieren.

3. Ergebnisse der Vernehmlassung

Mit Beschluss Nr. 1229/2016 ermächtigte der Regierungsrat die Direktion der Justiz und des Innern zur Durchführung eines Vernehmlassungsverfahrens. Zur Stellungnahme eingeladen wurden die Direktionen des Regierungsrates und die Staatskanzlei, die Finanzkontrolle, der Ombudsmann, der Datenschutzbeauftragte, die kantonalen Gerichte, die selbstständigen öffentlich-rechtlichen Anstalten, die verschiedenen Gemeindeverbände, die Städte Zürich und Winterthur sowie weitere Verbände und Vereinigungen öffentlicher Organe. Insgesamt gingen 25 Stellungnahmen ein.

Grundsätzlich wurde der Verordnungsentwurf begrüsst, insbesondere die Zusammenlegung der Regelungen zur Informationsverwaltung mit jenen zur Informationssicherheit. Positiv beurteilt wurden mehrheitlich auch Umfang und Ausgestaltung der Verordnung. Mehrfach wurde hervorgehoben, sie schaffe einerseits ein einheitliches Verständnis der zentralen Fragestellungen, lasse den öffentlichen Organen andererseits aber genügend Handlungsspielraum, um die notwendigen Massnahmen angepasst an die zu erfüllenden Aufgaben umzusetzen.

Bemängelt wurde vereinzelt, insbesondere aber vom Datenschutzbeauftragten, die Verminderung der Regelungstiefe im Bereich der Informationssicherheit. Die starke Straffung der Bestimmungen zur Informationssicherheit ist allerdings eine direkte Folge der Vernehmlassung

zum ursprünglich deutlich detaillierteren Entwurf für eine Informationssicherheitsverordnung. Damals wurde mehrheitlich kritisiert, die Regelungen griffen viel zu stark in die Organisationsautonomie der öffentlichen Organe ein. Die Bedenken einer Regulierungslücke im Bereich der Informationssicherheit wurden insofern ernst genommen, als gleichzeitig mit dem Erlass der IVSV eine Allgemeine Informationssicherheitsrichtlinie für die kantonale Verwaltung mit entsprechenden Ausführungsbestimmungen erlassen wird (RRB Nr. 795/2019). Dieses zweistufige Vorgehen sorgt einerseits für verbindliche Vorgaben, gewährleistet andererseits aber die nötige Flexibilität für Anpassungen an technische und organisatorische Änderungen.

Den Bedenken des Datenschutzbeauftragten wurde zudem durch eine Überarbeitung von § 12 (Informationssicherheit) Rechnung getragen. Neu werden die federführenden Stellen zu einer Beurteilung der Risiken und des Schutzbedarfs verpflichtet. Um der Gefahr unterschiedlicher Modelle für Schutzeinstufungen von Daten und Informationssystemen zu begegnen, werden die in der kantonalen Verwaltung verwendeten Schutzstufen für verbindlich erklärt. Gestützt auf die Beurteilung von Risiken und Schutzbedarf müssen die öffentlichen Organe einen Massnahmenplan festlegen sowie Wirkung, Kosten und Termine dokumentieren.

Überdies wurde in der jüngsten Vernehmlassung teilweise empfohlen, die Entwicklungen im Bereich Datenschutzrecht auf übergeordneter Ebene (EU, Bund, Revision IDG) abzuwarten. Da indessen nicht damit zu rechnen ist, dass diese Entwicklungen die vorliegenden Bestimmungen in grundlegender Weise beeinflussen würden, wird auf einen weiteren Aufschub der bereits seit mehreren Jahren laufenden Arbeiten zur Schaffung von Regelungen zur Informationsverwaltung und -sicherheit verzichtet.

4. Strategie Digitale Verwaltung (RRB Nr. 390/2018)

Das mit der Strategie Digitale Verwaltung eingesetzte Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) stellt die koordinierte Umsetzung der Strategie Digitale Verwaltung sicher. Es hat den vorliegenden Antrag am 15. Mai 2019 zuhanden des Regierungsrates vorgelegt und diesem unter Berücksichtigung der Beratung zugestimmt.

5. Finanzielle Auswirkungen

Die IVSV ist ein Ausführungserlass zu den §§ 5 und 7 IDG. Entsprechend werden keine grundlegend neuen Anforderungen an die Verwaltung und die Sicherheit von Informationen gestellt, die einen grossen Umstellungsaufwand verursachen würden und damit verbunden finanzielle Auswirkungen hätten. Für Organe, die bisher bestimmte, bereits geltende Anforderungen nicht oder nur teilweise erfüllt haben, entstehen vorübergehend gewisse Kosten, die sich mittelfristig durch die bessere Organisation jedoch wieder auszahlen dürften.

6. Regulierungsfolgeabschätzung

Mit der IVSV werden keine Handlungspflichten für Unternehmen im Sinne von § 1 des Gesetzes zur administrativen Entlastung der Unternehmen (LS 930.1) begründet oder verändert. Geregelt werden einzig die Pflichten öffentlicher Organe beim Umgang mit Informationen.

7. Zu den einzelnen Bestimmungen

A. Geltungsbereich

§ 1.

Die Verordnung präzisiert die Grundzüge über die Informationsverwaltung und -sicherheit, die namentlich in den §§ 5 und 7 IDG vorgegeben sind. Aufgrund seiner Vollzugsverordnungskompetenz gemäss Art. 67 Abs. 2 der Kantonsverfassung (LS 101) ist der Regierungsrat berechtigt, die Regelungen des IDG für alle öffentlichen Organe von Kanton und Gemeinden auf Verordnungsstufe zu konkretisieren. § 5 Abs. 4 IDG ist im Sinne einer verfassungskonformen Auslegung so zu verstehen, dass der Regierungsrat zum Erlass einer Verordnungsregelung für die kantonale Verwaltung verpflichtet, zum Erlass einer Verordnungsregelung für die übrigen öffentlichen Organe hingegen nur – aber immerhin – berechtigt ist.

Informationen öffentlicher Organe durchlaufen drei Lebensphasen:

1. Phase: laufende Dossiers zu laufenden Geschäftsfällen,
2. Phase: abgeschlossene Dossiers während der Aufbewahrungsfrist,
3. Phase: archivierte Dossiers.

Die vorliegende Verordnung regelt die ersten beiden Phasen von der Eröffnung eines Dossiers bis zu dessen Abschluss (Laufende Ablage), die Aufbewahrung von Informationen während der Aufbewahrungsfrist (Ruhende Ablage) und schliesslich die Anbietungspflicht an das Archiv bzw. die Vernichtungspflicht für vom Archiv nicht übernommene Dossiers. Die dritte Phase ist in der Archivverordnung geregelt.

B. Ordnungssystem und Dossiers

§ 2. Ordnungssystem

Ein Ordnungssystem (bisher in § 8 Abs. 4 der Archivverordnung «Registaturplan» genannt) ist eine zumeist hierarchische, aufgabenorientierte Struktur, die für alle vorkommenden Geschäftsfälle eine geeignete Ablageposition zur Verfügung stellt. Es erlaubt

- eine zielgerichtete, strukturierte Suche,
- die genaue Zuordnung von Informationen zum jeweiligen Dossier (keine Mehrfachablagen),
- die einfache Bewirtschaftung von Metadaten,
- die langfristige Erhaltung des Entstehungs- und Verwendungszusammenhangs von Informationen,
- die einheitliche Verwaltung unterschiedlicher Informationsträger.

Auf der Grundlage von Geschäftsregeln und zusammen mit den Metadaten wird das Ordnungssystem zu einem eigentlichen Managementsystem für die Informationsverwaltung. Der Detaillierungsgrad des Ordnungssystems ist dem jeweiligen öffentlichen Organ und der Anzahl seiner Aufgaben anzupassen.

Jedes neue Dossier wird bei seiner Eröffnung einer geeigneten Position im Ordnungssystem zugeordnet.

§ 3. Dossiers

Insbesondere um das Transparenzprinzip gemäss § 4 IDG zu erfüllen und um die Nachvollziehbarkeit des Verwaltungshandelns und die Rechenschaftsfähigkeit gemäss § 5 Abs. 1 IDG zu gewährleisten, sind alle Informationen zu einem Geschäftsfall in einem Dossier zu führen. Es darf keine Informationen geben, die ohne Zuordnung zu einem Dossier geführt werden. Ausgenommen sind Dokumente ohne direkte Relevanz für einen Geschäftsfall, beispielsweise Unterlagen von kurzfristiger Bedeutung (Informationen für den gleichen Tag) oder Schreiben Dritter, die lediglich zur Kenntnis genommen werden.

Zur Zuverlässigkeit von Informationen gehört, dass relevante Geschäftsvorgänge aufgezeichnet werden. So sind beispielsweise nur mündlich besprochene Vorgänge, die über den Tag hinaus von Bedeutung sind, in Form von Protokollen oder Telefonnotizen schriftlich festzuhalten.

Neben den üblichen Geschäftsfällen (z. B. Rechtsmittel, Bewilligungen usw.) sind auch Projekte, Objekte, Prozesse oder bestimmte Aufgaben als Geschäftsfälle zu betrachten. Entsprechend werden beispielsweise Dossiers zu IT-Projekten, zu Liegenschaften oder Betrieben geführt.

Aus verschiedenen Gründen müssen bestimmte Informationen separat, also ausserhalb des Dossiers, abgelegt werden, beispielsweise:

- Spezialformate: separate Ablagen für audiovisuelle Medien oder für Überformate (z. B. grossformatige Pläne),
- Informationen oder Unterlagen in Fachanwendungen (z. B. Datenbanken wie SAP usw.),
- handunterzeichnete Dokumente oder Originalurkunden, die zwecks Rechtsgültigkeit auf Papier aufbewahrt werden müssen.

Solche separat abgelegten Dokumente sind im Dossier zu vermerken, oder es sind Geschäftsregeln zu formulieren, welche die allgemeine Nachvollziehbarkeit von (Standard-)Geschäften gewährleisten.

§ 4. Federführung

Die Festlegung der Federführung folgt im öffentlichen Organ zu meist aus einer allgemeinen oder übergeordneten Zuständigkeitsregelung, kann aber auch für jeden Geschäftsfall einzeln erfolgen.

Diese Festlegung entlastet weitere an einem Geschäftsfall mitarbeitende Personen von der Dossierführung. Sie können allenfalls vorhandene Informationen zu einem Geschäftsfall jederzeit vernichten, weil sie durch die Festlegung der Federführung wissen, wer das vollständige Dossier führt.

Arbeiten mehrere öffentliche Organe zusammen (z. B. in Projekten), ist jedes Organ selber dafür verantwortlich, dass der eigene Beitrag zum gesamten Geschäftsfall nachvollziehbar und rechenschaftsfähig dokumentiert ist. Das heisst, dass neben dem federführenden Organ, welches das massgebliche Dossier führt, die mitarbeitenden Organe jeweils eigene Dossiers zum gleichen Geschäftsfall führen, in denen beispielsweise interne Meinungsbildungsprozesse oder die Erarbeitung von Grundlagen dokumentiert sind.

Wenn mehrere Organe am gleichen Geschäftsfall beteiligt sind und ein gemeinsames Dossier führen (z. B. auf einer Kollaborationsplattform), muss mindestens eines der beteiligten Organe zur Führung des massgeblichen Dossiers verpflichtet werden.

§ 5. Metadaten

Neben technischen Metadaten, die beispielsweise von Informationsverwaltungssystemen automatisch vergeben werden, sind Metadaten zum Inhalt und zum Schutzbedarf als beschreibende Merkmale für die systematische, effiziente und sichere Bewirtschaftung der Dossiers wichtig. Entsprechend kann die Vergabe von Metadaten – mit Ausnahme der im Erlassentext genannten – nicht generell-abstrakt festgelegt werden. Sie wird vielmehr von jedem öffentlichen Organ gemäss seinen Aufgaben und Organisationsstrukturen geregelt. Weitere Metadaten können beispielsweise das Aktenzeichen, die Position im Ordnungssystem, den Status eines Geschäftsfalls, Zugangsbestimmungen (sofern diese für das ganze Dossier gleich sind), eine Klassifizierung oder Aufbewahrungsfristen betreffen.

§ 6. Dossierabschluss

Für die Bewirtschaftung eines Dossiers ist dessen Abschluss sehr wichtig. Ab diesem Zeitpunkt beginnt die Aufbewahrungsfrist zu laufen (vgl. z.B. § 5 Abs. 2 IDG), nach deren Ablauf die öffentlichen Organe ihre Informationen dem zuständigen Archiv zur Bewertung anbieten müssen.

Beim Abschluss soll noch einmal die Vollständigkeit des Dossiers überprüft werden, damit die Nachvollziehbarkeit des Geschäftsfalls gewährleistet werden kann. Gleichzeitig können für die Nachvollziehbarkeit des Geschäftsfalls nicht mehr bedeutsame Informationen aus dem Dossier entfernt werden.

C. Informationsträger

§ 7. Wahl des Informationsträgers

Das öffentliche Organ legt in einem Grundsatzentscheid die massgebliche Form seiner Dossiers fest. Eine möglichst grosse Einheitlichkeit der gewählten Informationsträger vermindert Doppelspurigkeiten und erleichtert die Bewirtschaftung der Dossiers. Der Normalfall ist die elektronische Dossierführung. Es muss sichergestellt sein, dass alle für die Nachvollziehbarkeit eines Geschäftsfalls bedeutsamen Dokumente in elektronischer Form im Dossier abgelegt werden. Lassen sich bestimmte Dokumente gar nicht oder nicht mit einem verhältnismässigen Aufwand in elektronische Form bringen (z.B. dreidimensionale Gegenstände oder grossformatige Pläne), wird das Dossier in gemischter Form geführt, wobei im elektronischen Dossier auf die nur physisch vorliegenden Informationen verwiesen wird. Ist die elektronische Dossierführung für ein öffentliches Organ insgesamt oder in Teilen unwirtschaftlich, führt es die Dossiers in physischer Form.

Bei grundsätzlich elektronischer Dossierführung muss festgelegt werden, wie mit in physischer Form vorliegenden Informationen verfahren wird, beispielsweise mittels Regelungen zum Scanning bzw. zu physischen Informationen, die sich nicht digitalisieren lassen. Bestimmte Dokumente (z.B. handunterzeichnete Verträge und andere Originalurkunden) sind zur Wahrung der Rechtswirksamkeit oder zu Beweis Zwecken zusätzlich zur elektronischen Version weiterhin physisch zu führen und aufzubewahren. Für die tägliche Arbeit (z.B. an Sitzungen) wird es (zumindest vorläufig) weiterhin auch physische Doppel der im elektronischen Dossier abgelegten Dokumente geben. Diese müssen aber jederzeit ohne Informationsverlust vernichtet werden können und schliesslich – spätestens am Ende der Aufbewahrungsfrist des Geschäfts – tatsächlich auch datenschutzkonform vernichtet werden.

Bei grundsätzlich physischer Dossierführung muss festgelegt werden, wie mit in elektronischer Form vorliegenden Informationen verfahren wird, beispielsweise durch Vorschriften zum Ausdrucken elektronischer Dokumente bzw. zum Umgang mit elektronischen Dokumenten (wie etwa umfangreichen Excel-Dateien), die sich kaum in eine sinnvolle physische Form bringen lassen.

Um die Umstellung auf eine weitgehend elektronische Informationsverwaltung zu fördern, müssen öffentliche Organe, die ihre Dossiers noch nicht ausschliesslich in elektronischer Form führen, der vorgesetzten Stelle oder der Aufsichtsbehörde jährlich Bericht über die Gründe erstatten. Auf diese Weise erhalten die übergeordneten Organe laufend eine Übersicht über den Stand der Digitalisierung bzw. über die Hindernisse auf dem Weg zur Erreichung dieses Ziels.

§ 8. Technische Mittel

Werden neue technische Mittel zur Verwaltung von Informationen (beispielsweise elektronische Geschäftsverwaltungssysteme oder Fachanwendungen) eingeführt, müssen die in den Vorgängeranwendungen vorhandenen Informationen entweder vollständig übernommen werden können, oder es ist auf andere Art dafür zu sorgen, dass die Informationen samt Metadaten verwendbar bleiben, bis sie dem zuständigen Archiv zur Bewertung und Übernahme angeboten werden können. Das Gleiche gilt auch für technische Mittel im physischen Bereich: So muss etwa gewährleistet sein, dass Filme oder Tonbildschauen abgespielt werden können, bis diese zur Archivierung angeboten werden können. Während der ganzen Zeit ist zudem für die angemessene Sicherheit der Informationen zu sorgen.

Sämtliche in elektronischen Systemen verwalteten Informationen müssen grundsätzlich in archivtaugliche Datenformate exportiert und dem zuständigen Archiv abgeliefert werden können. Werden neue elekt-

ronische Systeme eingeführt, sind sie mit einer archivischen Ablieferungsschnittstelle auszurüsten, die einen strukturierten Export der Informationen in archivtauglichen Formaten erlaubt. Für die Kantonsverwaltung wurde mit RRB Nr. 538/2014 die Schnittstelle gemäss Standard eCH-0160 verbindlich erklärt.

Verfügt eine Verwaltungseinheit über Dossiers mit einer Aufbewahrungsfrist von mehr als zehn Jahren, ist die Umwandlung in ein archivtaugliches Dateiformat bereits vor der Archivierung angezeigt, um die Informationen lesbar zu halten.

D. Anbietungspflicht und Archivierung

§ 9. Anbietungspflicht

Die vorliegenden Regelungen werden von § 10 der Archivverordnung hierher übergeführt, weil sie den Abschluss der Informationsverwaltung bei den öffentlichen Organen betreffen und noch nicht die Archivierung.

Abs. 1: Das öffentliche Organ sondert regelmässig jene Dossiers aus, deren Aufbewahrungsfristen abgelaufen sind. Sofern es keine spezialrechtlichen Bestimmungen gibt, richten sich die Aufbewahrungsfristen nach § 5 Abs. 2 IDG und § 8 Abs. 1 des Archivgesetzes (LS 170.6) und betragen längstens zehn Jahre. Wird eine öffentliche Aufgabe in das Privatrecht übergeführt oder ganz aufgegeben, sind sämtliche bis zu diesem Zeitpunkt entstandenen Dossiers ebenfalls auszusondern (und dem zuständigen Archiv anzubieten, vgl. Abs. 2). Wird eine öffentliche Aufgabe hingegen lediglich einer privatrechtlich organisierten Körperschaft übertragen oder das mit der Erfüllung der öffentlichen Aufgabe betraute Organ in das Zivilrecht übergeführt, ohne dass auch die eigentliche Aufgabe materiell privatisiert wird, bleibt die Anbietungspflicht bestehen und die Aussonderung geschieht weiterhin nach Ablauf der Aufbewahrungsfrist.

Abs. 2: Das öffentliche Organ bietet die ausgesonderten Dossiers gemäss Abs. 1 dem zuständigen Archiv samt den dazugehörigen Metadaten (Verzeichnissen, Registerdaten, Geschäftskontrolldaten usw.) an. Das Archiv bewertet diese gemäss § 8 Abs. 2 des Archivgesetzes und § 6 der Archivverordnung auf ihre Archivwürdigkeit. Das öffentliche Organ sorgt für die Aufbereitung (z.B. Verpackung physischer Akten oder Umwandlung elektronischer Daten in archivtaugliche Formate) und die Übermittlung der archivwürdigen Dossiers und Metadaten in das zuständige Archiv.

Abs. 3: Gemäss § 5 Abs. 3 IDG sind angebotene Informationen, die vom zuständigen Archiv nicht übernommen werden, vom öffentlichen Organ unwiederbringlich zu vernichten. In physischer Form vorliegende Informationen sind zu schreddern oder auf andere Art physisch zu vernichten. Elektronische Informationen müssen mit einer geeigneten Lösungssoftware bearbeitet werden. Lediglich eine Einschränkung des Zugriffs auf die Informationen erfüllt diese Bestimmung nicht. Ebenfalls zu vernichten sind Doppel jener Informationen, die vom zuständigen Archiv übernommen wurden. Nach der Archivierung der Dossiers dürfen folglich nur noch im zuständigen Archiv Informationen zu den entsprechenden Geschäftsfällen vorhanden sein.

Abs. 4 entspricht § 10 Abs. 4 der Archivverordnung.

§§ 10 und 11. Übrige Pflichten des öffentlichen Organs und Weisungsrecht

Die vorliegenden Regelungen werden von den §§ 15 und 16 der Archivverordnung hierher übergeführt, weil sie grösstenteils bereits vor der Übernahme der Informationen in das Archiv in die Informationsverwaltung der öffentlichen Organe eingreifen.

E. Informationssicherheit

§ 12. Zuständigkeit

Das öffentliche Organ ist in seinem Zuständigkeitsbereich für die Einhaltung und Umsetzung der im IDG verankerten Grundsätze im Umgang mit Informationen verantwortlich. Dazu legt es die Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich Informationssicherheit fest.

Das öffentliche Organ regelt selbstständig, wie es die Informationssicherheit verwirklichen will. Es bleibt jedoch – unabhängig von einer Übertragung der Aufgabe an Verwaltungseinheiten, Ämter oder externe Dritte – immer dafür verantwortlich.

In einem ersten Schritt ermittelt das öffentliche Organ die für seine Informationen vorgegebenen Schutzziele. Allgemein gültig sind nach § 7 Abs. 2 lit. a–e IDG die folgenden Schutzziele: Vertraulichkeit, Unversehrtheit, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit. Darüber hinaus können für bestimmte Informationen besondere rechtliche Vorgaben gelten (vgl. dazu beispielsweise das Personalgesetz [LS 177.10], das Gesetz über die Auslagerung von Informatikdienstleistungen [LS 172.71] oder das Archivgesetz).

Die federführende Stelle beurteilt auf dieser Grundlage die Risiken für die von ihr verwalteten Informationen, bestimmt den entsprechenden Schutzbedarf und hält diesen in den Metadaten gemäss § 5 fest. In Anbetracht der übergreifenden Vernetzung vieler öffentlicher Organe ist es sinnvoll, einheitliche und damit vergleichbare Sicherheitseinstufungen zu verwenden. Um dies zu gewährleisten, werden von den öffentlichen Organen von Kanton und Gemeinden die gleichen Schutzstufen verwendet, wie sie vom Regierungsrat für die kantonale Verwaltung festgelegt werden.

Gestützt auf diese Risikobeurteilung und die entsprechende Bestimmung des Schutzbedarfs legt das öffentliche Organ in einem Plan geeignete Massnahmen fest, wobei gemäss § 7 Abs. 3 IDG die Art (Schutzwürdigkeit) der Information, die Art und der Zweck der Verwendung sowie der jeweilige Stand der Technik zu berücksichtigen sind. Es führt zudem Nachweise über die Verminderung von Risiken oder Folgen, über die Kosten und über die (Umsetzungs-)Termine.

Im Rahmen von Projekten und Systemanpassungen hat das öffentliche Organ frühzeitig die Anforderungen an die Informationssicherheit festzulegen und zu berücksichtigen. Die dafür nötigen Aufwendungen sind Teil der Projekt- und Betriebskosten und entsprechend zu budgetieren.

§ 13. Massnahmen

Die Liste der aufgeführten Massnahmen ist nicht abschliessend. Die Massnahmen orientieren sich an allgemein anerkannten internationalen Standards. Zurzeit ist ein Management der Informationssicherheit nach den Normen der ISO-27000-Reihe anzustreben. Insbesondere ist sicherzustellen, dass das Thema als ständiger Prozess wahrgenommen und das Sicherheitsbewusstsein der Mitarbeitenden regelmässig geschult wird.

Sicherheitsmassnahmen sind organisatorischer oder technischer Natur und müssen – unter Berücksichtigung der Gewährleistung von Grundrechten und der Einhaltung gesetzlicher Bestimmungen – entsprechend den betrieblichen und technischen Verhältnissen immer in einem angemessenen wirtschaftlichen Verhältnis zum möglichen Schaden stehen.

Die Informationssicherheit erstreckt sich auf alle Arten von Informationsträgern (Papier, Tonbänder, Filme, elektronische Datenträger usw.).

Neben den üblichen Massnahmen regelt das öffentliche Organ mit entsprechenden Konzepten, wie die Informationssicherheit bei Notfällen und in Krisenlagen sicherzustellen ist, beispielsweise wie bei einem Ausfall von Informatiksystemen vorzugehen ist, der länger als die definierten Verfügbarkeitsanforderungen dauert.

F. Qualitätssicherung

§ 14. Überprüfung

Das öffentliche Organ wählt einen den betrieblichen und technischen Verhältnissen angepassten Überprüfungsrhythmus. Im Bereich der Informationssicherheit empfiehlt es sich, mindestens alle zwei Jahre zu prüfen, ob die Sicherheitsmassnahmen angemessen sind und ob sie umgesetzt werden. Bei veränderter Bedrohungslage ist die Angemessenheit der Sicherheitsmassnahmen umgehend zu überprüfen.

§ 15. Informationsbearbeitung durch Dritte

Die Regelungen betreffend die Bearbeitung von Informationen durch externe Dritte gemäss § 6 IDG sowie § 25 der Verordnung über die Information und den Datenschutz (LS 170.41) gelten auch für die Informationsverwaltung und -sicherheit. Das heisst insbesondere, dass die Verantwortung für die Sicherheit der Informationen beim zuständigen öffentlichen Organ verbleibt.