Synopse

Teilrevision Datensicherheitsverordnung (DSV)

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
	Verordnung über die Informationssicherheit von Personendaten (VIP)
	Der Regierungsrat des Kantons Zug, gestützt auf § 7 des Datenschutzgesetzes vom 28. September 2000[BGS 157.1], *beschliesst:*
	I.
	Der Erlass BGS 157.12, Datensicherheitsverordnung (DSV) vom 16. Januar 2007 (Stand 27. Januar 2007), wird wie folgt geändert:
Datensicherheitsverordnung **(DSV)**	**~~Datensicherheitsverordnung~~Verordnung über die Informationssicherheit von Personendaten** **(~~DSV~~VIP)**
vom 16. Januar 2007 (Stand 27. Januar 2007)	
Der Regierungsrat des Kantons Zug,	
gestützt auf § 7 des Datenschutzgesetzes vom 28. September 2000[BGS 157.1],	
beschliesst:	
§ 1 Gegenstand und Geltungsbereich [1] Diese Verordnung regelt das Verfahren und die Zuständigkeiten zur Gewährleistung der Sicherheit von Daten, die mit elektronischen Hilfsmitteln oder auf andere Weise bearbeitet werden.	[1] Diese Verordnung regelt das Verfahren und die ~~Zuständigkeiten~~Verantwortlichkeit zur Gewährleistung der Sicherheit von ~~Daten~~Personendaten, die mit elektronischen Hilfsmitteln oder auf andere Weise bearbeitet werden.

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
[2] Sie gilt für die dem Datenschutzgesetz unterstellten Organe. Für Organe, die für den Kanton oder die Gemeinden öffentliche Aufgaben erfüllen, ist sie nur im Rahmen der übertragenen Aufgaben anwendbar.	
§ 2 Zweck der Datensicherheit [1] Die Datensicherheit bezweckt den Schutz von Daten insbesondere gegen: a) zufällige Bekanntgabe, Vernichtung oder Verlust; b) technische Fehler; c) unbefugte Kenntnisnahme; d) unbefugte Bearbeitung; e) Fälschung, Entwendung oder widerrechtliche Verwendung.	**§ 2** Zweck der ~~Datensicherheit~~Informationssicherheit [1] Die ~~Datensicherheit~~Informationssicherheit bezweckt den Schutz von ~~Daten~~Personendaten insbesondere gegen:
§ 3 Überprüfung der Datensicherheit [1] Die Organe sind verantwortlich für die Überprüfung der Sicherheit der Daten in den Phasen ihrer Erhebung, Bearbeitung, Aufbewahrung und Löschung. Für die Überprüfung der Sicherheit der Daten in der Phase der Archivierung ist das Archiv zuständig.	**§ 3** ~~Überprüfung der Datensicherheit~~Verantwortlichkeit [1] Die Organe sind verantwortlich für die ~~Überprüfung~~Gewährleistung der ~~Sicherheit der Daten~~ Informationssicherheit in ~~den~~allen Phasen ~~ihrer Erhebung, Bearbeitung, Aufbewahrung und Löschung~~der Datenbearbeitung. Für die ~~Überprüfung~~ Gewährleistung der Sicherheit der ~~Daten~~Personendaten in der Phase der Archivierung ist das Archiv ~~zuständig~~verantwortlich.
§ 4 Sicherheitsmassnahmen [1] Die Organe bestimmen die zum Schutz der Daten erforderlichen Sicherheitsmassnahmen, wie Zugangs-, Benutzer-, Zugriffs- oder Bearbeitungskontrollen.	[1] Die Organe ~~bestimmen die zum Schutz~~ sorgen für Vertraulichkeit, Integrität und Verfügbarkeit der ~~Daten~~ Personendaten sowie die Zurechenbarkeit und Nachvollziehbarkeit von Datenbearbeitungen. Sie ergreifen die erforderlichen technischen und organisatorischen Sicherheitsmassnahmen~~, wie~~ zum Zwecke der Zugangs-, Datenträger-, Transport-, Bekanntgabe-, Speicher-, Benutzer-, Zugriffs- oder ~~Bearbeitungskontrollen~~Eingabekontrolle.

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
[2] Sie berücksichtigen dabei den gegenwärtigen Stand der Technik sowie die Grundsätze der Verhältnismässigkeit und Wirtschaftlichkeit.	[2] ~~Sie berücksichtigen dabei den gegenwärtigen Stand der Technik sowie die Grundsätze der Verhältnismässigkeit~~ Die technischen und ~~Wirtschaftlichkeit.~~organisatorischen Massnahmen müssen angemessen sein und insbesondere folgenden Kriterien Rechnung tragen: a) dem Zweck der Datenbearbeitung; b) der Art und dem Umfang der Datenbearbeitung; c) den möglichen Risiken für die betroffenen Personen; d) dem gegenwärtigen Stand der Technik; und e) der Verhältnismässigkeit und Wirtschaftlichkeit.
[3] Sie erstellen einen Massnahmenkatalog, der Auskunft gibt über den Zweck und die Kosten der vorgeschlagenen Massnahmen sowie den Zeitbedarf für deren Umsetzung.	[3] ~~Sie~~Die Organe erstellen einen Massnahmenkatalog, der Auskunft gibt über den Zweck und die Kosten der vorgeschlagenen Massnahmen sowie den Zeitbedarf für deren Umsetzung.
§ 5 Umsetzung [1] Die Organe beantragen die Umsetzung des Massnahmenkatalogs – je nach Zuständigkeit – bei den Direktionen, dem Obergericht, dem Verwaltungsgericht, der Staatskanzlei sowie den vorgesetzten gemeindlichen Stellen. Bei ausgelagerter Datenbearbeitung gehen die betreffenden Organe sinngemäss vor.	
[2] Die Organe sorgen für die Instruktion der Mitarbeitenden und überprüfen alle vier Jahre die Wirksamkeit der bisherigen Massnahmen.	[2] Die Organe ~~sorgen~~ sind verantwortlich für die Instruktion und Kontrolle der Mitarbeitenden und überprüfen ~~alle vier Jahre~~ periodisch die Wirksamkeit der ~~bisherigen~~getroffenen Massnahmen.
	§ 5a Datenschutz-Folgenabschätzung [1] Eine Datenschutz-Folgenabschätzung enthält insbesondere Angaben zu:

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
	a) Art der Personendaten, Kreis der betroffenen Personen, gesetzliche Grundlage, Zweck, Art und Umfang der Datenbearbeitung, gemeinsame Datenbearbeitungen, Kombination von Datensätzen, Zugriff auf Personendaten anderer Organe, automatisierte Entscheidfindung, Auftragsdatenbearbeitung, grenzüberschreitende Datenbekanntgaben, Kreis der Empfängerinnen und Empfänger bzw. der Zugriffsberechtigten, Aufbewahrungsdauer, Anwendungen, Systeme und Netzwerke, Technologien und Verfahren; b) Eintrittswahrscheinlichkeit, Schwere und potenzielle Auswirkungen der Risiken für die Grundrechte der betroffenen Personen; und c) technische sowie organisatorische Massnahmen und deren Auswirkungen auf die Risiken. [2] Die Organe halten das Ergebnis der Datenschutz-Folgenabschätzung schriftlich fest.
§ 6 Regierungsrat [1] Der Regierungsrat erlässt eine Weisung zur Überprüfung der Datensicherheit.	[1] Der Regierungsrat erlässt eine Weisung zur ~~Überprüfung~~Gewährleistung der ~~Datensicherheit~~Informationssicherheit.
§ 7 Kantonale Datenschutzstelle [1] Die kantonale Datenschutzstelle berät die Organe in grundsätzlichen Fragen der Datensicherheit und stellt Merkblätter für die Instruktion der Mitarbeitenden zur Verfügung.	[1] Die kantonale Datenschutzstelle berät die Organe in grundsätzlichen Fragen der ~~Datensicherheit und stellt Merkblätter~~ Informationssicherheit von Personendaten. Die Erstellung von Merkblättern für die Instruktion der Mitarbeitenden zur ~~Verfügung~~Informationssicherheit sowie einer Vorlage für die Erarbeitung eines Massnahmenkatalogs erfolgt durch das Security Board gemäss § 29 ITV[BGS 153.53].
§ 8 Amt für Informatik und Organisation [1] Das Amt für Informatik und Organisation erarbeitet zu Handen des Regierungsrats eine Weisung zur Überprüfung der Datensicherheit inklusive einer Vorlage für die Erabeitung eines Massnahmenkatalogs.	[1] *Aufgehoben.*

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
[2] Es berät die Organe des Kantons bei der Überprüfung der Datensicherheit und der Erstellung von Massnahmenkatalogen.	[2] ~~Es~~ Das Amt für Informatik und Organisation berät die Organe des Kantons bei der ~~Überprüfung~~Gewährleistung der ~~Datensicherheit~~Informationssicherheit und der Erstellung von Massnahmenkatalogen.
	II.
	1. Der Erlass BGS 153.53, Informatikverordnung (ITV) vom 13. November 2018 (Stand 1. Januar 2019), wird wie folgt geändert:
§ 18 IT-Sicherheit [1] Der Schutz der IT-Mittel richtet sich nach anerkannten Standards, der Schutz der damit bearbeiteten Personendaten nach dem Datenschutzgesetz[BGS [157.1]]] und der Datensicherheitsverordnung[BGS [157.12]]]. [2] Die IT-Mittel sind einer regelmässigen Überprüfung zu unterziehen. [3] Audit- und Controllingberichte zur IT-Sicherheit können mit verbindlichen Auflagen zu Handen der verantwortlichen zentralen bzw. dezentralen IT verbunden werden.	[1] Der Schutz der IT-Mittel richtet sich nach anerkannten Standards, der Schutz der damit bearbeiteten Personendaten nach dem Datenschutzgesetz[BGS [157.1]]] und der ~~Datensicherheitsverordnung~~Verordnung über die Informationssicherheit von Personendaten[BGS [157.12]]].
§ 29 Security Board [1] Das Security Board setzt sich zusammen aus: a) der bzw. dem Sicherheitsbeauftragten des AIO (Vorsitz), b) der Leitung Operation des AIO, c) einer Vertretung des Dienstes Informatik, Communication und Technik der Zuger Polizei, d) der bzw. dem Datenschutzbeauftragten, e) einer Vertretung der kantonalen Schulen und	d) einer Vertretung der ~~bzw. dem Datenschutzbeauftragten,~~Datenschutzstelle,

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
f) einer Vertretung der Einwohnergemeinden. [2] Es hat folgende Aufgaben und Kompetenzen: a) Erarbeitung von Weisungen zur Überprüfung der Datensicherheit sowie von Standards zur IT-Sicherheit; b) Initialisierung von Audits, Erarbeitung von Controllingberichten und Erteilung verbindlicher Auflagen zur IT-Sicherheit; c) Initialisierung von Sicherheitsprojekten; d) Festlegung von Massnahmen zur Abwehr von Cyber Angriffen; e) Durchführung von Schulungen zur IT-Sicherheit. [3] Es fasst seine Beschlüsse mit einfachem Mehr der anwesenden Mitglieder. Bei Stimmengleichheit entscheidet die bzw. der Vorsitzende.	a) Erarbeitung von Weisungen zur ~~Überprüfung~~Gewährleistung der ~~Datensicherheit~~Informationssicherheit sowie von Standards zur IT-Sicherheit;
	2. Der Erlass BGS 154.28, Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis vom 17. Dezember 2002 (Stand 1. Juli 2010), wird wie folgt geändert:
§ 5 Leeren des elektronischen Briefkastens und Abwesenheit [1] Der elektronische Briefkasten ist regelmässig abzurufen. Bei unerwarteter länger dauernder Abwesenheit namentlich infolge Krankheit, Unfall, Entlassung, Freistellung oder Tod einer bzw. eines Mitarbeitenden oder aufgrund einer speziellen Vereinbarung zwischen Mitarbeiterin bzw. Mitarbeiter und vorgesetzter Stelle oder bei unpflichtgemässer unterlassener Einrichtung einer Abwesenheitsmeldung trotz länger dauernder Abwesenheit kann die vorgesetzte Stelle veranlassen, dass der IT-Leistungserbringer auf dem entsprechenden E-Mail-Konto eine Abwesenheitsmeldung einrichtet.	

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
[2] Das automatische Umleiten von E-Mails an E-Mail-Adressen ausserhalb des kantonalen Netzes, wie beispielsweise an die private Mailbox, ist aus Gründen der Datensicherheit untersagt. Davon ausgenommen sind die Netze der kantonalen Schulen.	[2] Das automatische Umleiten von E-Mails an E-Mail-Adressen ausserhalb des kantonalen Netzes, wie beispielsweise an die private Mailbox, ist aus Gründen der ~~Datensicherheit~~Informationssicherheit untersagt. Davon ausgenommen sind die Netze der kantonalen Schulen.
	3. Der Erlass BGS 159.11, Verordnung zum Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum (Videoüberwachungsverordnung; VideoV) vom 21. Juni 2016 (Stand 2. Juli 2016), wird wie folgt geändert:
§ 4 Ausbildung der zur Auswertung Berechtigten [1] Die Polizei bildet die zur Auswertung berechtigten Stellen in Zusammenarbeit mit der Datenschutzstelle aus. [2] Die Ausbildung umfasst mindestens: a) die Auswertung der Aufzeichnungen; b) die Gewährleistung von Datenschutz und Datensicherheit. [3] Die Polizei stellt den Ausgebildeten eine Ausbildungsbestätigung aus.	b) die Gewährleistung ~~von Datenschutz und Datensicherheit~~der Informationssicherheit.
	4. Der Erlass BGS 215.313, Verordnung über die Führung des Grundbuchs mittels Informatik (IT-Grundbuch-Verordnung) vom 3. Oktober 1995 (Stand 1. Januar 2019), wird wie folgt geändert:
§ 6 Datensicherheit und Datenschutz [1] Für die Datensicherheit und den Datenschutz sind die vom Regierungsrat genehmigten Konzepte massgebend. [2] Im Übrigen gelten die Bestimmungen der Datenschutzgesetzgebung.	**§ 6** ~~Datensicherheit und Datenschutz~~Informationssicherheit [1] Für die ~~Datensicherheit und den Datenschutz~~Informationssicherheit sind die vom Regierungsrat genehmigten Konzepte massgebend.
	5.

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
	Der Erlass BGS 821.13, Verordnung über das Krebsregister vom 14. Dezember 2010 (Stand 1. Januar 2011), wird wie folgt geändert:
4. Datensicherheit	**4. ~~Datensicherheit~~Informationssicherheit**
§ 12 Datensicherheit und Kreis der Zugriffsberechtigten [1] Die medizinische Leitung und sämtliche Mitarbeitenden des Krebsregisters sind über Sachverhalte und Daten, die ihnen in Ausübung ihrer Tätigkeit zur Kenntnis gelangen und die von vertraulicher Natur sind, zur Verschwiegenheit verpflichtet. [2] Das Krebsregister trifft räumliche Zugangsbeschränkungen sowie angemessene technische und organisatorische Massnahmen gegen den unbefugten Zugriff auf die bearbeiteten Daten. Es erstellt insbesondere ein Zugriffsreglement, in dem es regelt, welche Personen zu welchem Zweck und unter welchen Bedingungen Zugang zu den nicht anonymisierten Personendaten haben. [3] Der Zugriff auf personenbezogene Daten ist auf Personen zu beschränken, die den Zugriff zur Erfüllung ihrer Aufgaben benötigen und die eine Erklärung über die ihnen auferlegte Schweigepflicht unterschrieben haben. Personen, die nicht für das Krebsregister arbeiten sowie Hilfs- und Servicepersonal darf kein Zugriff auf nicht anonymisierte Personendaten gewährt werden. [4] Die getroffenen Massnahmen haben dem Stand der Technik zu entsprechen. Insbesondere bei der Pseudonymisierung und Anonymisierung von Personendaten sind die bestehenden technischen Möglichkeiten zu nutzen. Die elektronische Bearbeitung der personenbezogenen Daten von krebskranken Personen hat zudem in einem logistisch getrennten EDV-System zu erfolgen. [5] Der Zugang zur Datenbank hat über eine Zutrittskontrolle zu erfolgen, die dem aktuellen Stand der Technik entspricht. Die Zugriffe auf die Datenbank sind zu dokumentieren und während mindestens zehn Jahren aufzubewahren. Die Protokolldaten dürfen keine Registerdaten enthalten.	**§ 12** ~~Datensicherheit~~Informationssicherheit und Kreis der Zugriffsberechtigten
	III.
	Keine Fremdaufhebungen.

Geltendes Recht	[M05] Ergebnis 1. Lesung RR vom 9. Juni 2020
	IV.
	Diese Änderungen treten am Tag nach der Publikation im Amtsblatt in Kraft[In-krafttreten am ...].
	Zug, ... Regierungsrat des Kantons Zug Der Landammann Stephan Schleiss Der Landschreiber Tobias Moser Publiziert im Amtsblatt vom ...