Verordnung über die Informationssicherheit (ISV)

Vom 13. Dezember 2016 (Stand 18. Dezember 2016)

Der Regierungsrat des Kantons Basel-Stadt,

gestützt auf das Gesetz betreffend die Organisation des Regierungsrates und der Verwaltung des Kantons Basel-Stadt (Organisationsgesetz, OG) vom 22. April 1976 [1)] und das Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 [2)], unter Verweis auf seine Erläuterungen Nr. P161893,

beschliesst:

Kapitel I: Allgemeine Bestimmungen

§ 1. *Gegenstand und Zweck*

[1] Diese Verordnung regelt die Informationssicherheit im Kanton Basel-Stadt.
[2] Die Informationssicherheit bezweckt die Gewährleistung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen sowie die Zurechenbarkeit und Nachvollziehbarkeit von diese betreffende Handlungen oder Abläufen durch angemessene Massnahmen.

§ 2. *Geltungsbereich*

[1] Diese Verordnung gilt für die Organisationseinheiten des Kantons im Sinne von § 3 Abs. 1 lit. a IDG mit Ausnahme der Gerichte.

Kapitel II: Zuständigkeiten und Aufgaben

1. Strategische Ebene

§ 3. *Regierungsrat*

[1] Der Regierungsrat trägt die Gesamtverantwortung für die Informationssicherheit.
[2] Er legt die Informationssicherheitsstrategie fest und steuert mit einem Informationssicherheits-Management-System die Umsetzung der Informationssicherheitsstrategie und stellt deren zeitgerechte Anpassung an veränderte Verhältnisse sicher.

[1)] SG 153.100.
[2)] SG 153.260.

§ 4. *Steuerungsorgan für Informationssicherheit*

[1] Das Steuerungsorgan für Informationssicherheit steht dem Regierungsrat als beratendes Gremium zur Seite und stellt die Anträge zur Anpassung der Informationssicherheitsstrategie. Die oder der Vorsitzende des Steuerungsorgans für Informationssicherheit erstattet dem Regierungsrat einmal jährlich Bericht über die Erreichung der Ziele der Strategie in den Departementen.
[2] Das Steuerungsorgan für Informationssicherheit erlässt Weisungen und kontrolliert deren Einhaltung über eine jährliche Berichterstattung durch die kantonale Beauftragte oder den kantonalen Beauftragten für Informationssicherheit (ISB).
[3] Es entscheidet abschliessend über Ausnahmen von Informationssicherheitsmassnahmen.

2. Taktische Ebene

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

[1] Die oder der ISB führt die zentrale Fachstelle für Informationssicherheit und hat folgende Aufgaben:

a) die Erarbeitung der Informationssicherheitsstrategie unter Berücksichtigung der kantonalen Informatikstrategie;
b) die Erstellung eines jährlichen Berichts über die Informationssicherheit zu Handen des Steuerungsorgans für Informationssicherheit;
c) die Erhebung der gesamtkantonalen Informationssicherheitsrisiken auf Basis anerkannter Methoden;
d) die Überprüfung der von der Dateneignerin oder dem Dateneigner erhobenen Schutzbedarfs- und Risikoanalysen und die Empfehlung von risikomindernden Massnahmen;
e) die Erstellung und Aktualisierung eines Verzeichnisses über die vorhandenen Informationsbestände und Informations- und Kommunikations-Anwendungen (IKT-Anwendungen) inkl. Auflistung der jeweils verantwortlichen Dateneignerin oder des verantwortlichen Dateneigners, der Schutzstufe sowie die Führung eines Risiko- und Ausnahmenregisters;
f) die Leitung der Kommission Informationssicherheit;
g) die Unterstützung des Steuerungsorgans für Informationssicherheit und der Departemente bei der Wahrnehmung ihrer Aufgaben zur Einhaltung der Informationssicherheit;
h) die Durchführung von Informationssicherheitsprüfungen in den Departementen in Absprache mit dem zentralen Leistungserbringer;
i) die erstinstanzliche Entscheidung über Ausnahmebewilligungen von Informationssicherheitsmassnahmen - die Bewilligungen sind zeitlich zu befristen;
j) die Ausarbeitung von Ausführungsbestimmungen zur Umsetzung der Informationssicherheitsstrategie.

§ 6. *Kommission Informationssicherheit*

[1] Die Kommission Informationssicherheit unterstützt das Steuerungsorgan für Informationssicherheit und die oder den ISB bei der Wahrnehmung der ihnen übertragenen taktischen Aufgaben.
[2] Sie koordiniert die Tätigkeiten der departementalen Beauftragten für Informationssicherheit (ISBD) und entwickelt Sensibilisierungskampagnen zuhanden des Steuerungsorgans für Informationssicherheit.

3. Operative Ebene

§ 7. *Departemente*

[1] Die Departemente gewährleisten die operative Umsetzung der Informationssicherheitsstrategie mit angemessenen Massnahmen und dem Informationssicherheits-Management-System sowie eine jährliche Berichterstattung an die oder den ISB.
[2] Jedes Departement bezeichnet eine oder einen ISBD, die oder der die Departemente bei der Umsetzung der Massnahmen und der Berichterstattung gemäss Abs. 1 unterstützt.
[3] Die Aufgaben der Departemente umfassen insbesondere:

a) die Bereitstellung der finanziellen und personellen Ressourcen zur Umsetzung der Informationssicherheitsmassnahmen;
b) die Erstellung eines Verzeichnisses über die vorhandenen Informationsbestände und IKT-Anwendungen, deren Schutzstufen inkl. Bezeichnung der verantwortlichen Dateneignerin oder des verantwortlichen Dateneigners sowie eines Risikoregisters;
c) die regelmässige Aktualisierung des Verzeichnisses gemäss Bst. b und Meldung der Veränderungen an die oder den ISBD.

§ 8. *Dateneignerin oder Dateneigner*

[1] Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. Dieses ist insbesondere zuständig für die Ermittlung des Schutzbedarfs der vorhandenen Informationsbestände und IKT-Anwendungen nach den Schutzzielen gemäss § 8 Abs. 2 IDG. Ergibt eine entsprechende Ermittlung einen über den Grundschutz hinausgehenden Schutzbedarf, ist eine Risikoanalyse inkl. Massnahmenplan zur Risikosenkung durchzuführen.
[2] Der Massnahmenplan ist jährlich auf seine Zweckmässigkeit und Aktualität zu überprüfen und muss als Teil des Grundschutzes mindestens Regelungen zu den folgenden Punkten enthalten:

a) das Erstellen und Verwalten eines Zugriffs- und Berechtigungskonzepts;
b) die Datenaufbewahrung und -löschung unter Einhaltung der Archivierungsvorschriften;
c) den sicheren Informationsaustausch mit Dritten;

d) den Einbezug der Mitarbeitenden in den Sicherheitsprozess und
e) die Dokumentation von bewilligten und abgelehnten Ausnahmen von Informationssicherheitsmassnahmen sowie des Risikoregisters.

[3] Die Dateneignerin oder der Dateneigner berichtet über die Umsetzung von Informationssicherheitsmassnahmen im Rahmen der jährlichen departementalen Berichterstattung.

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

[1] Die oder der ISBD:
a) ist Ansprechpartnerin oder Ansprechpartner für die oder den ISB und die Datenschutzbeauftragte oder den Datenschutzbeauftragten;
b) führt und aktualisiert ein Risikoregister auf Ebene Departement und dokumentiert die Ausnahmebewilligungen;
c) prüft die Umsetzung der organisatorischen und technischen Sicherheitsmassnahmen;
d) empfiehlt Sicherheitsmassnahmen zur Umsetzung;
e) ist die zentrale Anlaufstelle für Sicherheitsfragen im Bereich der IKT-Anwendungen;
f) unterstützt die Departementsführung bei der Erstellung der organisatorischen Sicherheitsvorgaben;
g) unterstützt die Dateneignerin oder den Dateneigner, dass die Informationen im Departement durch angemessene organisatorische und technische Massnahmen geschützt werden;
h) verwaltet die internen und externen Sicherheitsprüfungen;
i) meldet technische Informationssicherheitslücken der oder dem ISB;
j) vertritt das Departement in der Kommission Informationssicherheit;
k) organisiert Informationsveranstaltungen zur Informationssicherheit auf Stufe Departement.

§ 10. *Der zentrale Leistungserbringer*

[1] Der zentrale Leistungserbringer ist für die Entwicklung, Beschaffung, Bereitstellung, den Unterhalt von IKT-Anwendungen sowie die Einhaltung und Umsetzung der Vorgaben im Bereich der Informationssicherheit zuständig, welche die Departemente unter Einhaltung der datenschutz- und informationssicherheitsrechtlichen Vorgaben zur Erfüllung ihrer gesetzlichen Aufgaben benötigen, soweit diese Anwendungen nicht dezentral beschafft werden.
[2] Werden die IKT-Anwendungen von Dritten bezogen, ist sicherzustellen, dass diese die Vorgaben gemäss Abs. 1 einhalten.
[3] Der zentrale Leistungserbringer erstellt den entsprechenden Bericht gemäss § 7 Abs. 1.

[4] Die oder der Informationssicherheitsbeauftragte des zentralen Leistungserbringers (ISBZ) übernimmt bei diesem die Funktionen der oder des ISBD.
[5] Der zentrale Leistungserbringer ist befugt, Dienstleistungen Dritten ausserhalb des Geltungsbereichs gemäss § 2 zu erbringen, wenn diese sich verpflichten, mindestens die kantonalen Sicherheitsvorgaben zu gewährleisten. Der zentrale Leistungserbringer ist befugt, entsprechende Kontrollen vorzunehmen oder zu delegieren.

Schlussbestimmung

Diese Verordnung ist zu publizieren. Sie wird sofort wirksam. Auf den gleichen Zeitpunkt wird die Verordnung zur Informatiksicherheit (ISV) vom 9. April 2002 aufgehoben. Die Änderung der Verordnung über das Informatiksystem der Staatsanwaltschaft wird am 1. Februar 2017 wirksam.