Verordnung über die Informationssicherheit (ISV)

1. Ausgangslage

Die vorliegende Verordnung ersetzt die bisherige Verordnung zur Informatiksicherheit vom 9. April 2002 (ISV, SG 153.320). Diese Ablösung ist aus zweierlei Gründen notwendig: Einerseits aufgrund des Informations- und Datenschutzgesetzes vom 9. Juni 2010 (IDG, SG 153.260), welches in § 8 klare Vorgaben zur Informationssicherheit enthält und andererseits aufgrund der Tatsache, dass die bestehende ISV aus dem Jahr 2002 stammt und damit den aktuellen Informationssicherheitsvorgaben nicht mehr entspricht.

2. Erläuterungen zu den einzelnen Bestimmungen

§ 1. *Gegenstand und Zweck*

Abs. 1

Informationssicherheit im Sinne dieser Verordnung bezeichnet den Zustand, in dem die beim Einsatz von IKT[1] oder jedem anderen Informationsträger aufgrund von Bedrohungen und Schwachstellen vorhandenen Risiken durch angemessene Massnahmen auf ein tragbares Mass reduziert sind. Nicht jedes Risiko lässt sich in jedem Fall beseitigen. Trotzdem gilt es diese so weit als möglich zu minimieren und anschliessend kontinuierlich zu bewirtschaften (zu managen). Dabei lassen sich Risiken dadurch managen, indem die dafür geeigneten Massnahmen ergriffen werden. Im Bereich von Informationssicherheits-Risiken bietet die Informationssicherheit das dafür notwendige Vorgehenskonzept und sieht die dafür notwendigen Massnahmen vor.

Abs. 2

Der Zweck der Informationssicherheit liegt in system- und technikbezogener Hinsicht in der Gewährleistung und Einhaltung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen und der für deren Bewirtschaftung betriebenen IKT-Anwendungen sowie der Zurechenbarkeit und Nachvollziehbarkeit von im Rahmen dieser Informationen und IKT-Anwendungen vorgenommenen Handlungen. Dabei ist die Vertraulichkeit einer IKT-Anwendung gegeben, wenn die darin enthaltenen Informationen vor unbefugter Kenntnisnahme geschützt sind. Die Verfügbarkeit einer IKT-Anwendung bedeutet dagegen, dass diese über eine uneingeschränkte Funktionalität verfügt. Sie gewährleistet, dass die darin enthaltenen Informationen zu einem bestimmten Zeitpunkt und/oder an einem bestimmten Ort nutzbar sind. Die Integrität einer Informationsanwendung ist gegeben, wenn die darin enthaltenen Informationen vor unbefugten und unberechtigten Veränderungen geschützt sind. Sie ist gewährleistet, wenn nur berechtigte Subjekte (Personen, Systeme oder Funktionen) die Informationen zu berechtigten Zwecken und nachvollziehbar bearbeiten können. Die Zurechenbarkeit und Nachvollziehbarkeit bedeuten schliesslich, dass eine durchgeführte Handlung eindeutig einer Kommunikationspartnerin oder einem Kommunikationspartner zugeordnet sowie auch nachverfolgt werden kann.

[1] IKT = Informations- und Kommunikationstechnologie; IKT-Anwendungen sind z.B. Office Anwendungen, spezifische Fachbereichsanwendungen, E-Mail-Programme, SAP usw.

§ 2. Geltungsbereich

Abs. 1

Die vorliegende Verordnung gilt für Organisationseinheiten des Kantons, wie sie sich weitgehend aus § 3 Abs. 1 lit. a IDG ergeben. Die Gerichte sind aufgrund ihrer Autonomie explizit ausgenommen. In dem bloss auf die Organisationseinheiten des Kantons Bezug genommen wird, sind kommunale Organe ebensowenig von der vorliegenden Regelung betroffen.

Die begriffliche Anlehnung an das IDG erfolgt, weil die vorliegende Verordnung mitunter auf diesem (siehe § 8 Abs. 4 IDG) basiert und es daher wenig sinnvoll wäre, den Begriff der Organisationseinheiten im Rahmen dieser Verordnung anders zu definieren als im IDG. Mit dieser Definition des Geltungsbereichs werden in der vorliegenden Verordnung die selbständigen öffentlich-rechtlichen Anstalten (z.B. die Basler Kantonalbank oder die Basler Verkehrsbetriebe) im Gegensatz zum IDG vom Geltungsbereich ausgenommen. Grund dafür ist, dass sich deren Geschäftstätigkeit teilweise erheblich von der allgemeinem Verwaltungstätigkeit unterscheidet und sich entsprechend ein Bedarf an geschäftsspezifischen und/oder über die vorliegende Verordnung hinausgehenden Regelungen ergeben kann.

Gemäss § 8 Abs. 4 IDG erlässt der Gemeinderat für die kommunale Verwaltung Ausführungsbestimmungen zu § 8 Abs. 1 bis 3 IDG. Dies bedeutet, dass der Gemeinderat für die kommunale Verwaltung ebenfalls für eine den aktuellen datenschutz- und informationsrechtlichen (insbesondere den Anforderungen von § 8 IDG entsprechende) sowie technisch zeitgemässe Informationssicherheit zu sorgen hat. Das heisst aber auch, dass die vorliegende Verordnung nicht auf die kommunale Verwaltung ausgedehnt werden kann. Jedoch können auch diese, wie auch andere dieser Verordnung nicht unterworfene Dritte, die Dienstleistungen des Zentralen Leistungserbringers beziehen (z.B. Anschluss ans DANEBS), sicherheitstechnisch diese Dienstleistung beeinflussen. Damit ist von deren für ihre eigenen Belange zur Anwendung gebrachtem Informationssicherheitssystem auch der Kanton betroffen. Deshalb wird in § 10 Abs. 5 der Zentrale Leistungserbringer verpflichtet dafür zu sorgen, dass an gemeinsame Einrichtungen angeschlossene Dritte ein dem vorliegenden Informationssicherheitssystem entsprechendes Sicherheitsniveau gewährleisten.

§ 3. Regierungsrat

Abs. 1 und 2

Der Regierungsrat trägt die Gesamtverantwortung für die Informationssicherheit und ist damit verantwortlich für die Vorgaben bezüglich der Informationssicherheitsstrategie. Grundlagen einer effektiven und effizienten Informationssicherheit sind eine kantonale Informationssicherheitsstrategie sowie die Sicherstellung der Umsetzung der Informationssicherheitsstrategie und deren zeitgerechte Anpassung an veränderte Verhältnisse. Der Regierungsrat formuliert die Informationssicherheitsstrategie und steuert mit einem dem Abstraktionsniveau des Regierungsrates angemessenen Informationssicherheits-Management-System (ISMS) deren Umsetzung. Damit kommt dem Regierungsrat eine Steuerungsfunktion zu. Das ISMS soll aufgrund der an den Regierungsrat erstatteten Berichte zeitgerecht an veränderte Verhältnisse angepasst werden. Mit diesen Aufgaben kann sowohl der hohen Dynamik als auch der Wichtigkeit der Thematik der Informationssicherheit begegnet werden.

§ 4. Steuerungsorgan für Informationssicherheit

Abs. 1

In Anlehnung an die im Kanton Basel-Stadt bestehende Governance-Struktur sieht die vorliegende Verordnung zur Sicherstellung der Umsetzung der Informationssicherheitsstrategie sowie der sich daraus ergebenden weiteren Aufgaben ein kantonales Steuerungsorgan für Informationssicherheit (Steuerungsorgan) vor (heute Konferenz für Organisation und Informatik, KOI). Damit der Regierungsrat die ihm im Zusammenhang mit der Erstellung und Überwachung der Informati-

onssicherheitsstrategie zukommende Verantwortung wahrnehmen kann, steht das Steuerungsorgan dem Regierungsrat als beratendes Gremium zur Seite und stellt die erforderlichen Anträge zur Einhaltung der Informationssicherheit. Die KOI wird dabei von der Stabsorganisation, der Informatiksteuerung und Organisation (ISO), beraten und unterstützt. Die ISO führt die Geschäfte der KOI und erarbeitet in deren Auftrag Entscheidungsgrundlagen. Der Vorsitz der KOI, welcher von der Leitung der ISO übernommen wird, berichtet dem Regierungsrat einmal jährlich über die Belange der kantonalen Informationssicherheit.

Abs. 2
Das Steuerungsorgan erlässt gestützt auf die kantonale Informatikstrategie sowie die Informationssicherheitsstrategie Weisungen, welche mittels Sicherheitsmassnahmen die Informationssicherheit konkretisieren. Diese Sicherheitsmassnahmen umfassen einerseits Anweisungen im Bereich des Grundschutzes, welche auf Standards basieren (im Normalfall die Umsetzung der Empfehlungen aus dem Standard DIN/ISO 27002) und aus jenen organisatorischen und technischen Massnahmen bestehen, die zwingend bei jeder IKT-Anwendung umzusetzen sind. Andererseits legt das Steuerungsorgan weitere Sicherheitsmassnahmen fest, wie die Erstellung eines Datenklassifikationsschemas unter Berücksichtigung der §§ 18 ff. der Verordnung über die Information und den Datenschutz vom 9. August 2011 (IDV, SG 153.270), die Festlegung von Massnahmen im Bereich der Notfallplanung sowie die Erarbeitung von Vorgaben zum Umgang mit Sicherheitsvorfällen.

Abs. 3
Dem Steuerungsorgan kommt die Kompetenz zu, über Ausnahmen von angewiesenen Informationssicherheitsmassnahmen zu entscheiden (Ausnahmebewilligungen). Diese Entscheidung ist abschliessend. Dem Steuerungsorgan steht jedoch die Möglichkeit offen, diese Entscheidungen zu einem Vorentscheid einer anderen Stelle zu delegieren, z.B. der oder dem kantonalen Beauftragten für Informationssicherheit. In jedem Fall empfiehlt es sich, diese Ausnahmen mit dem zentralen Leistungserbringer zu koordinieren.

§ 5. *Die oder der kantonale Beauftragte für Informationssicherheit (ISB)*

Abs. 1
Bei der bzw. beim ISB handelt es sich um eine Funktion, die spezielle Fachkompetenzen im Bereich Informationssicherheit erfordert. Sie ist in der Regel als Stabsstelle ausgestaltet und im Sinn dieser Verordnung insofern unabhängig, als sie weder den Interessen der Leistungsbezüger noch jenen der Leistungserbringer verpflichtet ist. Da es sich bei der Informationssicherheit um ein Thema handelt, welches das jeweilige Staatswesen in seiner Gesamtheit und weitgehend gleichermassen betrifft, soll entsprechend auch die oder der ISB für das gesamte Staatswesen zuständig sein. Wahrgenommen wird diese Funktion durch eine Stelle bei der ISO.

Inhaltlich umfasst die Aufgabe der oder des ISB alle Aspekte rund um die Informationssicherheit - so z.B. einerseits die Mitwirkung bei der Erstellung der Informationssicherheitsstrategie, die Unterstützung des Steuerungsorgans und der Departemente bei der Wahrnehmung ihrer Aufgaben zur Einhaltung der Informationssicherheit sowie die Erhebung der gesamtkantonalen Informationssicherheitsrisiken. Entsprechend sollte diese oder dieser eng mit dem Steuerungsorgan für Informationssicherheit zusammenarbeiten. Die oder der ISB leitet die Kommission Informationssicherheit (§ 6). Die weiteren Aufgaben und Kompetenzen ergeben sich aus dem in § 5 aufgeführten Katalog. Zentral ist dabei die jährliche Berichterstattung an das Steuerungsorgan, welches seinerseits gestützt auf diesen Bericht dem Regierungsrat berichtet (vgl. § 4 Abs. 1).

§ 6. Kommission Informationssicherheit

Abs. 1
Die Kommission Informationssicherheit (diese Funktion wird durch das Risk & Security Board, RSB wahrgenommen) unterstützt das Steuerungsorgan und die oder den ISB bei der dieser oder diesem übertragenen Aufgaben in taktischer Hinsicht. Das Gremium soll die Geschäfte zuerst vernehmlassen, welche anschliessend der KOI zum Entscheid vorgelegt werden.

Abs. 2
Die Kommission Informationssicherheit wird von dem oder der ISB geleitet und setzt sich aus Vertreterinnen und Vertretern der Departemente sowie einer Vertreterin oder einem Vertreter des zentralen Leistungserbringers zusammen (vgl. § 9 Abs. 1 lit. j). Die koordinativen Funktionen sind taktischer Natur, in operativen Belangen ist das IT-Board zuständig. Die Kommission Informationssicherheit kann zu ihrer Ausgestaltung sowie zur Präzisierung der ihr von der ISV übertragenen Aufgaben ein Kommissionsreglement erlassen.

§ 7. Departemente

Abs. 1
Die Departemente bzw. dessen Dienst- und Amtsstellen haben nach dem baselstädtischen IT-Governance-Modell einerseits die Rolle als Leistungsbezüger und andererseits auch jene als Leistungserbringer. Leistungsbezüger sind sie, wenn sie in ihrem Zuständigkeitsbereich IKT-Anwendungen betreiben (z.B. die Steuerverwaltung das NEST oder die Sozialhilfe das TUTORIS). Sie sind in Bezug auf diese IKT-Anwendungen dafür verantwortlich, dass dieselben die Vorgaben, wie sie sich einerseits aus dieser Verordnung und andererseits aus dem IDG ergeben, erfüllen. Ihre Zuständigkeit umfasst dabei die Umsetzung der Informatiksicherheitsstrategie in ihrem Aufgabenbereich sowie der in deren Zusammenhang entwickelten Massnahmen. Die oder der von § 5 dieser Verordnung vorgesehene ISB kann und soll sie bei der Wahrnehmung dieser Verantwortung unterstützen.

Abs. 2
Für die Umsetzung vor Ort (im Departement, Amt usw.) wird eine departementale Beauftragte oder ein departementaler Beauftragter für Informationssicherheit (ISBD) ernannt.

Abs. 3
Die Departemente sind zuständig für die Bereitstellung der erforderlichen finanziellen und personellen Ressourcen zur Umsetzung der erforderlichen Informationssicherheitsmassnahmen, das Führen eines Verzeichnisses der vorhandenen Informationsbestände und IKT-Anwendungen sowie die Bezeichnung der jeweiligen Dateneignerschaft.

§ 8. Dateneignerin oder Dateneigner

Abs. 1
Die Dateneignerin oder der Dateneigner trägt gemäss § 6 Abs. 1 IDG die Verantwortung für den Umgang mit den Informationen, die sie oder er zur Erfüllung ihrer gesetzlichen Aufgaben benötigt. Dazu gehört die Ermittlung des Schutzbedarfs der vorhandenen Informationen als auch das Erstellen eines Massnahmeplans basierend auf dem ermittelten Schutzbedarf. Bei erhöhtem oder sehr hohem Schutzbedarf obliegt der Dateneignerin oder dem Dateneigner zusätzlich die Durchführung einer Risikoanalyse. Der Massnahmenplan sollte dabei mindestens ein Zugriffs- und Berechtigungskonzept, Regelungen zur Datenaufbewahrung und Löschung, zum Informationsaustausch mit Dritten und zur Information und Schulung der Mitarbeitenden sowie zur Dokumentation von bewilligten Ausnahmen von umzusetzenden Informationssicherheitsmassnahmen umfassen. Die Dateneignerin oder der Dateneigner trägt zwar die erwähnten Verpflichtungen, muss die Erfüllung derselben jedoch nicht zwingend selbst übernehmen, sondern kann sich durch die oder

den departementalen Beauftragten für Informationssicherheit (ISBD) entsprechend unterstützen lassen.

Abs. 2
Die Dateneignerin oder der Dateneigner überprüft den Massnahmenplan regelmässig auf seine Zweckmässigkeit und Aktualität. Die im Rahmen des Massnahmenplans zu regelnden Punkte haben mindestens die im Katalog aufgeführten Minimalanforderungen zu erfüllen. Die Verpflichtungen spiegeln die gesetzlichen Verpflichtungen der Dateneignerin oder des Dateneigners, welche diese oder diesen aufgrund des IDG treffen. Mit der Formulierung eines Mindestniveaus an Schutzmassnahmen kann der raschen Entwicklung im Bereich der Informationssicherheit Rechnung getragen werden.

Abs. 3
Zentrales Rückgrat des Controllings im Bereich der Informationssicherheit ist die Berichterstattung über die Umsetzung der Informationssicherheitsmassnahmen. Die Dateneignerin oder der Dateneigner steuert ihre oder seine Befunde im Rahmen der departementalen Berichterstattung zuhanden des ISB bei.

§ 9. *Die oder der departementale Beauftragte für Informationssicherheit (ISBD)*

Abs. 1
Die oder der departementale Beauftragte für Informationssicherheit (ISBD) stellt die Schnittstelle im Departement zur oder zum ISB und zur Datenschutzbeauftragten oder zum Datenschutzbeauftragten sowie zu den Mitarbeiterinnen und Mitarbeitern in den Departementen sicher. Zentral ist, wiederum im Rahmen des Controllings und der damit verbundenen departementalen Berichterstattung, die Führung und Aktualisierung eines Risikoregisters sowie die Dokumentation der Ausnahmebewilligungen gemäss §§ 4 Abs. 3 und 5 Abs. 1 lit. i. Hervorzuheben ist bspw. die Verwaltung der in- und externen Sicherheitsprüfungen sowie die Meldung von technischen Sicherheitslücken an die oder den ISB. Zudem vertritt die oder der ISBD das Departement in der Kommission Informationssicherheit und ist für Schulungen auf Stufe Departement zuständig.

Es steht den Departementen frei, zusätzlich zur Funktion des ISBD weitere Funktionsträger zu ernennen, die den ISBD unterstützen.

§ 10. *Der zentrale Leistungserbringer*

Abs. 1
Bei der IT-Leistungserbringung wird zwischen zentralen, dezentralen und externen Leistungserbringern unterschieden. Die Zentralen Informatikdienste (ZID) sind die zentralen verwaltungsinternen IT-Dienstleister für Basisdienste. Den Departementen bzw. dessen Dienst- und Amtsstellen kommt die Funktion eines dezentralen Leistungserbringers zu, wenn diese klar definierte Unterstützungsleistungen (Mailservice, Dateiablagesystem, Fachanwendungen usw.) zugunsten eines Leistungsbezügers erbringen.

Abs. 2
Sowohl die zentralen als auch die dezentralen Leistungserbringer können auch auf externe IT-Provider (Dritte) zurückgreifen. Sie haben dann aber sicherzustellen, dass die Dritten über die kantonalen datenschutz- und informationssicherheitsrechtlichen Vorgaben informiert sind und diese einhalten. Bei der Beschaffung von IKT-Anwendungen (z.B. Office Anwendungen, spezifische Fachbereichsanwendungen, Emailprogramme, SAP usw.) ist darauf zu achten, dass diese

in Bezug auf ihre Ausgestaltung den Vorgaben der vorliegenden Verordnung sowie des IDG entsprechen. So muss eine IKT-Anwendung, um den Anforderungen dieser Verordnung zu entsprechen, Informationen gemäss dem ermittelten Schutzbedarf (§ 8 Abs. 1) schützen oder diese nach Ablauf der informationsspezifischen Aufbewahrungsfrist zuverlässig und idealerweise automatisiert löschen können (§ 8 Abs. 2 lit. b).

Abs. 3 und 4
Die Rolle der ZID für die Informationssicherheitsbelange des Kantons erfordert eine Berichterstattungspflicht für ihren Zuständigkeitsbereich sowie die Erwähnung eines Pendants zu den ISBD der Departemente (ISBZ).

Abs. 5
Wie bereits unter § 2 erwähnt, besteht für den Kanton ein erhebliches Interesse, beim Bezug von Leistungen, welche er mit dieser Verordnung nicht unterstellten Einheiten teilt (z.B. DANEBS), keinen Sicherheitsrisiken ausgesetzt zu sein, die er nicht kontrollieren kann. Aufgrund der beschränkten Rechtsetzungskompetenz kann der Regierungsrat z.B. weder den Gerichten noch den Gemeinden den Erlass von Informationssicherheitssystemen vorschreiben. Es steht dem Verordnungsgeber jedoch frei, dafür zu sorgen, die Erbringung von Dienstleistungen davon abhängig zu machen, dass alle Teilnehmenden vergleichbare Sicherheitsdispositive aufweisen. Mit Abs. 5 dieser Bestimmung wird klargestellt, dass die ZID befugt ist, Dienstleistungen Dritten im Sinne der Verordnung anzubieten. Diese Tätigkeit steht im Zeichen der Nutzung von Synergien sowohl im Interesse der Dritten als auch des Kantons. Diese Bestimmung soll aber sicherstellen, dass das mit dem Erlass der Verordnung angestrebte Sicherheitsniveau auch durch weitere Teilnehmende an gemeinsam bezogenen Services eingehalten wird. Diese Bestimmung lässt aber explizit offen, ob die Dritten oder die ZID die Sicherheitsbestimmungen formulieren sollen. Erlassen Dritte Regeln, wird die ZID deren Gleichwertigkeit zu beurteilen haben, soweit die Dritten nicht, soweit allenfalls sinnvoll, diese Verordnung übernehmen. Werden keine Regelungen erlassen, wird die ZID in den jeweiligen Vertragsbestimmungen Sicherheitsbedingungen vorsehen müssen.

3. Änderungen anderer Erlasse

In verschiedenen Verordnungen wird auf die vorbestehende ISV verwiesen. Diese Verweisungen sind zu aktualisieren, die entsprechenden Änderungen bedürfen keiner separaten Erläuterung. In § 7 der Verordnung über das Informatiksystem der Staatsanwaltschaft vom 2. November 2010 (SG 257.140) ist die entsprechende Verweisung jedoch bereits durch eine zwischenzeitlich im Zuge des Erlasses der Verordnung über die Zusammensetzung, Organisation und Befugnisse der Staatsanwaltschaft vom 28. Juni 2016 (SG 257.120) erfolgten Revision ersetzt worden. Der revidierte Wortlaut der Bestimmung in § 7 tritt erst auf den 1. Februar 2017 in Kraft und wird nicht mehr explizit auf die ISV verweisen, womit eine Anpassung des Wortlauts in der vorliegenden Revision an und für sich obsolet wäre.

Weil aber die künftige Fassung des § 7 Abs. 2 (inkl. Nennung des Begriffes „Informationssicherheit“ im Titel des entsprechenden Paragraphen) Anlass für Verwirrung stiften kann, werden Abs. 2 der Bestimmung und die Nennung der Informationssicherheit im Titel gestrichen. Die Verwirrung rührt daher, dass der Eindruck entstehen kann, die Staatsanwaltschaft wäre vom Geltungsbereich der ISV ausgenommen, was, im Gegensatz zu den Gerichten, nicht der Fall ist. Die in § 7 Abs. 2 erwähnte Weisungsbefugnis stellt die auch anderen Dienststellen im Kanton im internen Bereich zustehende Weisungsbefugnis (innerhalb der Regelung der ISV und der darauf beruhenden Weisungen) dar, die nicht geregelt zu werden braucht. Damit wird § 7 bereits vor dessen Wirksamwerden angepasst. Mit Wirksamkeit am 1. Februar 2017 wird bloss noch § 7 Abs. 1 sowie ein verkürzter Titel (Nennung des Begriffs „Verantwortung“) in Wirksamkeit erwachsen.

Synopse

Verordnung über das Informatiksystem der Staatsanwaltschaft vom 2. November 2010 (SG 257.140) – Fassung gemäss Verordnung über die Zusammensetzung, Organisation und Befugnisse der Staatsanwaltschaft vom 28. Juni 2016 (SG 257.120) – wirksam per 1. Februar 2017.	**Verordnung über das Informatiksystem der Staatsanwaltschaft vom 2. November 2010 (SG 257.140)** – Fassung gemäss neuer ISV
§ 7 Verantwortung und Informationssicherheit [1] Die Erste Staatsanwältin oder der erste Staatsanwalt ist verantwortlich für das Informatiksystem im Sinne von § 6 IDG. [2] Sie oder er erlässt die nötigen Weisungen für die Nutzung des Informatiksystems und die Informationssicherheit.	§ 7 Verantwortung [1] Die Erste Staatsanwältin oder der erste Staatsanwalt ist verantwortlich für das Informatiksystem im Sinne von § 6 IDG. ~~[2]~~ Aufgehoben.