

# Kurze Einführung in das luzernische Gesetz über den Schutz von Personendaten

## A. Verschiedene Erlasse im Bereich des Datenschutzes

1. Der Kanton Luzern hat am 2. Juli 1990 das Gesetz über den Schutz von Personendaten erlassen (SRL Nr. 38; nachfolgend **DSG-LU**). Am 26. Februar 1991 wurde noch die entsprechende Verordnung zum Datenschutzgesetz (SRL Nr. 38b; nachfolgend **VDSG-LU**) erlassen. Wichtige datenschutzrechtliche Bestimmungen befinden sich in der Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz vom 10. Dezember 2002 (SRL Nr. 38c). Beachtenswert sind zudem: das Synodalgesetz zum **kirchlichen Datenschutz**, Satzung zum kirchlichen Datenschutz vom 27. Oktober 2004/2. Mai 2004 (veröffentlicht im Kantonsblatt Nr. 46, vom 13. November 2004, S. 2883 ff.), die Verordnung über die **Verwaltung und Aufbewahrung von Akten durch das Verwaltungsgericht** und die seiner Aufsicht unterstellten Schätzungskommissionen vom 3. November 2004 (SRL Nr. 47), die Verordnung über die **Aufbewahrung von gerichtlichen Akten** vom 19. Dezember 2003 (SRL Nr. 262), das Reglement **über die Information** durch die Zivil- und Strafgerichte vom 26. November 2004 (SRL Nr. 262a), das Gesetz über das **Archivwesen** vom 16. Juni 2003 (SRL Nr. 585) sowie das Gesetz über die **Geoinformation** und die amtliche Vermessung vom 8. September 2003 (SRL Nr. 29). Das parlamentarische Verfahren zu einem **Informatikgesetz** wurde eingeleitet (siehe Botschaft des Regierungsrates an den Grossen Rat zum Entwurf eines Informatikgesetzes vom 27. Januar 2004, B 38).

## B. Begriffe

### a. Begriffe im DSG-LU

2. § 2 DSG-LU enthält verschiedene Begriffsbestimmungen. Diese werden nachfolgend kurz erläutert.
3. **Personendaten:** Gemäss § 2 Abs. 1 DSG-LU sind Personendaten „Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person oder eine Personengesellschaft des Handelsrechts“. Bestandteile der Begriffsumschreibung:
  - 3.1 Unter **Angaben** ist jede Art von Information zu verstehen (Tatsachenfeststellung, Werturteil usw.), ungeachtet der verwendeten Technik (analoges oder digitales Zeichen, Wort, Bild, Ton oder Kombination), der Datenträger (Papier, Film, elektronische Datenträger) und des Übermittlungswegs (unter Anwesenden, per Post oder elektronische Übermittlung). Nicht erfasst ist hingegen das Wissen einer Person, welches nirgends festgehalten oder gespeichert ist (zur Begriffsumschreibung).
  - 3.2 **Bestimmte Person:** Eine Person ist dann bestimmt, wenn sie aus der Information selbst eindeutig identifiziert werden kann (z.B. Nennung des Namens und der Adresse). Diese Identifikation kann auch über einen in der Information enthaltenen eindeutigen Schlüssel möglich sein (AHV-Nummer, Personenidentifikationsnummer, Kundennummer usw.).
  - 4.3 **Bestimmbare Person:** Eine Person ist dann bestimmbar, wenn sie aus der Information selbst zwar nicht eindeutig identifiziert werden kann, indes eine solche Identifikation durch die Kombination verschiedener Informationen ohne einen unverhältnismässigen Aufwand möglich ist. Ob der notwendige Aufwand verhältnismässig ist oder nicht beurteilt sich im konkreten Fall jeweils nach objektiven Kriterien und nach dem Stand der Technik. Nur wenn ein Rückschluss oder eine Zuordnung von Personendaten auf eine Person einen unverhältnismässigen Aufwand verursachen würde, kann man von anonymisierten Daten sprechen, welche wie Sachdaten behandelt werden (z.B. in der Statistik).
4. **Betroffene Personen:** Als betroffene Person bezeichnet § 2 Abs. 3 DSG-LU alle Personen oder Personengesellschaften, auf welche sich die Angaben beziehen. Damit spricht das Gesetz mehrere Punkte an:
  - 4.1 Der Datenschutz ist grundsätzlich **auf Personen oder Personengesellschaften** anwendbar. Dadurch wird die Verknüpfung des Datenschutzes mit der Persönlichkeit bzw. mit einer gesetzlichen Gesellschaftsform ersichtlich.
  - 4.2 Da der Datenschutz an die Persönlichkeit geknüpft wird, ist er **durch deren Existenz** bestimmt. Die Person kommt grundsätzlich von Geburt an bis zu ihrem Tod (bzw. von der Gründung an bis zu ihrer Auflösung, für juristische Personen) in den Genuss des Datenschutzes (siehe auch Art. 31 ZGB). Das bedeutet aber nicht, dass nach dem Tod einer Person sämtliche Datenbearbeitungen ohne weiteres zulässig wären. Die Rechtsprechung hat im Gegenteil sehr nuancierte Regeln aufgestellt, die

es Dritten (bzw. Angehörigen) erlauben, eine unzulässige Datenbearbeitung zu untersagen.

Nach dem Tod kann keine Person mehr einen Persönlichkeitsschutz **für sich selbst** geltend machen. Es kann auch niemand im Namen des Verstorbenen Rechte geltend machen. Dies schliesst indes nicht aus, dass nahe Angehörige für den Schutz der den Tod überdauernden Persönlichkeitsgüter besorgt sind, indem sie sich hierfür auf ihr eigenes Persönlichkeitsrecht berufen, das mindestens in einem gewissen Umfang auch die Wahrung des Ansehens naher Verwandter zum Gegenstand haben kann. Die Angehörigen haben ein berechtigtes Interesse daran, dass eine verstorbene Person nicht verunglimpft wird und keine negativen persönlichkeitsrelevanten Umstände über sie publiziert werden

Das Verbot von persönlichkeitsverletzenden Datenbearbeitungen hängt nicht von der Existenz des einzelnen Individuum ab. Infolgedessen sind die einschlägigen Datenschutzgesetze auch für die Bearbeitung von Personendaten eines verstorbenen Menschen anwendbar. Für die Bekanntgabe ihrer Daten kann die Zustimmung verstorbener Personen weder eingeholt noch vorausgesetzt werden. In Bezug auf die Bekanntgabe von Daten verstorbener Personen wird die Auskunft erteilt, sofern der Gesuchsteller ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen. Das ärztliche Berufsgeheimnis gilt auch nach dem Tod der geheimnisberechtigten Person. Ihr Recht, die Arztperson vom Berufsgeheimnis zu entbinden, ist höchstpersönlicher Natur. Nur ein gegenüber dem Geheimhaltungsinteresse deutlich höherwertiges öffentliches oder privates Offenbarungsinteresse rechtfertigt die Befreiung vom Berufsgeheimnis.

4.3 Anders als in anderen Rechtsordnungen (so zum Beispiel in Deutschland § 3 Abs. 1 BDSG) schützt das DSG auch die **juristische Person**. Das Bundesgericht hat schon vor der Normierung des Datenschutzes der juristischen Person einen „generellen Persönlichkeitsschutz“ zugesprochen, sofern ein Anspruch nicht Eigenschaften voraussetzt, die ihrer Natur nach nur dem Menschen, also der natürlichen Person zukommen. Deshalb war es für den Gesetzgeber klar, dass der Datenschutz grundsätzlich auch die juristische Person erfasst

5. **Besonders schützenswerte Personendaten** : Alle Personendaten haben nicht die gleiche Bedeutung für die betroffene Person. Da die Gefahr einer Persönlichkeitsverletzung bei bestimmten Informationen vom Gesetzgeber höher gewichtet wird, hat er einen **abschliessenden Katalog** von besonders schützenswerten Personendaten festgelegt (§ 2 Abs. 2 DSG-LU). Es handelt sich hierbei um Daten über:

5.1 die religiöse, weltanschauliche oder politische Haltung;

5.2 die Gesundheit, die Intimsphäre oder die ethnische Zugehörigkeit;

5.3 Massnahmen der Sozialhilfe;

5.4 administrative oder strafrechtliche Massnahmen und Sanktionen.

Angaben über das steuerbare Vermögen und Einkommen gehören demnach nicht zu den besonders schützenswerten Daten.

6. **Persönlichkeitsprofil** : Das Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt (§ 2 Abs. 2 DSG-LU). Aus dieser Umschreibung ist ersichtlich, dass der Gesetzgeber Persönlichkeitsprofile juristischer Personen nicht erfasst. Der Begriff des Persönlichkeitsprofils kann nicht generell definiert werden, sondern hängt auch von den konkreten Umständen (der Zusammenhang, in dem die Daten verwendet werden) ab. Für die Frage, ob eine Zusammenstellung mehrerer Daten einer bestimmten Person ein Persönlichkeitsprofil ergibt, sind Menge und Inhalt der personenbezogenen Informationen ausschlaggebend. Daten, die über einen längeren Zeitraum zusammen-

getragen werden und so ein biographisches Bild ergeben ("Längsprofil"), sind eher als Persönlichkeitsprofil zu qualifizieren als solche, die eine blosser Momentaufnahme darstellen ("Querprofil"). Name, Vorname, Adresse, Geburtsdatum und bestandene Prüfung ergeben in der Regel noch kein Persönlichkeitsprofil. Hingegen ist das Konsumverhalten einer Person (z.B. erhoben dank einer Kundenkarte) als Persönlichkeitsprofil zu werten.

7. **Bearbeiten:** Unter dem Begriff "bearbeiten" versteht der Gesetzgeber jeden Umgang mit Personendaten, unabhängig von den angewandten Mittel und Verfahren, insbesondere das Erheben, Beschaffen, Aufzeichnen, Sammeln, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (§ 2 Abs. 4 DSG-LU). Damit will der Gesetzgeber sowohl in zeitlicher (Beschaffung bis Vernichtung) als auch in verfahrensmässiger Hinsicht (ungeachtet der angewandten Mittel und Verfahren) alle Handlungen erfassen, welche Personendaten betreffen können. Die Aufzählung des Gesetzgebers ist nicht abschliessend („wie das“) und kann damit der technischen Entwicklung Rechnung tragen.
8. **Datensammlung :** Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind, ist eine Datensammlung im Sinne von § 2 Abs. 5 DSG-LU. Es handelt sich also um einen Bestand von Personendaten (Liste, Ordner, Aktenablage, elektronischer Datenträger usw.), der mit einem vernünftigen Aufwand erlaubt, Daten nach Personen zu finden. Dabei kommt es nicht darauf an, dass eine Datensammlung zentral oder dezentral geführt wird, sich an einem oder an mehreren Orten befindet. Ebenso wenig sind Form oder Struktur der Datensammlung entscheidend, solange die Personendaten nach Personen aussortiert werden können .
9. **Inhaber der Datensammlung:** Der Gesetzgeber definiert den Inhaber einer Datensammlung als Organ, das über den Zweck und den Inhalt einer Datensammlung entscheidet (§ 2 Abs. 6 DSG-LU).

Die Legaldefinition ist sehr stark von der Entstehungsgeschichte des DSG-LU bzw. vom Stand der Technologie in den achtziger Jahren des letzten Jahrtausends geprägt. Mit den heutigen technologischen Mitteln ist es nicht immer möglich den Inhaber einer Datensammlung zweifelsfrei zu bestimmen. Dies gilt insbesondere für zentrale Datensammlungen (so genannte **Datenpools**): Mehrere Organe bringen Personendaten in eine einzige Datensammlung ein und bearbeiten diese gemeinsam. Es ist oft schwierig in einem solchen Gebilde einen "Inhaber der Datensammlung" im Sinne des Gesetzes ausfindig zu machen. Entweder müssen alle Beteiligte als solche gelten oder oftmals keiner. Bei den Datenpools entsteht eine neue, vom Gesetzgeber nicht erfasste, Funktion: die des Betreibers des Datenpools.
10. **Organe** sind "Behörden, Dienststellen und Verwaltungseinheiten, die für ein Gemeinwesen handeln, und private Personen, soweit ihnen öffentliche Aufgaben übertragen sind“ (§ 2 Abs. 7 DSG-LU).

## b. Weitere Begriffe

11. **Abrufverfahren** (auch „Online-Zugriff“ genannt): Unter einem Abrufverfahren versteht man jedes automatisierte Verfahren, welches einem Dritten ermöglicht, über die Daten ohne Intervention des bekanntgebenden Organs zu verfügen. Im Sinne der Rationalisierung und der Vermeidung von Redundanzen ist das Abrufverfahren eine sehr effiziente Massnahme. Es erlaubt dem informationssuchenden Organ, sich seine Informationen anhand des Datenbestandes eines anderen Organs selber, zielgerichtet und fristgerecht zu beschaffen (sozusagen im „Selbstbedienungsverfahren“). Dies entspricht ganz dem Geiste des „New Public Management“. Ein oft zitiertes Anwendungsbeispiel für Abrufverfahren sind „Websites“ der öffentlichen Verwaltung, bei denen sich sowohl Private (im Sinne von E-Government) wie staatliche Organe mit Informationen und manchmal auch mit Personendaten eindecken können.
12. **Amtshilfe** ist die gegenseitige Unterstützung von Verwaltungseinheiten (die in keinem Subordinationsverhältnis zueinander stehen) bei deren gesetzlicher Aufgabenerfüllung durch Hilfeleistungen, die nicht verfahrensrechtlich (zivil-, straf- oder verwaltungsprozessual) geregelt sind. Beim Datenschutz steht die informationelle Amtshilfe im Vordergrund.
13. **Datenpool** (auch zentrale Datenbank oder Data Warehouse genannt): Der Datenpool im hier verwendeten Sinne ist eine zentrale Grossdatenbank, welche von den operativen Systemen in der Regel (aber nicht notwendigerweise) losgelöst ist und in der die erfassten Daten regelmässig aus den verschiedenen operativen Datenverarbeitungssystemen zwecks Auswertung zusammengeführt und aktualisiert werden. Hauptmerkmal eines Datenpools ist die Tatsache, dass mehrere Beteiligte Daten zur Verfügung stellen und, dass mehreren Beteiligten (nicht nur die eigenen) Daten zur Verfügung gestellt werden.
14. **Rechtshilfe** ist die gegenseitige Unterstützung staatlicher Stellen durch die Vornahme von verfahrensrechtlich (zivil-, straf- oder verwaltungsprozessual) geregelten Handlungen mit Ausnahme des erstinstanzlichen Verwaltungsverfahrens.

## C. Die Grundsätze des Datenschutzes

15. Das DSG-LU enthält verschiedene Grundsätze, welche mit denen des Bundesgesetz über den Datenschutz vom 19. Juli 1992 (SR 235; nachfolgend **DSG**) vergleichbar sind:
  - 15.1 Rechtmässige Bearbeitung: § 4 Abs. 1 DSG-LU;
  - 15.2 Treu und Glauben: § 4 Abs. 4 DSG-LU;
  - 15.3 Verhältnismässigkeit: § 4 Abs. 3 DSG-LU sowie § 5 VDSG-LU;
  - 15.4 Zweckbindung: § 4 Abs. 4 DSG-LU;
  - 15.5 Integrität: § 4 Abs. 2 DSG-LU;
  - 15.6 Datensicherheit: § 7 DSG-LU sowie § 6 VDSG-LU;

## a. **Rechtmässige Bearbeitung**

16. Der Grundsatz der Rechtmässigkeit der Bearbeitung von Personendaten bedeutet, dass sowohl die Beschaffung wie die Verwendung der Personendaten nicht rechtswidrig erfolgen darf. Eine rechtswidrige Beschaffung von Personendaten liegt dann vor, wenn **gegen eine Norm verstossen** wird. Diese Norm kann im StGB (Art. 179 ff. StGB), im Privatrecht (Art. 28 f. OR) oder im DSGVO selbst (§§ 4 f. DSGVO) verankert sein. Mit anderen Worten ist die Verletzung der Rechtsordnung für die Bearbeitung (inkl. Beschaffung) von Personendaten unzulässig.

## b. **Treu und Glauben**

17. Der Grundsatz von Treu und Glauben (siehe auch Art. 2 Abs. 1 ZGB) ist bei der **Erkennbarkeit** und der **Transparenz** der Datenbearbeitung von grosser Bedeutung. Eine Verletzung dieses Grundsatzes kann beispielsweise vorliegen, wenn ohne Wissen der betroffenen Person Telefongespräche aufgezeichnet werden. Ebenso muss in der Regel davon ausgegangen werden, dass die notwendigen Personendaten bei der betroffenen Person (und nicht bei Dritten) beschafft werden (§ 8 DSGVO).

## c. **Verhältnismässigkeit**

18. Eine Massnahme ist **verhältnismässig** – im Sinne von Art. 36 Abs. 3 BV – wenn sie für die Erreichung eines im Gesetz verankerten Zwecks notwendig (geringstmöglicher Eingriff) und geeignet (Zwecktauglichkeit) ist und wenn zwischen der Massnahme und dem Zweck ein vernünftiges Verhältnis besteht (Verhältnismässigkeit im engeren Sinne).

## d. **Zweckbindung**

19. Personendaten dürfen nur zum Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Dieser Grundsatz setzt einerseits voraus, dass der Bearbeitungszweck bei der Erhebung von Personendaten bestimmt und bekannt ist. Personendaten dürfen nicht auf Vorrat, ohne konkretes Ziel, beschafft werden. Andererseits müssen gemäss dem vorgenannten Grundsatz von Treu und Glauben Personendaten in der Regel direkt bei der betroffenen Person unter Angabe des Zweckes beschafft werden (Transparenz). Damit kann die betroffene Person die ungefähre Tragweite des Eingriffs in ihre Persönlichkeitsrechte abwägen. Wenn aber die bearbeitende Person die Personendaten der betroffenen Person für einen anderen Zweck verwenden will oder Dritten bekanntgibt, die einen anderen

Bearbeitungszweck geltend machen, wird das Vertrauen gebrochen und der Eingriff in die Persönlichkeit entspricht nicht mehr dem ursprünglich angegebenen.

20. Zum Zweckbindungsgebot bestehen zwei Ausnahmen:

20.1 Die (freie und aufgeklärte) **Einwilligung** der betroffenen Person: Die betroffene Person kann ohne weiteres nachträglich auch andere Verwendungszwecke zulassen, als die bei der Beschaffung angegebenen. Diese Aussage ist aber insofern zu relativieren, als eine Einwilligung in der Regel keine fehlende gesetzliche Grundlage ersetzen kann. Hier gilt also die Einwilligung nur wenn der neue Zweck zusätzlich noch durch eine gesetzliche Grundlage abgedeckt ist.

20.2 Das **Gesetz**: Gesetzesbestimmungen können dazu führen, dass die datenbearbeitende Person oder das Organ eigene Daten für andere Zwecke benutzen dürfen oder zur Verfügung stellen müssen (z.B. Art. 91 Abs. 5 SchKG; siehe aber auch Art. 19 DSG).

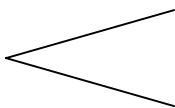
#### e. **Integrität**

21. Der Grundsatz der Integrität von bearbeiteten Personendaten bedeutet, dass diese richtig sein müssen. Es handelt sich um eine wichtige materielle Pflicht des Datenbearbeiters. Von diesem Grundsatz leiten sich folgerichtig die Kontrollrechte der betroffenen Person ab (§§ 15 ff. DSG-LU). Grundsätzlich müssen Personendaten **nachgeführt bzw. korrigiert** werden, wenn sie nachträglich unrichtig werden. Diese Pflicht entfällt aber, wenn die Information nur eine Momentaufnahme enthält, welche zum massgeblichen Zeitpunkt richtig war.

#### f. **Datensicherheit**

22. Die Datensicherheit ist ein Grundsatz des Datenschutzes, der in seiner Tragweite und seiner Bedeutung kaum überschätzt werden kann. Ohne Datensicherheit ist ein wirksamer Datenschutz nicht möglich. Personendaten müssen durch **angemessene technische und organisatorische Massnahmen** gegen unbefugtes Bearbeiten geschützt werden. Angemessen heisst im Bereich der Datensicherheit, dass die Massnahmen dem Gefährdungspotential entsprechen müssen. Die Adressliste eines lokalen Sportvereins ist nicht gleich zu schützen wie die elektronische Datenbank eines Strafgerichtes.

23. Die Datensicherheit kann sogar als eigener Bereich des Datenschutzes betrachtet werden. In einer schematischen Darstellung würde dies bedeuten, dass der Datenschutz wie folgt zu unterteilen ist:

Der Datenschutz besteht aus:  dem Datenschutz im engeren Sinne  
und  
der Datensicherheit

24. Der **Datenschutz im engeren Sinne** muss die Frage beantworten, wer, wann, unter welchen Voraussetzungen, in welchem Ausmass, welche Personendaten, bearbeiten darf (materielle Zulässigkeit der Datenbearbeitung). Die **Datensicherheit** muss ihrerseits die Frage beantworten, welche organisatorischen und technischen Massnahmen zu ergreifen sind, damit nur die berechtigten Personen die Personendaten bearbeiten können. Primäres Ziel der Datensicherheit ist also die Vermeidung der Bearbeitung von Personendaten durch Unbefugte.
25. Die Lehre geht aber noch weiter in ihren Anforderungen an die Datensicherheit. Es sind nicht nur **Vertraulichkeit** (nur Berechtigte haben Zugriff) sondern auch **Verfügbarkeit** (Personendaten stehen für die Bearbeitung zum gewünschten Zeitpunkt zur Verfügung), **Integrität** (der Inhalt der Personendaten kann nicht unzulässig verändert oder vernichtet werden) und **Authentizität** (Übereinstimmung zwischen dem angegebenen Benutzer und dem effektiven Benutzer) sicherzustellen. Zumindest die Verfügbarkeit scheint aber kein spezifisches Datenschutzproblem darzustellen.

## D. Der Geltungsbereich

26. **Persönlicher Geltungsbereich:** Das DSG-LU ist auf den Kanton und auf die Einwohnergemeinden anwendbar (§ 3 Abs. 1 DSG-LU). Zudem gilt es für die Bürger-, Kirch- und Korporationsgemeinden sowie für die Gebäudeversicherung des Kantons Luzern (§ 3 VDSG-LU). Gemäss Verweis von § 3 Abs. 1 lit. c DSG-LU gilt das Gesetz auch für die vermögensfähigen Verwaltungseinheiten des Kantons, der Gemeinden und der Landeskirchen, wie Anstalten mit Rechtspersönlichkeit, Körperschaften, Zweckverbände und andere Organisationen des öffentlichen Rechts. Schliesslich ist es noch auf private Personen anwendbar, soweit ihnen öffentliche Aufgaben übertragen sind (§ 2 Abs. 7 DSG-LU).
27. **Sachlicher Geltungsbereich:** Das DSG-LU findet grundsätzlich auf alle Bereiche des kantonalen öffentlichen Rechts Anwendung. Ausnahmen werden durch § 3 Abs. 2 DSG abschliessend aufgezählt:
- 27.1 Hängige Verfahren der Zivil- und Strafrechtspflege sowie hängige, durch Entscheid zu erledigende Verwaltungssachen (siehe dazu § 4 VDSG-LU): Hier zeigt sich ein markanter **Unterschied zum DSG**. Erstinstanzliche durch Entscheid zu erledigende Verwaltungsverfahren sind nach Wortlaut von § 3 Abs. 2 Bst. a DSG-LU dem Datenschutzrecht entzogen. Ob und inwiefern dieser Wortlaut auch einer umfassenden und verfassungskonformen Auslegung der Bestimmung standhält ist unklar. Da dieser Wortlaut in der Schweiz ziemlich einzigartig ist, kann nicht ausgeschlossen werden, dass er differenziert auszulegen ist.
- 27.2 Geschäfte über welche die Stimmberechtigten oder Parlamente beschliessen: Dies bedeutet, dass beispielsweise die Bearbeitung von Personendaten für Einbürgerungsgeschäfte vor der Gemeindeversammlung oder dem Gemeindeparlament nicht durch das DSG-LU erfasst sind. Trotzdem muss die Privatsphäre der



- Einbürgerungswilligen berücksichtigt werden, da Art. 13 BV und insbesondere Art. 36 Abs. 4 BV auch auf solche Geschäfte anwendbar sind.
- 27.3 Öffentliche Register des Privatrechtsverkehrs (insbesondere das Grundbuch, das Handelsregister und das Zivilstandsregister).
- 27.4 Verwaltungsinterne Akten wie Notizbücher und Agenden, die dem Inhaber als persönliche Arbeitsmittel dienen.

## E. Die Bekanntgabe von Personendaten

28. Die **Einwohnerkontrollen** geben auf Gesuch Namen, Vornamen, Geschlecht, Geburtsdatum und Adresse bekannt, sofern ein schutzwürdiges Interesse glaubhaft gemacht wird (§ 11 Abs. 1 DSG-LU). Die Gemeinden können aber in einem Reglement oder in der Gemeindeordnung festhalten, dass diese Personendaten auch ohne schutzwürdiges Interesse zu politischen, kulturellen, gesellschaftlichen, wohltätigen und wissenschaftlichen Zwecken veröffentlicht oder bekanntgegeben werden (§ 11 Abs. 3 DSG-LU). Von dieser Möglichkeit haben viele Gemeinden Gebrauch gemacht. Das führt dazu, dass beispielsweise runde Geburtstage in einem Informationsorgan der Gemeinde öffentlich mitgeteilt werden können. Soweit die vorgenannten Personendaten zur Wahrung des schutzwürdigen Interesses nicht ausreichen, darf die Einwohnerkontrolle auch Auskunft über den Beruf und Titel von Einzelpersonen, Zivilstand, Heimatort, Staatsangehörigkeit und zivilrechtliche Handlungsfähigkeit sowie über Ort und Datum des Zu- und Wegzugs geben (§ 11 Abs. 2 DSG-LU). Jede betroffene Person kann diese Bekanntgaben durch die Einwohnerkontrolle **sperr**en lassen. Dieses Sperrecht ist aber nicht absolut (siehe dazu § 11 Abs. 4 DSG-LU).

29. Für die Bekanntgabe von Personendaten der **Polizei**, lautet § 7 VDSG-LU wie folgt:

<sup>1</sup> Soweit nicht ein Rechtssatz dazu verpflichtet oder ermächtigt, dürfen Personendaten, die von der Polizei ausserhalb hängiger Strafverfahren zur Verhütung oder Verfolgung strafbarer Handlungen bearbeitet werden, nichtpolizeilichen Organen oder Dritten nur auf schriftliches Gesuch hin und nur mit Einwilligung des Vorstehers des Sicherheitsdepartementes bekanntgegeben werden. Im Gesuch ist darzulegen, dass die Voraussetzungen des § 9 Absatz 1b bzw. des § 10 Absatz 1b des Datenschutzgesetzes erfüllt sind.

<sup>2</sup> Für das Bekanntgeben bestimmter Personendaten kann der Vorsteher des Sicherheitsdepartementes seine Befugnis zur Einwilligung an die Polizeikommandanten delegieren.

Für die Bekanntgabe von Personendaten ist aber noch § 4 Abs. 2 Gesetz über die Kantonspolizei vom 27. Januar 1998 (SRL Nr. 350) als besonderer ermächtigender Rechtssatz im Sinne von § 7 Abs. 1 VDSG-LU zu berücksichtigen. Dieser lautet wie folgt:

„Sie kann Daten im Rahmen der Zusammenarbeit mit Polizeiorganen anderer Gemeinwesen und mit staatlichen Institutionen erheben, bearbeiten und weitergeben. Daten dürfen nur weitergegeben werden, wenn dies zur Erfüllung der gesetzlichen Aufgaben der Informationsempfängerinnen und -empfänger erforderlich ist.“

30. § 8 VDSG-LU schafft noch eine ausdrückliche Rechtsgrundlage für verschiedene Veröffentlichungen der dem Gesetz unterstellten Organe.

## **F. Die Kontrollrechte**

31. Die Kontrollrechte im kantonalen Recht sind durch §§ 14 ff. DSG-LU geregelt. Diese sind mit dem System des DSG grundsätzlich vergleichbar.

### **a. Rechte**

32. Die betroffenen Personen verfügen über verschiedene Rechte. Diese werden nachfolgend kurz erläutert. Insbesondere das Auskunftsrecht und das Recht auf Berichtigung werden anschliessend kurz beschrieben. Die Kontrollrechte sind im Einzelnen das:

32.1 Auskunftsrecht (§ 15 f. DSG-LU);

32.2 Recht auf Berichtigung unrichtiger Personendaten (§ 17 DSG-LU);

32.3 Recht auf Vernichtung von Personendaten, die unbefugt bearbeitet werden (§ 18 Abs. 1 DSG-LU);

32.4 Recht auf Beseitigung von Folgen aus einer unbefugten Bearbeitung von Personendaten (§ 18 Abs. 1 DSG-LU);

32.5 Recht auf Bekanntgabe eines Entscheides an Dritte oder an Organe (§ 18 Abs. 2 DSG-LU).

33. Die Kontrollrechte müssen gegenüber dem Inhaber einer Datensammlung ausgeübt werden. Ein Auskunftsbegehren gegenüber der Polizei muss schriftlich beim Kommando der Kantonspolizei gestellt werden (§ 11 VDSG-LU).

34. Die Ausübung der Kontrollrechte ist unverjährbar.

35. Die Ablehnung des Begehrens ist schriftlich als Verfügung mitzuteilen (§ 19 Abs. 1 DSG-LU). Ausnahmen sind durch § 19 Abs. 2 DSG-LU und § 11 Abs. 2 VDSG-LU ausdrücklich und abschliessend geregelt. Sofern die betroffene Person mit der ergangenen Verfügung nicht einverstanden ist, richtet sich die Anfechtung, unter Einschluss der Kosten des Verfahrens, nach dem Gesetz über die Verwaltungsrechtspflege (§ 21 DSG-LU).

36. Die Ausübung des Kontrollrechts ist grundsätzlich kostenfrei (§ 20 DSG-LU). Ausnahmen werden durch § 12a Abs. 2 VDSG-LU geregelt:

„Kosten können erhoben werden, wenn die Behandlung eines Gesuchs einen unverhältnismässigen Verwaltungsaufwand erfordert oder wenn die betroffene Person wiederholt in dieselben Daten Einsicht nimmt oder darüber Auskunft verlangt.“

### **b. Das Auskunftsrecht**

37. Das Auskunftsrecht ist eine **Grundvoraussetzung für die Ausübung der Kontrollrechte** und für die Überprüfung der Einhaltung der Datenschutzgesetzgebung. Wenn die betroffene Person nicht erfahren kann, wer über sie welche Daten bearbeitet, wie soll sie in der Lage sein, eine unzulässige Datenbearbeitung zu verhindern oder einstellen zu lassen, die Berichtigung unrichtiger Daten oder die Vernichtung widerrechtlich erfasster Daten zu verlangen?
38. **Auskunftsberechtig** ist jede (natürliche oder juristische) Person über die Personendaten bearbeitet werden, ohne dass sie ein Interesse für die Auskunft nachweisen oder glaubhaft machen muss. Auf dieses Recht kann niemand im Voraus verzichten. Für die Ausübung dieses Rechts genügt die Urteilsfähigkeit.
39. **Adressat des Auskunftsrechts** ist grundsätzlich der Inhaber der Datensammlung. Dies gilt selbst, wenn er die Daten durch einen Dritten bearbeiten lässt (so genanntes „Outsourcing“).
40. **Gegenstand** des Auskunftsrechts sind Daten einer Datensammlung, die sich auf die eigene Person beziehen. Grundsätzlich ist das Auskunftsrecht ein höchstpersönliches Recht und kann nicht für Dritte ausgeübt werden (selbst nicht für unmündige aber urteilsfähige Personen).
41. **Das Auskunftsrecht ist nicht unbegrenzt.** § 15 Abs. 4 DSG-LU sowie § 16 DSG-LU erläutern die möglichen Einschränkungen. Dabei sieht das Gesetz vier Arten von Einschränkungen vor: die Verweigerung (als weitestgehende Einschränkung), die Einschränkung im eigentlichen Sinne (als inhaltliche Einschränkung), die Auskunft mit Auflagen (als Einschränkung der freien Verwendung der erhaltenen Informationen) und die Mitteilung an einen Dritten (als persönliche Einschränkung).
42. Die Einschränkung ist an das Bestehen von **überwiegenden Interessen** gebunden. So kann ein **überwiegendes Interesse eines Dritten** die Einschränkung begründen. Bei diesem Grund muss eine eigentliche Güterabwägung zwischen den Interessen des Gesuchstellers und den Interessen des Dritten vorgenommen werden. Dabei ist nicht aus den Augen zu verlieren, dass das Auskunftsrecht die Regel ist, und die Einschränkung eine Ausnahme. Die Einschränkung kann demnach nur bei Vorliegen von wichtigen Gründen erfolgen. Andererseits kann ein **überwiegendes öffentliches Interesse** die Auskunft einschränken (z.B. Staatsschutz). Der Dritte allgemeine Einschränkungsgrund ist als so genanntes **"therapeutisches Privileg"** in § 15 Abs. 4 DSG-LU verankert. Diese Bestimmung sieht vor, dass die Mitteilung an einen Dritten (z.B. Arzt) erfolgt, falls die Gesundheit der betroffenen Person durch die direkte Mitteilung gefährdet werden könnte (so genannter "Aufklärungsschaden").

### c. Das Recht auf Berichtigung

43. Das Recht auf Berichtigung setzt voraus, dass unrichtige Personendaten bearbeitet werden. Eine solche Unrichtigkeit kann durch die betroffene Person behauptet werden. Diesfalls muss das bearbeitende Organ, die Richtigkeit der Personendaten beweisen (§ 17 Abs. 2 DSG-LU). Die betroffene Person muss aber bei der Abklärung mitwirken. Sofern weder die Richtigkeit noch die Unrichtigkeit der bearbeiteten Personendaten bewiesen werden kann, ist ein Vermerk in der Datensammlung aufzunehmen (so genannter „Bestreitungsvermerk“; siehe § 17 Abs. 3 DSG).

## G. Der Datenschutzbeauftragte

44. Der Regierungsrat hat als kantonale Aufsichtsstelle einen Beauftragten für den Datenschutz zu wählen. Dieser ist fachlich selbständig und unabhängig (§ 22 DSG-LU).
45. Die Aufgaben des Datenschutzbeauftragten sind in § 23 DSG-LU wie folgt formuliert:
- <sup>1</sup> Der Beauftragte für den Datenschutz
    - a. überwacht die Einhaltung der Vorschriften über den Datenschutz,
    - b. berät die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherung,
    - c. erteilt den betroffenen Personen Auskunft über ihre Rechte,
    - d. vermittelt zwischen Organen und Personen in allen Anständen über den Datenschutz, namentlich bei Begehren um Auskunft, Berichtigung und Unterlassung,
    - e. reicht in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden Stellungnahmen zu Datenschutzfragen ein,
    - f. orientiert die Organe über wesentliche Anliegen des Datenschutzes,
    - g. sorgt für die Instruktion der Mitarbeiter von Organen über den Datenschutz,
    - h. erstattet dem Regierungsrat jährlich Bericht über seine Tätigkeit und stellt gleichzeitig der Geschäftsprüfungskommission des Grossen Rates eine Kopie zu.
  - <sup>2</sup> Er führt für den Kanton das Register über die Datensammlungen.
46. Für die Erfüllung seiner Aufgabe verfügt er über verschiedene Befugnisse. Wichtig ist aber insbesondere, dass die öffentlichen Organe ihn bei der Erfüllung seiner Aufgaben zu unterstützen haben (§ 24 Abs. 1 DSG-LU). Im übrigen sind seine Befugnisse wie folgt umschrieben:
- <sup>2</sup> Der Beauftragte kann ungeachtet allfälliger Geheimhaltungsvorschriften bei Behörden schriftlich und mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Datensammlungen und ihre Unterlagen nehmen und sich das Bearbeiten von Personendaten vorführen lassen.
  - <sup>3</sup> Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, fordert der Beauftragte die verantwortliche oder deren vorgesetzte Behörde auf, die erforderlichen Massnahmen zu ergreifen.
  - <sup>4</sup> Er darf unter Vorbehalt besonderer Geheimhaltungsvorschriften Kenntnisse, die er bei seiner Tätigkeit erlangt, nur soweit bekanntgeben, als es zur Erfüllung seiner Aufgabe notwendig ist.
47. Der Datenschutzbeauftragte verfügt hingegen über keine Entscheidbefugnisse. Er kann Empfehlungen abgeben, welche in der Regel auch akzeptiert werden.