

Nr. 26

Informatikgesetz

vom 7. März 2005* (Stand 1. Januar 2007)

Der Grosse Rat des Kantons Luzern,

nach Einsicht in die Botschaft des Regierungsrates vom 27. Januar 2004¹,

beschliesst:

I. Allgemeine Bestimmungen

§ 1 *Zweck*

Dieses Gesetz legt die Organisation der Informatik fest und regelt den Einsatz der Informatikmittel unter Einbezug des Datenschutzes.

§ 2 *Geltungsbereich*

¹ Das Gesetz gilt für die kantonale Verwaltung (einschliesslich Spitäler und kantonaler Schulen) und für die Gerichte. Ausgenommen sind die Ausgleichskasse Luzern, die IV-Stelle Luzern, die Arbeitslosenkasse, die Gebäudeversicherung, die Luzerner Pensionskasse, die im Rahmen eines Konkordats geführten Hochschulen und Fachhochschulen sowie die Universität.

² Für die in Absatz 1 ausgenommenen Stellen und für andere vom Regierungsrat durch Verordnung bezeichnete Stellen gelten die Teile I, II und VI. Der Teil V ist für sie anwendbar, soweit sie Informatikmittel des Kantons Luzern benutzen.

³ Für die Gemeinden gelten die Teile I, II und VI.

⁴ Der Regierungsrat kann bestimmte Anlagen vom Geltungsbereich dieses Gesetzes ausnehmen.

* K 2005 563 und G 2005 87

¹ GR 2005 22

§ 3 *Begriffe*

¹ Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «betroffene Person», «Bearbeiten von Personendaten», «Datensammlung», «Inhaber einer Datensammlung» sowie «Organ» richten sich nach dem kantonalen Datenschutzgesetz.

² Der Begriff Informatik umfasst die Steuerung, Planung und Einführung sowie den Betrieb und Unterhalt von Prozessen und Techniken, welche der maschinellen oder maschinell unterstützten Bearbeitung von Informationen aller Art dienen.

³ Informatikmittel sind Geräte, Einrichtungen und Dienste, wie insbesondere Computersysteme, Computerprogramme, Kommunikationsdienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen.

⁴ Zentrale Datenbanken bestehen aus Datensammlungen verschiedener Organe. Sie können sich an einem beliebigen Ort befinden. Datenwarenhäuser und Datendreh scheiben sind zentrale Datenbanken.

⁵ Datenwarenhäuser (data warehouses) dienen der dauerhaften Speicherung von Daten.

⁶ In Datendreh scheiben stehen Daten für den Datenaustausch vorübergehend zur Verfügung.

⁷ Abrufverfahren sind automatisierte Verfahren, welche es Dritten ermöglichen, Personendaten ohne Intervention des bekanntgebenden Organs zu bearbeiten.

⁸ Eine Auslagerung ist das Zurückgreifen eines Organs auf Informatikmittel Dritter zur Erfüllung seiner Aufgaben. Organe innerhalb eines Gemeinwesens gelten nicht als Dritte.

§ 4 *Grundsätze*

¹ Die Informatik unterstützt die Wirtschaftlichkeit und die Wirksamkeit von Geschäfts- und von Lernprozessen.

² Der Informatikeinsatz muss wirtschaftlich sein, der Erfüllung der öffentlichen Aufgaben dienen und den Bedürfnissen der Benutzerinnen und Benutzer entsprechen.

³ Techniken, die geeignet sind, aus Daten oder Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen, dürfen nur dann eingesetzt werden, wenn die Voraussetzungen gemäss § 5 Absatz 2 des Datenschutzgesetzes² erfüllt sind.

² SRL Nr. 38. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

II. Zentrale Datenbanken und Abrufverfahren

§ 5 *Zulässigkeit zentraler Datenbanken*

¹ Die Errichtung und der Betrieb zentraler Datenbanken sind zulässig, sofern die Vorschriften über den Datenschutz und die Bestimmungen dieses Gesetzes eingehalten werden.

² Die Errichtung und der Betrieb zentraler Datenbanken setzen eine zwischen den angeschlossenen Organen und dem Betreiber abgeschlossene und durch die zuständigen Behörden genehmigte Leistungsvereinbarung voraus. Diese regelt mindestens folgende Punkte:

- a. Struktur der zentralen Datenbank,
- b. Inhalt der Datenbank insbesondere in Bezug auf Personendaten,
- c. verwendete Techniken, einschliesslich Entwicklung und Wartung,
- d. Zugriffsverwaltung,
- e. Sicherheits- und Datenlöschkonzept,
- f. Standort der Hardware,
- g. Kontrollrechte und -pflichten,
- h. Verantwortlichkeiten,
- i. Publikation gemäss § 10.

³ Der Regierungsrat kann, nachdem er die Stellungnahme des oder der Beauftragten für den Datenschutz eingeholt hat, vor Inkrafttreten eines formellen Gesetzes eine zentrale Datenbank mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen während einer einmaligen befristeten Zeitspanne von höchstens fünf Jahren bewilligen, wenn

- a. die Aufgaben, die diese Bearbeitung erforderlich machen, in einem formellen Gesetz geregelt sind,
- b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden,
- c. die praktische Umsetzung einer Datenbearbeitung vor Inkrafttreten eines formellen Gesetzes zwingend eine Testphase erfordert und
- d. die Zustimmung des zuständigen obersten Gerichtes vorliegt für den Fall, dass an der zentralen Datenbank ausschliesslich Organe des kantonalen Gerichtswesens beteiligt sind.

⁴ Wird eine zentrale Datenbank gestützt auf eine Bewilligung gemäss Absatz 3 betrieben, orientieren die an der zentralen Datenbank angeschlossenen Organe den Regierungsrat jährlich über den Stand der Projektarbeiten und über die Notwendigkeit der Weiterführung des Betriebs.

§ 6 *Betreiber*

¹ Der Betreiber einer zentralen Datenbank ist für den technischen Betrieb und die technische Sicherheit zuständig und verantwortlich.

² Betreiber kann ein an der zentralen Datenbank beteiligtes Organ, ein Organ der Informatik gemäss § 17 Absatz 2 oder, unter Vorbehalt der Bestimmungen über die Auslagerung, ein Dritter sein.

³ Dem Betreiber stehen die für die Erfüllung seiner Aufgaben erforderlichen Zugriffs- und Bearbeitungsrechte auf die gespeicherten Personendaten zu. Die Systemadministration und die Zugriffsverwaltung dürfen nicht derselben Person übertragen werden.

⁴ Der Betreiber und jede von ihm mit Aufgaben des Betriebs betraute Person ist über die von ihm wahrgenommenen Personendaten zur Verschwiegenheit verpflichtet.

⁵ § 6 Absatz 3 des Datenschutzgesetzes ist auf zentrale Datenbanken nicht anwendbar.

§ 7 *Zugriffsverwaltung und Löschung der Personendaten*

¹ Der Umfang der Zugriffs- und Bearbeitungsberechtigung von Organen auf Personendaten einer zentralen Datenbank bestimmt sich nach Massgabe des Datenschutzgesetzes und ist technisch und organisatorisch auf geeignete Weise sicherzustellen. § 6 Absatz 3 bleibt vorbehalten.

² Werden die in einem Datenwarenhaus gespeicherten Personendaten von keinem beteiligten Organ mehr benötigt, sind sie dem zuständigen Archiv zur Übernahme anzubieten. Werden sie vom Archiv als nicht archivwürdig eingestuft, sind sie umgehend zu löschen.

§ 8 *Erhebung von Personendaten*

¹ Personendaten, welche in einem Datenwarenhaus gespeichert werden sollen, können für mehrere Organe gemeinsam erhoben werden.

² Werden Personendaten, welche in einem Datenwarenhaus gespeichert werden sollen, für mehrere Organe gemeinsam erhoben, so ist die betroffene Person anlässlich der Erhebung auch auf die Speicherung ihrer Personendaten im Datenwarenhaus und auf die daran beteiligten Organe hinzuweisen.

§ 9 *Datenschutzfreundliche Technologien*

¹ Bei der Beschaffung von Informatikmitteln für zentrale Datenbanken ist die Datenschutzfreundlichkeit der Technologien angemessen zu berücksichtigen.

² Bevor Informatikmittel für zentrale Datenbanken beschafft werden, sind die zuständigen Aufsichtsstellen für den Datenschutz anzuhören. Sie können innert angemessener Frist eine Stellungnahme abgeben.

§ 10 *Publikation und Register*

¹ Die Errichtung von Datenwarenhäusern ist vom Betreiber vor der Betriebsaufnahme im Kantonsblatt zu publizieren. In der Publikation sind für jedes Datenwarenhaus die daran beteiligten Organe und die entsprechenden Datensammlungen sowie der Betreiber aufzuführen. Ferner hat die Publikation für jede Datensammlung Auskunft zu geben über die Rechtsgrundlage, den Zweck, die Mittel und Verfahren des Bearbeitens, die Art und Herkunft der Personendaten und deren regelmässige Empfänger sowie über das Vorhandensein und den Aufbewahrungsort von Kopien.

² In der Publikation sind ferner die Kontrollrechte jeder Person sowie die zuständigen Aufsichtsstellen für den Datenschutz gemäss diesem Gesetz und dem Datenschutzgesetz anzugeben.

³ Die zuständige Aufsichtsstelle für den Datenschutz führt ein Register über die Datenwarenhäuser. Das Register enthält die Angaben gemäss Absatz 1.

§ 11 *Kontrollrechte der betroffenen Person*

¹ Jede Person kann bei der zuständigen Aufsichtsstelle für den Datenschutz Auskunft verlangen

- a. über den Inhalt des Registers,
- b. ob über sie in einem Datenwarenhaus Personendaten gespeichert sind; sie hat sich dabei über ihre Identität auszuweisen.

² Die zuständige Aufsichtsstelle für den Datenschutz und der oder die zuständige Informatikverantwortliche prüfen gemeinsam, ob über die betroffene Person im Datenwarenhaus Personendaten gespeichert sind und welchen Organen dafür Zugriffs- oder Bearbeitungsrechte zustehen. Der zuständigen Aufsichtsstelle für den Datenschutz und dem oder der Informatikverantwortlichen stehen die dazu erforderlichen Zutrittsrechte zu den Räumen und Anlagen des Betreibers sowie die erforderlichen Zugriffs- und Bearbeitungsrechte auf im Datenwarenhaus gespeicherte Personendaten zu. Der Betreiber hat alle für die Prüfung notwendige Unterstützung zu leisten.

³ Die zuständige Aufsichtsstelle für den Datenschutz gibt der betroffenen Person Auskunft darüber, welche am Datenwarenhaus beteiligten Organe berechtigt sind, auf ihre Personendaten zuzugreifen oder sie zu bearbeiten. Die zuständige Aufsichtsstelle für den Datenschutz darf diese Auskunft aus überwiegenden öffentlichen Interessen oder überwiegenden privaten Interessen Dritter oder der betroffenen Person einschränken, mit Auflagen versehen oder verweigern.

⁴ Das Verfahren betreffend Auskunft über die über eine betroffene Person vorhandenen Personendaten sowie betreffend Einsicht, Berichtigung und anderen Ansprüchen richtet sich nach dem Datenschutzgesetz. Auf Begehren der betroffenen Person leitet die zuständige Aufsichtsstelle für den Datenschutz bei den Organen, welche berechtigt sind, auf ihre Personendaten zuzugreifen oder sie zu bearbeiten, das Verfahren ein.

⁵ Die Aufsichtsstellen für den Datenschutz und die Informatikverantwortlichen sind über die von ihnen wahrgenommenen Personendaten zur Verschwiegenheit verpflichtet.

§ 12 *Abrufverfahren*

Teil II dieses Gesetzes ist auf die Errichtung und den Betrieb von Abrufverfahren sinngemäss anwendbar. Vorbehalten bleiben die Vorschriften über Publikation und Register.

III. Auslagerung

§ 13 *Zulässigkeit*

¹ Die Auslagerung von Informatikdienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Die finanzrechtlichen Vorschriften bleiben vorbehalten.

² Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt:

- a. Inhalt der Dienstleistung,
- b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten,
- c. Verantwortlichkeiten,
- d. verwendete Techniken, einschliesslich Entwicklung und Wartung,
- e. Zugriffs- und Zutrittsrechte,
- f. Sicherheits- und Datenlöschkonzept,
- g. Standorte der Hardware und der Datenbearbeitung,
- h. Kontrollrechte,
- i. Beizug von Dritten,
- j. Archivierung,
- k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung.

³ Das auslagernde Organ stellt durch organisatorische oder technische Massnahmen sowie vertraglich sicher, dass die staatliche Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.

§ 14 *Genehmigungs- und Meldepflicht*

¹ Die Auslagerung von Informatikdienstleistungen von übergeordnetem oder strategischem Interesse bedarf der Genehmigung des Regierungsrates.

² Die übrigen Auslagerungsvorhaben sind vorgängig der zuständigen Behörde zu melden.

§ 15 *Pflichten des Auftragnehmers*

¹ Der Auftragnehmer, einschliesslich dessen Mitarbeitende und Hilfspersonen, muss diejenigen Amts-, Berufs- und besonderen Geheimhaltungspflichten übernehmen sowie die Bestimmungen über den Datenschutz und die Informatiksicherheit einhalten, an welche das auslagernde Organ gebunden ist.

² Er hat dem auslagernden Organ, der zuständigen Behörde für den Datenschutz sowie der Finanzkontrolle Zutritt zu den Räumen und Anlagen sowie die erforderlichen Zugriffsrechte auf die entsprechenden Daten zu gewähren und sie angemessen zu unterstützen.

§ 16 *Kontrollrechte der betroffenen Person*

¹ Als Inhaber der Datensammlung gilt das auslagernde Organ.

² Werden beim Auftragnehmer Kontrollrechte gemäss Datenschutzrecht geltend gemacht, hat dieser die betroffene Person an das auslagernde Organ zu verweisen und eine materielle Bearbeitung der Begehren zu unterlassen.

IV. Informatikorganisation

§ 17 *Organisationsstruktur*

¹ Die Informatikorganisation des Kantons Luzern besteht aus der Konzerninformatik und der Departementsinformatik.

² Der Regierungsrat bezeichnet die Organe der Informatik und bestimmt deren grundsätzliche Aufgaben, Funktionen und Zuständigkeiten.

³ Die Departementsinformatik ist unter Berücksichtigung der strategischen Vorgabe der Konzerninformatik Sache der Departemente, der Staatskanzlei sowie der obersten Gerichte.

V. Informatiksicherheit

§ 18 *Zuständigkeit*

¹ Die Informatikmittel sind durch den Inhaber einer Datensammlung beziehungsweise den Betreiber einer zentralen Datenbank gegen Verlust und unerwünschte Einwirkungen zu sichern. Personendaten sind vor unbefugtem Zugriff und unbefugter Bearbeitung zu schützen.

² Die Organe der Informatik unterstützen die Inhaber von Datensammlungen und die Betreiber von zentralen Datenbanken bei der Festlegung und der Umsetzung von Sicherheitsmassnahmen.

§ 19 *Grundsätze*

¹ Die Dienststellen und die Gerichte sowie die andern gemäss § 2 Absatz 2 dem Geltungsbereich unterliegenden Stellen klassifizieren die Daten und die Informatikmittel und legen gestützt darauf die Schutzziele fest. Sie erstellen einen Massnahmenplan zur Erreichung der Schutzziele.

² Schutzziele und Massnahmenplan sind periodisch zu überprüfen.

³ Der Regierungsrat regelt das Nähere.

§ 20 *Benutzung von Informatikmitteln am Arbeitsplatz*

¹ Alle Anwenderinnen und Anwender sind für die Benutzung der Informatikmittel im Rahmen der geltenden Rechtsordnung und dieses Gesetzes persönlich verantwortlich. Informatikmittel dürfen nicht in missbräuchlicher Weise benutzt werden.

² Der Regierungsrat regelt die Benutzung der Informatikmittel am Arbeitsplatz und bezeichnet die Fälle der missbräuchlichen Benutzung.

³ Für Kontroll- und Überwachungsmassnahmen gelten die folgenden Grundsätze:

- a. Kontroll- und Überwachungsmassnahmen dienen in erster Linie der Überprüfung und der Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel.
- b. Sämtliche Internetzugriffe und der gesamte E-Mail-Verkehr der Anwenderinnen und Anwender werden aufgezeichnet (protokolliert). Der Inhalt der E-Mails darf ohne Zustimmung der betroffenen Anwenderinnen und Anwender nicht gelesen werden. Von diesem Grundsatz darf nur abgewichen werden, wenn es für die staatliche Aufgabenerfüllung unerlässlich ist.
- c. Protokolldaten sind in anonymisierter Form auszuwerten.
- d. Personenbezogene Auswertungen sind ausnahmsweise zulässig, sofern die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel ernsthaft gefährdet sind und dies zur Störungsbehebung unumgänglich ist. Diese Auswertungen dürfen sich nicht auf den Inhalt von E-Mails und Internetzugriffen beziehen.
- e. Bei begründetem Verdacht auf Missbrauch von Informatikmitteln sind nach schriftlicher Ankündigung personenbezogene Auswertungen möglich, welche sich auch auf den Inhalt von E-Mails und Internetzugriffen beziehen.
- f. Technische Überwachungs- und Kontrollinstrumente sowie Filtersperren sind mit Ausnahme sogenannter Spionageprogramme zulässig.

⁴ Der Regierungsrat regelt das Nähere, insbesondere das Kontrollverfahren. Er kann insbesondere vorsehen, anonymisierte Plausibilitätskontrollen über eine jeweils beschränkte Benutzungsdauer durchführen zu lassen.

VI. Schlussbestimmungen

§ 21 *Zuständige Behörde*

¹ Der Regierungsrat bestimmt die zuständige Behörde gemäss § 5 Absatz 2 und § 14 Absatz 2.

² In den Gemeinden bestimmt der Gemeinderat die zuständige Behörde.

§ 22 *Änderung von Erlassen*

Folgende Erlasse werden gemäss Anhang³ geändert:

- a. Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990⁴,
- b. Gesetz über die Kantonspolizei vom 27. Januar 1998⁵.

§ 23 *Strafen und Massnahmen*

¹ Wer die Vorschriften der §§ 4 Absatz 3, 6 Absatz 4, 10 Absatz 1 und 15 Absatz 1 verletzt, wird mit Busse bis 5000 Franken bestraft.⁶

² Der Regierungsrat kann durch Verordnung für Verstösse gegen die Vorschriften von § 20 oder gegen Ordnungsbestimmungen, die gestützt auf diese Bestimmung erlassen werden, Bussen bis zu 3000 Franken vorsehen.

³ An die Stelle der Strafe kann eine Massnahme treten, sofern der Fehlbare einwilligt. Diese besteht aus einem Datenschutzunterricht auf Kosten des Fehlbaren.

⁴ Der oder die Beauftragte für den Datenschutz organisiert den Datenschutzunterricht. Dieser kann durch Dritte erteilt werden.

⁵ Vorbehalten bleiben die Bestimmungen des Schweizerischen Strafgesetzbuches⁷.

³ Die Erlassänderungen, die der Grosse Rat am 7. März 2005 zusammen mit dem Informatikgesetz beschlossen hat, bilden gemäss § 22 einen Bestandteil dieses Gesetzes. Sie wurden in einem Anhang wiedergegeben, der am 21. Mai 2005 in der Gesetzessammlung veröffentlicht wurde (G 2005 96). Bei der vorliegenden Ausgabe wird auf die Wiedergabe dieses Anhangs mit den Erlassänderungen verzichtet.

⁴ SRL Nr. 38

⁵ SRL Nr. 350

⁶ Fassung gemäss Änderung des Gesetzes über die Strafprozessordnung vom 11. September 2006, in Kraft seit dem 1. Januar 2007 (G 2006 277).

⁷ SR 311.0

§ 24 *Inkrafttreten*

Das Gesetz tritt am 1. Juli 2005 in Kraft. Es unterliegt dem fakultativen Referendum⁸.

Luzern, 7. März 2005

Im Namen des Grossen Rates

Die Präsidentin: Bernadette Schaller-Kurmann

Der Staatsschreiber: Viktor Baumeler

⁸ Die Referendumsfrist lief am 11. Mai 2005 unbenützt ab (K 2005 1198).