Verordnung betreffend Informatiksicherheit (Informatiksicherheitsverordnung, ISV)

vom 2. Dezember 2014

Der Regierungsrat des Kantons Schaffhausen

beschliesst:

I. Grundsatz und Geltungsbereich

§ 1

Grundsatz

[1] Diese Verordnung bezweckt eine geordnete, wirksame und wirtschaftliche Informatik- und Informations-Sicherheit.

[2] Die Verordnung bestimmt

a) das Verfahren, die Zuständigkeiten und Verantwortlichkeiten zur Gewährleistung der Sicherheit von Daten und Informationen, die mit Informatiksystemen und -anwendungen bearbeitet werden,

b) die grundsätzlichen Sicherheitsanforderungen, die bei der Bearbeitung von Daten oder Informationen mit Informatiksystemen und -anwendungen einzuhalten sind.

§ 2

Geltungsbereich

Diese Verordnung gilt für:

a) die kantonale Verwaltung, die Justizbehörden und öffentlich-rechtliche Anstalten,

b) für die Gemeinden und für alle öffentlich-rechtlichen Körperschaften im Kanton Schaffhausen, soweit sie gemeinsam mit der kantonalen Verwaltung Informatiksysteme und -anwendungen betreiben, Daten oder Informationen austauschen oder eigene Anwendungen bei der KSD betreiben lassen,

Amtsblatt 2014, S. 1759

c) Dienststellen oder Verwaltungseinheiten, die Bundesrecht vollziehen oder Bundesaufgaben erfüllen und dafür eigene oder fremde Informatiksysteme oder -anwendungen einsetzen, soweit keine Sicherheitsanforderungen seitens des Bundes vorhanden sind.

II. Allgemeine Bestimmungen

§ 3

Begriffe

[1] Die folgenden Ausdrücke bedeuten:

a) Informatiksysteme: Geräte und Einrichtungen sowie die dazugehörende Infrastruktur und Betriebssoftware, die zur elektronischen Bearbeitung oder zum elektronischen Austausch von Daten oder Informationen eingesetzt werden.

b) Informatikanwendungen: Programme, welche die Nutzung von Informatiksystemen für die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen, einschliesslich der dabei bearbeiteten Daten.

c) Informationen: Informationen sind Ergebnisse von konkreten Abfragen, welche aus Sach-, Finanz- oder Personendaten gewonnen werden.

d) Inhaber der Datensammlung: Jede Organisationseinheit der öffentlichen Verwaltung des Kantons, der Gemeinden oder anderer öffentlich-rechtlicher Körperschaften im Kanton Schaffhausen, welche im Rahmen einer gesetzlichen Grundlage die Bearbeitung von Daten oder Informationen zu verantworten hat.

e) Betreiber zentraler Datenbanken: In der Regel der kantonale Informatik-Servicedienstleister KSD, in Ausnahmefällen Drittbetreiber oder der jeweilige Inhaber der Datensammlung, soweit die Datenbank dezentral betrieben wird.

[2] Ist aufgrund einer gesetzlichen Aufgabe nicht klar bestimmt oder nicht bestimmbar, wer Inhaber einer Datensammlung oder Betreiber einer Datenbank ist, muss dies unter allen Beteiligten schriftlich vereinbart und ein verantwortlicher Inhaber der Datensammlung bezeichnet werden.

§ 4

Zuständigkeiten

[1] Der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank sind in ihren jeweiligen Aufgabenbereichen verpflichtet, Informatiksysteme, -anwendungen, Daten oder Informationen gegen Verlust und unerwünschte Einwirkungen zu sichern, vor unbefugtem Zugriff und unbefugter Bearbeitung zu schützen,

die diesbezüglich notwendigen Notfallvorsorgemassnahmen sicherzustellen und die Grundsätze dieser Verordnung gemeinsam durchzusetzen.

[2] Sofern die Gesetzgebung nichts anderes vorsieht, gelten für die Ordnungsmässigkeit und Sicherheit im Umgang mit Informatiksystemen, -anwendungen, Daten oder Informationen die anerkannten internationalen und nationalen Standards für das Informatiksicherheits- und das Informationsmanagement.

[3] Die KSD:

a) bewirtschaftet die Basisinfrastrukturen,

b) unterstützt alle dieser Verordnung unterstellten Organisationseinheiten bei der Einrichtung und beim Betrieb einer sicheren Informatik sowie bei der Umsetzung und Kontrolle der Sicherheitsmassnahmen,

c) überwacht die Einhaltung der technischen Sicherheitsanforderungen,

d) ist Ansprechpartnerin für alle dieser Verordnung unterstellten Organisationseinheiten in Fragen der Informatiksicherheit.

[4] Der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank sind in ihrem Zuständigkeitsbereich in Bezug auf die eingesetzten Informatiksysteme, -anwendungen, Daten oder Informationen verantwortlich für:

a) die Bestimmung der Schutzziele,

b) die Klassifizierung nach den Schutzzielen,

c) die Erstellung eines Massnahmenplanes zur Erreichung der Schutzziele und die Umsetzung der Sicherheitsanforderungen,

d) die Kontrolle des in ihrem Zuständigkeitsbereich liegenden Informatikbetriebes und der Informatiksicherheit.

[5] Der Informatiksicherheitsbeauftragte (ISB) der KSD ist verantwortlich für den Aufbau, die Implementierung, die Umsetzung und die Anpassung der gesamten Sicherheitsgrundsätze für den Informatik- und Telekommunikationsbetrieb der KSD als zentrale IT-Servicedienstleisterin und gegenüber allen dieser Verordnung unterstehenden Organisationseinheiten.

[6] Der Fachausschuss der KSD ernennt ein Sicherheits-Gremium (Security-Board), bestehend aus mindestens drei Personen, wovon mindestens zwei Fachspezialisten, welche mit den Fragen der Informatiksicherheit vertraut und erfahren sind. Dieses Gremium berät den ISB, ist Kontrollorgan über die Tätigkeiten des ISB und Eskalationsstelle im Sinne von § 16 Abs. 1 dieser Verordnung.

III. Schutzziele und Klassifizierung

§ 5

Schutzziele

[1] Für Informatiksysteme, -anwendungen und Informationen gelten folgende Schutzziele:

a) Verfügbarkeit: Informatiksysteme, -anwendungen, Daten oder Informationen sind zugänglich und nutzbar.

b) Vertraulichkeit: Daten oder Informationen sind nur den berechtigten Personen zugänglich.

c) Integrität: Informatiksysteme, -anwendungen, Daten oder Informationen sind vor unberechtigten Änderungen geschützt. Alle Daten und Informationen sind vollständig und richtig.

d) Nachvollziehbarkeit: Eine Ereigniskette kann nachträglich nachvollzogen werden.

e) Beweistauglichkeit und Revisionssicherheit: gemäss § 12 Abs. 3 dieser Verordnung.

[2] Der Inhaber der Datensammlung und der Betreiber einer Datenbank haben den Schutzbedarf der Daten und Informationen anhand dieser Schutzziele festzulegen.

§ 6

Klassifizierung

[1] Die Informatiksysteme, -anwendungen sowie die Daten und Informationen sind von allen dieser Verordnung unterstehenden Organisationseinheiten nach folgenden Kriterien zu klassifizieren:

a) Verfügbarkeit: Ausfalldauer 3 Tage und mehr (Stufe tief); Ausfalldauer 1 – 3 Tage (Stufe mittel); Ausfalldauer bis ein Tag (Stufe hoch)

b) Vertraulichkeit: Stufe P (public), Stufe N (nicht klassifizierte interne Daten), Stufe V (vertraulich), Stufe G (besonders schützenswert)

c) Integrität: Ausmass einer Beeinträchtigung in der Datennutzung dauert mehrere Jahre (Stufe sehr hoch); maximal bis zu einem Jahr (Stufe hoch); hat einen signifikanten, jedoch nicht über ein Jahr dauernden Einfluss auf das Geschäftsergebnis (Stufe mittel)

d) Nachvollziehbarkeit: keine Nachvollziehbarkeit; anonymisierte Nachvollziehbarkeit; personenbezogene Nachvollziehbarkeit.

e) Beweistauglichkeit und Revisionssicherheit: durch elektronische Signierung und Aufbewahrungsfristen.

[2] Die KSD erlässt eine Weisung betreffend Klassifizierung von Daten und Informationen.

[3] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank sind befugt, für ihren Zuständigkeitsbereich die Klassifizierung zu verfeinern und zusätzliche interne Weisungen für ihre eigene Organisationseinheit zu erlassen.

§ 7

Massnahmenplan

[1] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank erstellen einen Plan der organisatorischen und technischen Massnahmen, welche die Erreichung der ermittelten Schutzziele sicherstellt. Die Massnahmen richten sich nach den Anforderungen an den Betrieb und die Sicherheit (§ 9 ff.) sowie nach den weiteren Vorgaben der KSD (§ 14 und § 17). Dabei sind der Grundsatz der Verhältnismässigkeit, der Stand der Technik und die verfügbaren Mittel zu berücksichtigen.

[2] Der Massnahmenplan enthält für alle im Einsatz stehenden Informatiksysteme, -anwendungen, Daten oder Informationen folgende Angaben:

a) Schutzziele und Klassifizierung,
b) Inhalt,
c) Kosten,
d) Verantwortlichkeiten,
e) Umsetzungsschritte und Termine,
f) Restrisiko,
g) Dokumentation.

§ 8

Instruktion des Personals

[1] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank informieren ihre Mitarbeitenden über die Sicherheitsmassnahmen, die sie zu beachten haben.

[2] Sie sorgen für eine periodische Schulung ihrer Mitarbeitenden.

IV. Anforderungen an den Betrieb und die Sicherheit

§ 9

Schutz der Informatiksysteme, -anwendungen und Informationen

[1] Zur Verhinderung von Verlust, Beschädigung und Missbrauch von Informatiksystemen, -anwendungen, Daten oder Informationen und zur Verhinderung eines Unterbruchs von Geschäftsaktivitäten müssen die Gebäude, Räume und Geräte vor Sicherheitsbedrohungen geschützt werden.

[2] Die KSD stellt sicher, dass Verletzungen der Sicherheitsgrundsätze gemäss dieser Verordnung mit angemessenem Aufwand nachvollzogen und beweistauglich reproduziert werden können.

§ 10

Authentisierung und Authentifizierung

[1] Der Zugriff auf Informatiksysteme, -anwendungen, Daten oder Informationen wird über die Mitgliedschaft in Berechtigungsgruppen und/oder -rollen geregelt. Die Benutzer werden in die zur Ausübung ihrer Tätigkeiten erforderlichen Berechtigungsgruppen und/oder -rollen aufgenommen. Sie haben sich an Informatiksystemen entsprechend zu authentisieren.

[2] Für die Zuordnung der Zugangsrechte sowie für deren laufende Aktualisierung ist der Inhaber einer Datensammlung zuständig und verantwortlich. Informatiksysteme müssen in der Lage sein, Benutzer entsprechend ihren Berechtigungen zu authentifizieren.

[3] Authentifizierungsmethoden sind der Risikosituation und dem Stand der Technik laufend anzupassen.

§ 11

Beendigung oder Änderung der Anstellung

[1] Die Zugangsrechte von Mitarbeitenden, Auftragnehmern oder Drittbenutzern zu Informatiksystemen, -anwendungen, Daten oder Informationen müssen vom Inhaber einer Datensammlung sofort entzogen werden, wenn ihre Anstellung, ihr Auftrag oder eine entsprechende Nutzung beendet sind oder ein Missbrauch oder eine Verletzung der Sicherheitsgrundsätze gemäss dieser Verordnung festgestellt werden.

[2] Ändern Anstellung, Auftrag oder Nutzung, sind die Zugangsrechte vom Inhaber einer Datensammlung umgehend anzupassen.

§ 12

Datensicherung

[1] Für die Datensicherung auf den zentralen Informatiksystemen der kantonalen Verwaltung ist die KSD zuständig. Die Sicherung umfasst:

a) die Benutzeridentifikationen und deren Zugriffsrechte (Objekte);
b) die Fachanwendungen und deren Daten;
c) die Datenablagen;
d) die Verbindungsdaten des Internet- und E-Mail-Verkehrs;
e) alle für die Rekonstruktion der EDV-Systeme notwendigen Daten- und Programmbereiche.

[2] Die Datensicherung kann auch Protokollierungsdateien umfassen.

[3] Die gesicherten Daten werden gesondert und sicher aufbewahrt und können zur Rekonstruktion von verlorenen Daten beigezogen und im Rahmen der festgelegten Sicherungskonzepte auch ausgewertet werden. Deren beweistaugliche, gesetzeskonforme und revisionssichere Aufbewahrung sowie deren digitale Langzeitarchivierung bleiben im Verantwortungsbereich des Inhabers einer Datensammlung.

[4] Für die Datensicherung auf den lokalen oder dezentralen Informatiksystemen ist der Inhaber einer Datensammlung selber verantwortlich.

§ 13

Weitere Anforderungen

[1] Die KSD kann im Rahmen von Richtlinien oder Weisungen die nötigen Anforderungen an den Betrieb und die Sicherheit weiter definieren oder konkretisieren, insbesondere betreffend:

a) die Standardisierung und Organisation der Infrastrukturen;
b) den Zugriffsschutz und die Sicherheitsauswertungen;
c) die elektronische Datenkommunikation;
d) den Datenaustausch;
e) die Datensicherung und Datenablage;
f) die Sicherstellung des Geschäftsbetriebs;
g) Internet- und E-Mail-Nutzung;
h) den Schutz vor Bedrohungen wie Malware, Computer-Viren, Social Engineering, Phishing, usw.;
i) mobile Speichermedien und Endgeräte;
j) Anforderungen an den Einsatz und die Sicherheitsvorkehrungen von sozialen Medien;
k) den Umgang der Mitarbeitenden mit der Informatik am Arbeitsplatz und ausserhalb der Büroräumlichkeiten;
l) den Umgang bei Beendigung oder Änderung des Anstellungsverhältnisses;
m) neue Technologien und Infrastrukturen.

[2] Die KSD kann für die Ausarbeitung von Richtlinien oder Weisungen die Fachkräfte der Inhaber von Datensammlungen beiziehen und anhören.

V. Kontrolle und Überprüfung der Sicherheitsmassnahmen

§ 14

Meldung von Vorkommnissen und Schwachstellen

[1] Auftretende Unregelmässigkeiten, unerklärliches Systemverhalten, Verlust oder Veränderung von Informatiksystemen, -anwendungen, Daten oder Informationen, Verdacht auf Missbrauch der eigenen Benutzererkennung oder andere sicherheitsrelevante Vorkommnisse sind umgehend dem Informatiksicherheitsbeauftragten der KSD (ISB) zu melden. Der ISB orientiert den Datenschutzbeauftragten.

[2] Der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank richten Verfahren ein, welche eine schnelle, wirksame und planmässige Erkennung und Reaktion auf sicherheitsrelevante Vorkommnisse ermöglichen. Die KSD unterstützt sie dabei.

§ 15

Überprüfung

[1] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank überprüfen regelmässig, jedoch mindestens einmal jährlich, die Schutzziele und die Klassifizierung der in ihrem Zuständigkeitsbereich liegenden Informatiksysteme, -anwendungen, Daten und Informationen, die Einhaltung und Angemessenheit der Sicherheitsmassnahmen sowie die Zugangsrechte.

[2] Der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank führen die notwendigen Dokumentationen gemäss dieser Verordnung aktuell nach und informieren die KSD angemessen und zeitnah.

[3] Ändern Aufgaben, Organisation oder eingesetzte Informatiksysteme, -anwendungen oder die damit bearbeiteten Daten und Informationen, treffen der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank die nötigen Anpassungen (vgl. auch § 11).

[4] Der Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank können die Schutzziele und die Klassifizierung sowie die getroffenen Massnahmen in Abstimmung mit der KSD zusätzlich durch eine qualifizierte unabhängige externe Stelle prüfen lassen. Die Finanzkontrolle von Kanton und Stadt Schaffhausen, die KSD sowie der oder die kantonale Datenschutzbeauftragte können Einsicht in die Berichte nehmen.

§ 16

Bereinigung von Differenzen

[1] Ist der Inhaber einer Datensammlung oder der Betreiber einer zentralen Datenbank nicht mit den Vorgaben der KSD einverstanden, ist das Security Board der KSD (§ 4 Abs. 6) anzurufen. Das Security Board versucht unter Einbezug der anrufenden Stelle eine einvernehmliche Lösung zu finden.

[2] Kann innert drei Monaten seit Anmeldung der Differenz beim Security Board keine einvernehmliche Lösung gefunden werden, entscheidet der Regierungsrat. Der Datenschutzbeauftragte kann vorgängig angehört werden.

VI. Schlussbestimmungen

§ 17

Weisungen der KSD

[1] Die KSD erlässt und publiziert alle notwendigen Weisungen, Richtlinien oder Reglemente über die Nutzung der Informatiksysteme, -anwendungen, Daten und Informationen, für die Sicherstellung eines sicheren und wirtschaftlichen Einsatzes und Betriebes der Informatik und für die Konkretisierung der Schutzziele und die Sicherheitsanforderungen.

[2] Die KSD unterstützt die Inhaber einer Datensammlung und die Betreiber einer zentralen Datenbank in allen Belangen des Vollzuges dieser Verordnung.

§ 18

Übergangsbestimmung

Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank haben für alle Informatiksysteme, -anwendungen, Daten und Informationen innerhalb von zwei Jahren nach Inkrafttreten dieser Verordnung die Schutzziele (§ 5), die Klassifizierung (§ 6) und den Massnahmenplan (§ 7) in Abstimmung mit der KSD zu erstellen.

§ 19

Aufhebung bisherigen Rechts

Das Reglement über den Schutz und die Sicherung von Daten bei der «KSD Kanton und Stadt Schaffhausen Datenverarbeitung» (Datenschutzreglement) vom 22. April 1980 wird aufgehoben.

§ 20

Inkrafttreten

[1] Diese Verordnung tritt auf den 1. Januar 2015 in Kraft.

[2] Sie ist im Amtsblatt zu veröffentlichen [1)] und in die kantonale Gesetzessammlung aufzunehmen.

Fussnoten:

1) Amtsblatt 2014, S. 1759.