

TÄTIGKEITSBERICHT 2025

der Datenschutzbeauftragten
des Kantons Luzern

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2 Vorwort	
4 Inhalt	
5 A. Gesetzlicher Auftrag	
7 B. Statistische Angaben	
10 C. Datenschutzverletzung	
13 D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)	
17 E. Projekte	
23 F. Exkurs: Künstliche Intelligenz in der Verwaltung	
28 G. Kontrollen	
29 H. Schulungen und Informationsveranstaltungen / Vorträge	
30 I. Gesetzgebung und Vernehmlassungen	
32 J. Zusammenarbeit mit anderen Datenschutzstellen	
34 K. Website www.datenschutz.lu.ch	
35 L. Adresse	

VORWORT

Die Datenschutzbeauftragte (nachfolgend DSB) hat gemäss § 23 Absatz 3 des kantonalen Datenschutzgesetzes (KDSG)¹ dem Regierungsrat jährlich Bericht über die Schwerpunkte der Tätigkeit der Aufsichtsstelle zu erstatten und stellt der Aufsichts- und Kontrollkommission sowie der Planungs- und Finanzkommission des Kantonsrats eine Kopie zu; der Bericht wird zudem über die Website der DSB² öffentlich zugänglich gemacht. Regierungsrat und Kantonsrat nehmen vom Bericht Kenntnis. Der vorliegende Tätigkeitsbericht erstreckt sich über den Zeitraum vom 1. Januar bis 31. Dezember 2025. Die am 28. Januar 2025 gewählte DSB trat am 1. Mai 2025 ihr Amt in einem 100%-Pensum an.

Mit 483 neuen Geschäftsfällen (+24 %) erreichte das Aufkommen im Berichtsjahr einen historischen Höchststand. Treiber dieser Entwicklung sind die zunehmende Digitalisierung und die gestiegenen IT-Anfragen. Kritisch zu bewerten ist jedoch die unverändert niedrige Zahl an Datenschutzkontrollen (1). Auch die Erledigungsquote von 89 % bei den Anfragen verdeutlicht die angespannte Ressourcensituation.

Der Schutz der Privatsphäre und der verantwortungsvolle Umgang mit Personendaten bilden eine zentrale Grundlage für das Vertrauen der Bevölkerung in das staatliche Handeln. In einer zunehmend digitalisierten Verwaltung gewinnt der Datenschutz stetig an Bedeutung – rechtlich, organisatorisch und technisch. Er ist kein statischer Zustand, sondern ein fortlaufender Prozess, der eine kontinuierliche Auseinandersetzung mit neuen Entwicklungen und Risiken erfordert.

Der vorliegende Tätigkeitsbericht gibt einen Überblick über die Schwerpunkte und Aktivitäten der DSB im Berichtsjahr. Er zeigt auf, welche Fragestellungen und Herausforderungen im Fokus standen, welche Beratungs- und Kontrolltätigkeiten durchgeführt wurden und in welchen Bereichen Handlungsbedarf besteht. Im Zentrum standen dabei insbesondere die Begleitung von Digitalisierungsprojekten sowie die Prüfung neuer Bearbeitungsvorhaben.

Eine ausreichende personelle und fachliche Ausstattung ist Voraussetzung für eine wirksame Umsetzung der datenschutzrechtlichen Vorgaben. Wo Ressourcen knapp sind, besteht das Risiko, dass Datenschutzfragen zu spät oder nicht mit der erforderlichen Tiefe berücksichtigt werden. Datenschutz darf jedoch nicht als nachgelagerte Zusatzaufgabe verstanden werden, sondern muss integraler Bestandteil von Projekten und Prozessen sein.

Parallel dazu schreitet die Auslagerung von IT-Dienstleistungen und Datenbearbeitungen in Cloud-Umgebungen weiter voran. Cloud-Lösungen bieten erhebliche Effizienz- und Innovationspotenziale, werfen jedoch komplexe Fragen hinsichtlich Da-

1 Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990, SRL Nr. 38.

2 datenschutz.lu.ch

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstaltungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse

tenhoheit, Transparenz, Zugriffsmöglichkeiten durch Dritte sowie technischer und organisatorischer Sicherheitsmassnahmen auf. Eine sorgfältige rechtliche und technische Prüfung bleibt deshalb unabdingbar.

Ziel bleibt es, die öffentlichen Organe bei der rechtskonformen Umsetzung ihrer Aufgaben zu unterstützen und zugleich die Rechte der betroffenen Personen wirksam zu schützen. Gesetzliche Entwicklungen, technologische Innovationen und veränderte gesellschaftliche Erwartungen verlangen dabei eine vorausschauende, unabhängige und konstruktive Datenschutzaufsicht.

Das Berichtsjahr war geprägt durch

- a. die Beantwortung einer hohen Zahl an Anfragen;
- b. die Unterstützung von Arbeitsgruppen und Projekten im Bereich eGovernment;
- c. die Betreuung der Datenschutzinstrumente; und
- d. die Begleitung einer grossen Zahl neuer Projekte, insbesondere IT-Projekte.

Im Folgenden erhalten Sie konkrete statistische Informationen zum Berichtsjahr sowie einen summarischen Überblick auf folgende Themenbereiche:

- Anfragen
- Projekte
- Kontrollen
- Gesetzgebung und Vernehmlassungen
- Schulungen und Informationsveranstaltungen/Vorträge

Das Berichtsjahr stand insbesondere im Zeichen der Cloud-Nutzung und der Künstlichen Intelligenz; entsprechend wurde dies zum Anlass genommen, in einem Exkurs allgemeine Ausführungen zur Auslagerung sowie zur Künstlichen Intelligenz in der Verwaltung darzulegen.

Die DSB bedankt sich bei allen Mitarbeitenden der kantonalen und kommunalen Behörden für die konstruktive Zusammenarbeit, dem DSB-Team sowie beim Vorgänger Matthias R. Schönbächler für das engagierte und fachlich fundierte Wirken im Berichtsjahr.

Natascha Ofner-Venetz

Datenschutzbeauftragte des Kantons Luzern

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



INHALT

Vorwort	2
A. Gesetzlicher Auftrag	5
B. Statistische Angaben	7
C. Datenschutzverletzung	10
D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)	13
E. Projekte	17
F. Exkurs: Künstliche Intelligenz in der Verwaltung	23
G. Kontrollen	28
H. Schulungen und Informationsveranstaltungen / Vorträge	29
I. Gesetzgebung und Vernehmlassungen	30
J. Zusammenarbeit mit anderen Datenschutzstellen	32
a. privatim	32
b. Schengen Koordinationsgruppe	33
K. Website datenschutz.lu.ch	34
L. Adresse	35

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

A. GESETZLICHER AUFTRAG

Der Auftrag und die Aufgaben der oder des DSB sind in den §§ 22 f. KDSG³ verankert:

§ 22 Aufsicht

¹ Der Kantonsrat wählt auf Antrag des Regierungsrates einen Beauftragten oder eine Beauftragte für den Datenschutz auf eine Amtsdauer von vier Jahren. Wiederwahl ist möglich.

^{1 bis} Bei der erstmaligen Wahl des oder der Beauftragten legt der Regierungsrat jeweils den Besoldungsrahmen und die Besoldungsentwicklung fest.

^{1ter} Der Regierungsrat kann das Arbeitsverhältnis aus wichtigen Gründen vor Ablauf der Amtsdauer auflösen. Die Auflösung aus wichtigen Gründen bedarf der Genehmigung durch die Geschäftsleitung des Kantonsrates.

² Der oder die Beauftragte ist fachlich selbständig und unabhängig; administrativ ist er oder sie der Staatskanzlei zugeordnet.

³ ...

§ 23 Aufgaben

¹ Der oder die Beauftragte für den Datenschutz

- a. überwacht die Einhaltung der Vorschriften über den Datenschutz,
- b. verfolgt die massgeblichen Entwicklungen und berät die verantwortlichen Organe in Fragen des Datenschutzes,
- c. erteilt den betroffenen Personen Auskunft über ihre Rechte und behandelt aufsichtsrechtliche Anzeigen innert angemessener Frist,

- c^{bis}. gibt gegenüber den Organen Empfehlungen zu Datenbearbeitungen ab,
- d. ...

- e. reicht in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden und in Vernehmlassungsverfahren zu Entwürfen von rechtsetzenden Erlassen Stellungnahmen zu Datenschutzfragen ein,

- f. orientiert die Organe und die Öffentlichkeit über wesentliche Anliegen des Datenschutzes,

- g. sorgt für die Instruktion der Mitarbeiter von Organen über den Datenschutz,

- h. nimmt zu Datenbearbeitungen Stellung, die ein hohes Risiko für Verletzungen von Persönlichkeits- und Grundrechten der betroffenen Personen bergen,

- i. veröffentlicht Stellungnahmen,

- j. arbeitet mit den Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen,

- k. ...

³ Zuletzt geändert/eingefügt mit Kantonsratsbeschluss G 2021-054 vom 10.5.2021 mit Inkrafttreten per 1.9.2021.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



2 ...

3 Der oder die Beauftragte erstattet dem Regierungsrat jährlich Bericht über die Schwerpunkte der Tätigkeit der Aufsichtsstelle. Er oder sie stellt den Tätigkeitsbericht der Aufsichts- und Kontrollkommission sowie der Planungs- und Finanzkommission des Kantonsrates zu und veröffentlicht ihn im Internet. Regierungsrat und Kantonsrat nehmen vom Bericht Kenntnis.

Die Zuständigkeit der oder des DSB ergibt sich aus dem Geltungsbereich des Datenschutzgesetzes gemäss § 3 KDSG. Demnach ist die oder der DSB zuständig zur Überwachung von Datenbearbeitungen durch

- a. den Kanton,
- b. die Gemeinden,
- c. andere Gemeinwesen gemäss § 1 des Gesetzes über die Verwaltungspflege (SRL Nr. 40), vordergründig also die vermögensfähigen Verwaltungseinheiten des Kantons, der Gemeinden und der Landeskirchen, wie Anstalten mit Rechtspersönlichkeit, Körperschaften, Gemeinde- und Zweckverbände und andere Organisationen des öffentlichen Rechts;
- d. die übrigen Personen und Organisationen des öffentlichen und des privaten Rechts, denen kantonale Aufgaben übertragen sind, z.B. mittels Leistungsvereinbarungen.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

B. STATISTISCHE ANGABEN

Die Dienstleistungen der DSB im Berichtsjahr (umfassend sämtliche Neuzugänge inkl. Medienanfragen, die bei den Anfragen neu dazugezählt wurden; aber ohne pendente Geschäfte des Vorjahres) lassen sich wie folgt auflisten:

Dienstleistungen	2019	2020	2021	2022	2023	2024	2025	Entwicklung (2024–25)
1. Auskunft								
Anfragen*	243	264	238	276	365	325	418	+ 28 %
Meldungen von Datenschutzverletzungen**	--	--	4	10	6	7	6	- 14 %
Total Auskünfte	243	264	242	286	371	332	424	+ 28 %
Anfragen in Bearbeitung**	31	40	32	35	48	41	43	+ 5 %
Anfragen abgeschlossen**	212	221	210	251	323	291	381	+ 31 %
Verhältnis abgeschlossene Anfragen**	87 %	82 %	87 %	88 %	87 %	88 %	89 %	+ 1 %
2. Projekte und Weiterbildung								
Mitarbeit in Projekten ⁴	41	52	67	63	45	57	54	- 5 %
wovon Informatikprojekte**	25	33	42	38	32	40	47	+ 18 %
wovon Nicht-Informatikprojekte**	16	19	25	25	13	17	7	- 59 %
Leitung von Projekten inkl. Audits	1	2	0	1	1	1	1	0 %
Geleitete Ausbildungsveranstaltungen	1	2	2	0	1	1	1	0 %
Gehaltene Vorträge	7	2	4	4	3	0	3	+ 300 %
Total neue Geschäftsfälle	293	322	313	354	421	391	483	+ 24 %
Anfragen im Detail								
Anfragen Gemeinden	39	68	49	66	81	49	49	0 %
Anfragen Kanton	91	73	91	83	138	98	172	+ 76 %
Anfragen Private	113	123	98	119	146	162	154	- 5 %
Anfragen:								
<i>Im Bereich Informatik</i>	17	35	30	37	88	72	95	+ 32 %
<i>Im Bereich Polizei</i>	23	15	11	17	52	62	42	- 32 %
<i>Im Bereich Bildung</i>	15	24	21	15	49	50	49	- 2 %
<i>Im Bereich Soziales</i>	49	57	41	98	58	40	25	- 38 %
<i>Im Bereich Privat</i>	58	37	28	29	27	22	33	+ 50 %
<i>Im Bereich Gesundheit</i>	19	34	43	24	31	25	53	+ 112 %
<i>In versch. anderen Bereichen (Diverse)</i>	34	59	44	29	41	43	78	+ 81 %
Total Auskünfte	243	264	242	286	371	332	375	+ 13 %
Anfragen in Bearbeitung**	31	40	32	35	48	41	41	0 %
Anfragen abgeschlossen**	212	221	210	251	323	291	334	+ 15 %
Verhältnis abgeschlossene Anfragen**	87 %	82 %	87 %	88 %	87 %	88 %	89 %	+ 1 %

* inklusive politische Vorstösse, Vernehmlassungen, Medienanfragen;
Zahlen wurden von den früheren publizierten Tätigkeitsberichten übernommen

** ab dem Jahr 2019 unterschieden

*** Rubrik seit 2021

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

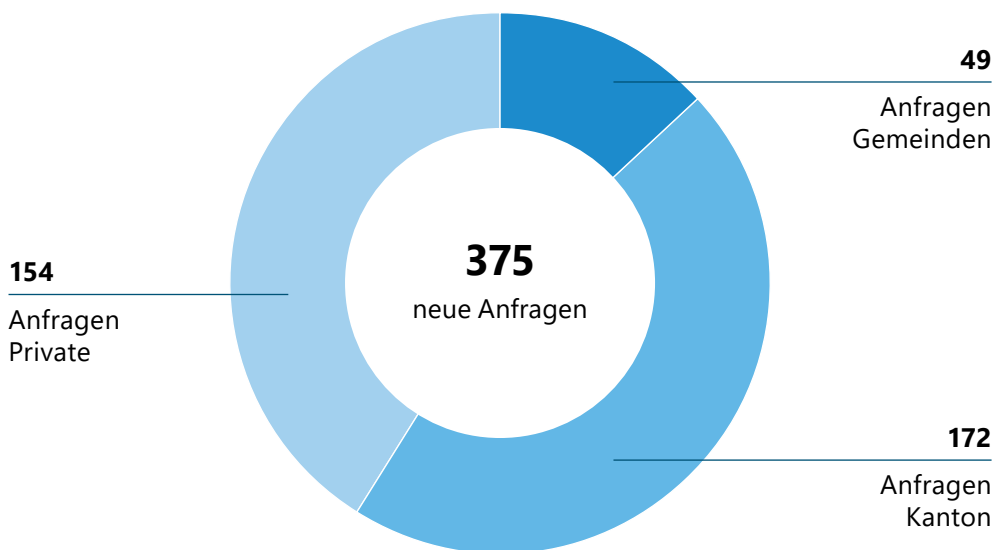
L. Adresse

Mit 483 neuen Geschäftsfällen (+24 %) erreichte das Aufkommen im Berichtsjahr einen historischen Höchststand. Treiber dieser Entwicklung sind die zunehmende Digitalisierung und die gestiegenen IT-Anfragen. Kritisch zu bewerten ist jedoch die unverändert niedrige Zahl an Datenschutzkontrollen (1). Auch die Erledigungsquote von 89 % bei den Anfragen verdeutlicht die angespannte Ressourcensituation.

Im Berichtsjahr verzeichnete die DSB insgesamt 375 neue Anfragen, was einem deutlichen Anstieg von 13 % entspricht. Während die Anfragen aus den Gemeinden auf dem Niveau des Vorjahres stagnierten, sank das Interesse von Privatpersonen leicht (-5 %). Herausragend ist hingegen die Zunahme der Anfragen aus der kantonalen Verwaltung, die ein Plus von 76 % aufzeigt.

Inhaltlich stiegen insbesondere die Themenbereiche Informatik (von 72 auf 95) und Gesundheit (von 25 auf 53) im Vergleich zum Vorjahr an. Im Gegensatz dazu waren die Fallzahlen in den Bereichen Polizei, Bildung und Soziales rückläufig. Auffallend ist zudem die starke Zunahme bei diversen Anfragen (von 43 auf 78) sowie im Privatbereich (22 auf 33), der verhältnismässig das grösste Wachstum aufwies.

Anfragen im Berichtsjahr 2025

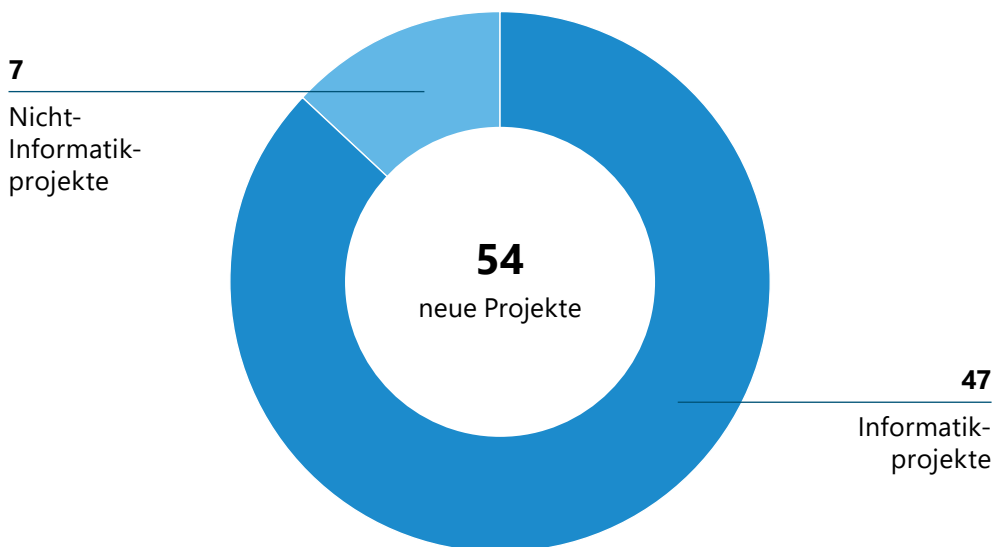


Im Berichtsjahr beteiligte sich die DSB an insgesamt 54 neuen Projekten, was einem leichten Rückgang von 5 % entspricht. Während die Anzahl der Informatikprojekte von 40 auf 47 anstieg, sank die Beteiligung an Nicht-Informatikprojekten von 17 auf 7. Lediglich bei einem Informatikprojekt erfolgte die Eingabe als Vorabkonsultation nach einer durchgeführten Datenschutz-Folgenabschätzung.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstal- tungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Neue Projekte im Berichtsjahr 2025



Die Meldepflicht für Datenschutzverletzungen nach § 7 KDSG scheint in der Verwaltung immer noch nicht Routine zu sein: Seit der Einführung des Instruments im September 2021 gingen insgesamt 33 Meldungen von Datenschutzverletzungen ein (6 davon im Berichtsjahr). Die Dunkelziffer scheint immer noch gross zu sein und die Institutionalisation der Prozesse bleibt ausbaufähig. Zur Erinnerung: Meldepflichtig sind Vorfälle mit voraussichtlich hohem Risiko für die Grundrechte oder die Persönlichkeit der Betroffenen (§ 6b Abs. 2 KDSV)⁵. Entsprechende Hilfsmittel wie Merkblatt und Formular stehen online zur Verfügung.

E-Mail-Anfragen an die Datenaufsicht bleiben auch in diesem Berichtsjahr mit 70 % die am häufigsten gewählte Art der Kontaktaufnahme. Telefonische Anfragen (24 %) sowie Anfragen über das Kontaktformular (4 %) erfreuen sich bei der Bevölkerung einer weitgehend konstanten Beliebtheit. Demgegenüber spielen schriftliche Anfragen per Briefpost weiterhin eine untergeordnete Rolle: Mit 8 Eingaben, was rund 2 % aller Anfragen entspricht, bleiben sie auch in diesem Berichtsjahr eher die Ausnahme.

Die Digitalisierung schreitet unvermindert voran. Neben dem anhaltenden Trend zur Auslagerung in die Cloud gewinnen KI-basierte Projekte zunehmend an Bedeutung. Dass präventive Instrumente wie die Vorabkonsultation kaum genutzt werden, lässt auf eine hohe Dunkelziffer bei der Datenverarbeitung schliessen – ein Defizit, das durch die unregelmässigen Kontrollen kritischer Systeme nicht kompensiert werden kann.

Ergänzend ist festzuhalten, dass die im Berichtsjahr bewilligte Stellenerhöhung um 50 % (auf 310 %) erst mit dem Amtsantritt der DSB vollumfänglich wirksam wurde. Ab 2026 verfügt die DSB über insgesamt 360 Stellenprozent. Das Budget für externe Unterstützung bleibt aufgrund kantonaler Sparmassnahmen unverändert bei CHF 20'000.–. Die personelle Belastungssituation bleibt weiterhin angespannt.

⁵ Kantonale Datenschutzverordnung (KDSV) vom 26.02.1991, SRL Nr. 38b

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



C. DATENSCHUTZVERLETZUNG

Allgemeines Vorgehen

Kommt es bei einem öffentlichen Organ zu einer Verletzung der Datensicherheit (Datenschutzverletzung), sind die gesetzlichen Vorgaben gemäss § 7 KDSG und § 6b KDSV anwendbar.

Eine Datenschutzverletzung bzw. eine unbefugte Datenbearbeitung ist eine Verletzung der Datensicherheit (Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit), die Personendaten betrifft. Das Gesetz nennt dabei insbesondere Verlust, Fälschung, Entwendung und Kenntnisnahme durch nicht berechtigte Dritte als Beispiele unbefugter Datenbearbeitungen, wobei diese Liste nicht als abschliessend zu verstehen ist.

Wird eine solche Verletzung festgestellt, hat das verantwortliche Organ zunächst unverzüglich geeignete technische und organisatorische Massnahmen zu ergreifen, um die Verletzung zu beheben oder ihre Auswirkungen zu begrenzen. Gleichzeitig ist eine Risikobeurteilung vorzunehmen, insbesondere hinsichtlich möglicher Beeinträchtigungen der Persönlichkeit oder der Grundrechte der betroffenen Personen. Der Vorfall ist zudem zu dokumentieren.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstal- tungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Ergibt die Risikobeurteilung, dass die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, besteht eine Meldepflicht gegenüber der oder dem DSB. Diese Meldung hat spätestens innerhalb von drei Tagen nach Kenntnisnahme des Vorfalls zu erfolgen.

Die Meldung muss mindestens folgende Angaben enthalten (vgl. § 6b Abs. 3 KDSV):

- die Art der Verletzung der Datensicherheit,
- die Kategorien der betroffenen Personendaten sowie – soweit möglich – die Anzahl der betroffenen Personen,
- die voraussichtlichen Auswirkungen der Datenschutzverletzung,
- die bereits ergriffenen oder geplanten Massnahmen zur Behebung der Verletzung sowie zur Minderung möglicher negativer Folgen.

Zusätzlich kann eine Informationspflicht gegenüber den betroffenen Personen oder weiteren Stellen bestehen, sofern dies zum Schutz der betroffenen Personen erforderlich ist oder von der/dem DSB verlangt wird.

Zusammengefasst umfasst das Vorgehen bei einer Datenschutzverletzung insbesondere folgende Schritte:

- Sofortige Sicherungs- und Abhilfemassnahmen zur Begrenzung des Schadens.
- Dokumentation des Vorfalls und Durchführung einer Risikobeurteilung.
- Meldung an die bzw. den kantonalen DSB, sofern ein hohes Risiko für die betroffenen Personen besteht (spätestens innert drei Tagen).
- Information der betroffenen Personen, sofern dies zum Schutz ihrer Rechte erforderlich ist oder von der Aufsichtsbehörde verlangt wird.

Konkreter Vorfall mit analogem Ursprung und digitaler Rechtswirkung

Die Dienststelle Steuern Luzern versandte in Zusammenarbeit mit einem externen Partner Erinnerungsschreiben an Personen und Unternehmen, welche zum Zeitpunkt des Versandes die Steuererklärung 2024 noch nicht eingereicht hatten. Im Zuge der Aufbereitung der Sendungen kam es zu einem Fehler im Druckprozess: Der als einseitig vorgesehene Brief wurde doppelseitig bedruckt, sodass auf der Rückseite jeweils ein anderer Empfänger angeschrieben war. Dadurch erhielten die Empfängerinnen und Empfänger neben dem eigenen Schreiben zugleich Angaben, die einer Drittperson zuzuordnen waren. Betroffen waren rund 18'000 Schreiben.

Gemäss Meldung umfassten die offengelegten Daten insbesondere Name, Kontaktinformationen, PersID sowie den Zugangscode zum eFiling-Verfahren. Damit bestand objektiv die Möglichkeit, dass aufgrund der Angaben auf der Rückseite für eine andere Person die Steuererklärung 2024 eingereicht werden konnte. Für betroffene Personen ist zudem wesentlich, dass sich eine Offenlegung im Postversand nachträglich nur eingeschränkt nachvollziehen lässt.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

Die DSB qualifizierte den Vorfall als klare Datenschutzverletzung. Sie hielt fest, dass Zugangscookies, welche rechtsverbindliche elektronische Handlungen ermöglichen, als vertrauliche Authentisierungsmerkmale zu behandeln sind. Durch die Offenlegung dieser Zugangscookies war die rechtliche Zurechenbarkeit elektronisch eingereicher Erklärungen objektiv nicht mehr gewährleistet.

Der Vorfall verdeutlicht die Bedeutung einer prozessual optimierten Qualitätssicherung bei Massenverarbeitungen im Einlieferung- und Druckprozess, welche die eingelieferten Daten (Blatt, Kuvert) korrekt abbildet. Gleichzeitig bestätigt der Fall, dass die Verantwortung für die Datensicherheit auch bei Einbindung externer Partner beim verantwortlichen Organ verbleibt.



INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse

D. EXKURS: ALLGEMEINE AUSFÜHRUNGEN ZUR AUSLAGERUNG (CLOUD)

Die Auslagerung von Informatikdienstleistungen an Dritte ist für öffentliche Organe seit Jahren gelebte Praxis und gewinnt im Zuge der fortschreitenden Digitalisierung weiter an Bedeutung. Cloud-basierte Dienste versprechen Effizienzgewinne, Skalierbarkeit sowie eine Reduktion des internen Betriebsaufwands. Gleichzeitig stellt die Auslagerung von IT-Leistungen aus datenschutzrechtlicher und staatspolitischer Sicht einen besonders sensiblen Vorgang dar. Sie berührt nicht nur die Einhaltung der datenschutzrechtlichen Grundsätze, sondern auch Fragen der Kontrolle, der Verantwortlichkeit und der digitalen Souveränität des Gemeinwesens.

Nach geltendem kantonalem Recht ist die Auslagerung von Informatikdienstleistungen grundsätzlich zulässig, sofern die einschlägigen Vorschriften über den Datenschutz sowie die weiteren gesetzlichen Anforderungen eingehalten werden. Diese gesetzliche Zulässigkeit ist jedoch nicht als Freipass zu verstehen. Auch bei einer vollständigen technischen oder organisatorischen Auslagerung verbleibt die Verantwortung für die Rechtmässigkeit der Datenbearbeitung beim öffentlichen Organ. Die Auslagerung ändert weder an der datenschutzrechtlichen Rollenverteilung noch an der Pflicht des verantwortlichen Organs, jederzeit die Einhaltung der gesetzlichen Vorgaben sicherzustellen.

Wesensmerkmal jeder Auslagerung ist ein Verlust an unmittelbarer Kontrolle über die Bearbeitung der Daten. Dieser Kontrollverlust ist systemimmanent und kann nicht vollständig beseitigt werden. Er kann jedoch durch eine sorgfältige Auswahl der Anbieter, eine angemessene vertragliche Ausgestaltung sowie durch klar definierte technische und organisatorische Massnahmen teilweise kompensiert werden. In der Praxis zeigt sich jedoch regelmässig, dass gerade dieser kompensierende Rahmen unzureichend ausgestaltet ist. Verträge über Auftragsbearbeitungen bleiben häufig auf einem hohen Abstraktionsniveau, enthalten unpräzise oder pauschale Sicherheitszusagen und verschieben Risiken einseitig auf das auslagernde öffentliche Organ. Insbesondere bei grossen internationalen Cloud-Anbieterinnen ist der Verhandlungsspielraum faktisch stark eingeschränkt. Standardisierte Vertragswerke lassen kaum Anpassungen zu, obwohl sie nicht selten Schwachstellen im Hinblick auf Kontrollrechte, Auditmöglichkeiten oder Subunternehmerketten aufweisen.

Ein besonderes Augenmerk ist auf die technischen und organisatorischen Massnahmen zu richten. Diese müssen sich am konkreten Risiko der jeweiligen Datenbearbeitung orientieren und ausreichend bestimmt sein. Allgemeine Verweise auf branchenübliche Sicherheitsstandards genügen den gesetzlichen Anforderungen in der Regel nicht. Die Erfahrung der DSB zeigt, dass technische Massnahmen häufig zu wenig spezifisch beschrieben werden und die tatsächliche Umsetzung beim Anbieter nicht hinreichend überprüfbar ist. Damit besteht die Gefahr, dass die formale Vertragserfüllung zwar behauptet, der materielle Schutz der Personendaten jedoch nicht gewährleistet ist.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse



Über die rein datenschutzrechtliche Betrachtung hinaus wirft die Auslagerung von Informatikdienstleistungen zunehmend Fragen der digitalen Souveränität auf. Digitale Souveränität bedeutet, dass ein Gemeinwesen seine informationstechnischen Infrastrukturen und Datenbearbeitungen eigenständig steuern und im Einklang mit seinem Rechtssystem kontrollieren kann. Diese Steuerungsfähigkeit kann erheblich beeinträchtigt werden, wenn zentrale staatliche Aufgaben von Cloud-Diensten abhängen, die ausländischem Recht unterstehen. Besonders problematisch ist dies bei Anbieterinnen mit Sitz in den Vereinigten Staaten, da diese dem US-amerikanischen CLOUD Act unterliegen. Dieser kann Anbieter verpflichten, Daten an US-Behörden herauszugeben, selbst wenn sich diese Daten physisch ausserhalb der USA befinden. Eine solche Zugriffsmöglichkeit steht in einem Spannungsverhältnis zu den datenschutzrechtlichen Anforderungen des schweizerischen Rechts und kann im Einzelfall dazu führen, dass eine Auslagerung nicht mehr als rechtmässig beurteilt werden kann.

Vor diesem Hintergrund ist bei jeder Auslagerung nicht nur die unmittelbare rechtliche Zulässigkeit, sondern auch die langfristige strategische Perspektive der Informatiksteuerung zu berücksichtigen. Auslagerungen können strukturelle Abhängigkeiten von einzelnen Anbieterinnen begründen, namentlich dann, wenn proprietäre Technologien, exklusive Schnittstellen oder fehlende Migrationsmöglichkeiten einen Anbieterwechsel faktisch verunmöglichen oder wirtschaftlich unververtretbar machen. Solche Abhängigkeiten entstehen häufig schleichend und werden erst dann als Problem erkannt, wenn sich Geschäftsmodelle ändern, Leistungen nur noch in bestimmten Bereitstellungsformen angeboten werden oder die Nutzung zusätzlicher

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

Funktionen faktisch erzwungen wird, um den Betrieb aufrechtzuerhalten. Die Erfahrung zeigt, dass Verwaltungen in solchen Konstellationen zunehmend unter Handlungsdruck geraten und Alternativen als nicht mehr realistisch wahrgenommen werden, obwohl diese bei frühzeitiger strategischer Weichenstellung durchaus vorhanden gewesen wären.

Eine kluge IT-Strategie bedeutet in diesem Zusammenhang, Abhängigkeiten bewusst zu begrenzen und nicht allein Komfort- oder Effizienzüberlegungen zu folgen. Öffentliche Verwaltungen unterscheiden sich in ihren rechtlichen Rahmenbedingungen, ihrem Schutzbedarf und ihrem öffentlichen Auftrag wesentlich von privatwirtschaftlichen Unternehmen. Daraus folgt, dass nicht jede am Markt etablierte Lösung oder Funktionalität zwingend in gleichem Umfang erforderlich oder zulässig ist. Strategische Entscheidungen sollten daher nicht ausschliesslich auf Zusicherungen von Anbietern oder Wiederverkäufern abgestützt werden, sondern auf einer eigenständigen Bewertung der langfristigen Auswirkungen auf Steuerbarkeit, Datenhoheit und Souveränität beruhen. Die Bündelung möglichst vieler zentraler Verwaltungsfunktionen bei einer einzelnen Anbieterin mag betrieblich attraktiv erscheinen, erhöht jedoch das Risiko einer faktischen Alternativlosigkeit und schränkt den zukünftigen Handlungsspielraum erheblich ein.

Eng damit verbunden ist die Frage der Exit-Strategie. Eine solche ist kein optionales Element, sondern integraler Bestandteil einer rechtssicheren und nachhaltigen Auslagerung. Sie muss bereits vor Vertragsabschluss konzeptionell durchdacht und vertraglich abgesichert werden. Dazu gehören insbesondere Regelungen zur Rückführung oder Migration der Daten, zur Sicherstellung der Datenintegrität, zur Nutzung offener und dokumentierter Schnittstellen sowie zur Weiterverwendbarkeit der Daten und Prozesse in alternativen Systemen. Ohne eine realistische Exit-Strategie besteht die Gefahr, dass Auslagerungen faktisch irreversibel werden und strategische Entscheidungen der Vergangenheit die Verwaltung dauerhaft binden.

Ein weiteres, in der Praxis häufig unterschätztes Risiko betrifft webbasierten Lösungen, die im Rahmen von Auslagerungen eingesetzt werden. Immer wieder stellt die Aufsichtsbehörde fest, dass solche Anwendungen mit Marketing- oder Tracking-Technologien ausgestattet sind. Während in der Privatwirtschaft unter bestimmten Voraussetzungen eine Rechtfertigung über Einwilligungen möglich sein kann, fehlt der öffentlichen Verwaltung hierfür in der Regel die rechtliche Grundlage. Der Einsatz solcher Technologien ist im öffentlich-rechtlichen Kontext meist unzulässig und kann nicht durch vertragliche Zusicherungen der Anbieter geheilt werden.

Schliesslich ist festzuhalten, dass datenschutzrechtliche Probleme bei Auslagerungen häufig nicht auf fehlendes Wissen, sondern auf unzureichende Prozesse zurückzuführen sind. Die DSB wird vielfach erst in einem späten Stadium beigezogen, wenn technische und vertragliche Entscheidungen bereits getroffen wurden. In dieser Phase sind Korrekturen oft nur noch mit erheblichem Aufwand oder gar nicht mehr möglich. Anbieterinnen präsentieren den Fachstellen ihre Lösungen in einem stark

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse

vereinfachten oder beschönigten Licht, während eine kritische rechtliche und organisatorische Prüfung zu spät erfolgt. Aus Sicht der Aufsichtsbehörde ist daher eine frühzeitige Einbindung der datenschutzrechtlichen Expertise zwingend erforderlich, um rechtliche, technische und strategische Risiken rechtzeitig zu erkennen und zu minimieren.

Dabei ist klarzustellen, dass die DSB eine reine Aufsichtsstelle ist und weder rechtlich noch organisatorisch die Verantwortung für die Bearbeitung von Personendaten trägt. Verantwortlich im datenschutzrechtlichen Sinn bleibt stets das jeweilige öffentliche Organ. Ebenso wenig verfügt die Aufsichtsbehörde über die personellen Ressourcen, um die datenschutzrechtliche Expertise für sämtliche Projekte der Verwaltung zu erbringen. Eine solche Aufgabenverlagerung an die Aufsichtsstelle wäre weder sachgerecht noch systemkonform und würde zwangsläufig zu einer unverhältnismässigen Aufblähung des Aufsichtsapparats führen. Der kantonale Gesetzgeber hat diesem Umstand Rechnung getragen, indem er mit dem Instrument der Datenschutzberaterin bzw. des Datenschutzberaters eine dezentrale fachliche Unterstützungsfunktion geschaffen hat (§ 6d KDSV). Für bestimmte Aufgabenbereiche, namentlich die Staatsanwaltschaft, die Luzerner Polizei sowie den Strafvollzug, besteht eine entsprechende Pflicht; für die übrigen kantonalen Dienststellen ist eine solche Funktion zumindest empfohlen. Aus Sicht der Aufsichtsbehörde wäre es ausdrücklich zu begrüssen, wenn auch weitere Dienststellen – idealerweise zumindest auf Ebene der Departemente – Datenschutzberaterinnen oder Datenschutzberater etablieren würden. Dadurch könnte die erforderliche datenschutzrechtliche und organisatorische Expertise frühzeitig in Projekte eingebracht werden.

Die Auslagerung von Informatikdienstleistungen ist damit kein rein technisches oder betriebswirtschaftliches Vorhaben, sondern eine rechtlich und strategisch anspruchsvolle Entscheidung. Sie verlangt eine sorgfältige Abwägung zwischen Effizienzgewinnen und Kontrollverlusten, zwischen kurzfristigem Nutzen und langfristiger Souveränität sowie zwischen vertraglichen Zusicherungen und faktischer Durchsetzbarkeit. Nur wenn diese Aspekte frühzeitig und systematisch berücksichtigt werden, kann eine Auslagerung den gesetzlichen Anforderungen genügen und zugleich den Interessen des Gemeinwesens nachhaltig dienen.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



E. PROJEKTE

Die DSB begleitet Informatikprojekte und andere wesentliche Vorhaben mit Auswirkungen auf den Datenschutz und gibt den Organen Empfehlungen zur datenschutzkonformen Umsetzung. In der Praxis wird die DSB jedoch in vielen Fällen erst in späteren Projektphasen beigezogen.

Wie bereits erwähnt, stellt die DSB insbesondere bei der Auslagerung von Datenbearbeitungen vermehrt fest, dass die Aufsichtsbehörde zu spät einbezogen wird, so dass notwendige Korrekturen nur noch mit erheblichem Aufwand oder gar nicht mehr möglich sind. Dabei gelten auch bei ausgelagerten Lösungen die Grundsätze von «Privacy by Design» und «Privacy by Default» (§ 5 Abs. 1 lit. b KDSV i.V.m. § 4 Abs. 3 KDSG).

Insbesondere bei webbasierten Anwendungen von Auftragsbearbeitern oder bei eingekauften Standardlösungen zeigt sich regelmässig, dass Drittservices (z. B. Support-Tools, Analyse-Dienste oder Sicherheitsdienste) eingebunden werden, die im öffentlich-rechtlichen Kontext datenschutzrechtlich problematisch sind. Während im privatrechtlichen Umfeld eine Bearbeitung über Einwilligungen in Datenschutzerklärung häufig zumindest formal abgestützt werden kann, ist dies im öffentlich-rechtlichen Bereich meist unzulässig.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

Bereits die Einbindung einzelner externer Dienste (z.B. reCAPTCHA) kann dazu führen, dass Personendaten bearbeitet und an Dritte bekannt gegeben werden – ohne dass dafür eine hinreichende gesetzliche Grundlage besteht.

Nachfolgend ein Einblick in ausgewählte Projekte, die die DSB im Berichtsjahr begleitet:

M365

Wie bereits im Vorjahr war die DSB auch 2025 stark mit der Einführung und mit Fragestellungen rund um die Cloud-Services «Microsoft 365» (M365) beschäftigt – sowohl auf kantonaler als auch auf kommunaler Ebene.

Um eine konsistente aufsichtsrechtliche Haltung sicherzustellen und diese transparent zu kommunizieren, hat die DSB ihre Position zu M365 öffentlich publiziert. Ergänzend wurde ein Merkblatt zu besonders schützenswerten Personendaten erarbeitet. Im Weiteren hat privatim eine Resolution zu M365 verabschiedet.

Die DSB weist seit fünf Jahren auf die Risiken von Auslagerungen in globale Cloud-Ökosysteme hin und hat bereits im Tätigkeitsbericht 2020 vor einem schleichenden Verlust digitaler Souveränität gewarnt. Mit der Einführung von M365 in der kantonalen Verwaltung wurde das Thema der digitalen Souveränität im Berichtsjahr vermehrt auch durch Politik und Medien aufgegriffen. Die geopolitischen Entwicklungen – insbesondere die aussenpolitische Ausrichtung des amtierenden US-Präsidenten – haben diese Diskussion zusätzlich verstärkt. Damit hat nicht nur im Kanton Luzern, sondern schweiz- und europaweit ein politischer und gesellschaftlicher Diskurs begonnen, der längst überfällig war.

Die DSB hat in der Vergangenheit wiederholt darauf hingewiesen, dass sich die Verwaltung des Kantons Luzern mit der breiten Einführung von M365 in eine Abhängigkeit von erheblichem Ausmass begibt. Sie begrüsst es aber, dass die Sensibilität für diese Fragestellungen deutlich zugenommen hat und vermehrt über Optionen und Alternativen nachgedacht wird.

In der kantonalen Verwaltung wurde – unter Einbezug externer Fachunterstützung und in Abstimmung mit der DSB – eine Datenschutz-Folgenabschätzung (DSFA) zu M365 Exchange Online (E-Mail aus der Cloud) erarbeitet. Dazu hat die DSB im Juni 2025 ausführlich Stellung genommen. Zudem hat die DSB darauf hingewirkt, dass der Regierungsratsbeschluss vom 6. September 2024, insbesondere in Bezug auf besonders schützenswerte Personendaten, präzisiert wird. Mit Beschluss vom 9. Dezember 2025 hat der Regierungsrat den Einsatz von M365 insbesondere im Umgang mit besonders schützenswerten Personendaten präzisiert. Diese müssen primär in Fach- und GEVER-Anwendungen bearbeitet und gespeichert werden; M365 darf hierfür nur in eng begrenzten Ausnahmefällen für kurzfristige Kommunikation und Zusammenarbeit (insbes. mit Externen) eingesetzt werden, wenn keine geeignete

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

Fach- oder GEVER-Anwendung verfügbar ist, keine dauerhafte Speicherung erfolgt und sie auf das notwendige Minimum beschränkt wird.

Die DSB wird die weiteren Einführungsschritte von M365 weiterhin eng begleiten, um den datenschutzkonformen Einsatz so weit wie möglich sicherzustellen.

Nebula Epic

Im Gesundheitswesen vollzieht sich ein fundamentaler Paradigmenwechsel: weg von der rein reaktiven Behandlung von Krankheiten hin zu einer proaktiven Versorgung, die auf Prävention und Prädiktion setzt.

- Prävention bedeutet, Krankheiten durch gezielte Massnahmen zu verhindern oder frühzeitig zu erkennen (z. B. Screening-Programme, digitale Präventionsapps).
- Prädiktion nutzt grosse Datenmengen und künstliche Intelligenz (KI), um individuelle Risiken zu berechnen und Krankheitsverläufe vorherzusagen. So können Hochrisikopatienten identifiziert und Komplikationen früh abgefangen werden.

Diese Entwicklung stützt sich auf den Einsatz moderner Technologien: Elektronische Patientendossiers, Wearables, (auch Genom-Analysen) und KI-Modelle erlauben eine personalisierte und vorausschauende Versorgung. Spitäler und Gesundheitssysteme investieren deshalb zunehmend in Datenplattformen und KI-Anwendungen, um Ressourcen effizienter einzusetzen und die Versorgungsqualität zu steigern.

Mit der Cloud Service Plattform «Nebula» plante die LUKS Gruppe, ausgewählte KI-Funktionen des Klinikinformationssystems LUKiS (Epic) in einer Cloud-Umgebung bereitzustellen. Die Plattform wird durch Epic Systems angeboten und technisch als Managed Service auf Microsoft Azure betrieben; ergänzend werden Sicherheits- und Edge-Dienste von Cloudflare eingesetzt. Ziel der vorgesehenen Lösung war es, KI-Anwendungen zur Effizienzsteigerung, Qualitätsverbesserung und Entlastung des medizinischen Personals nutzbar zu machen.

Die DSB zeigt grundsätzlich Verständnis für das strategische Anliegen des Spitals, KI und datengetriebene Technologien in der Versorgung einzusetzen. Insbesondere in einem Umfeld, das zunehmend auf Prävention und prädiktive Unterstützung setzt, sind KI-Anwendungen aus Sicht der Versorgungsqualität und Ressourcensteuerung nachvollziehbar. Gleichzeitig ist jedoch festzuhalten, dass im Spitalumfeld besonders schützenswerte Personendaten bearbeitet werden: Gesundheitsdaten betreffen den innersten Kern der Privatsphäre und unterliegen zusätzlich dem strafrechtlich geschützten Berufsgeheimnis.

Im Rahmen der Prüfung standen insbesondere jene Use Cases im Vordergrund, bei denen nicht-pseudonymisierte Patientendaten in Klartext an cloudbasierte KI-Dienste übermittelt würden. Dazu zählen namentlich generative KI-Funktionen wie:

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

- das Erstellen von Antwortentwürfen auf Patientenanfragen,
- das automatisierte Zusammenfassen ambulanter Notizen,
- sowie das Zusammenfassen stationärer Verläufe.

Aus Sicht der DSB sind diese Anwendungsfälle datenschutzrechtlich und berufsgheimnisrechtlich besonders heikel, weil sie die Übermittlung von medizinischen Freitextinformationen an externe KI-Infrastrukturen voraussetzen. Auch wenn die Datenresidenz vertraglich auf EU/EFTA/CH konfiguriert werden kann, verbleiben wesentliche Restrisiken, insbesondere aufgrund der Einbindung von US-Anbietern und der damit verbundenen Drittstaatenbindung (z. B. CLOUD Act / FISA 702).

Die DSB kam deshalb zum Schluss, dass trotz der im Konzept umfassend beschriebenen vertraglichen, technischen und organisatorischen Massnahmen ein hohes Risiko für die Grund- und Persönlichkeitsrechte der betroffenen Personen bestehen bleibt. Die vorgesehene Bearbeitung von Patientendaten in der Cloud wurde unter den gegebenen Umständen als nicht rechtskonform beurteilt, solange keine spezifische gesetzliche Grundlage oder eine ausdrückliche, informierte Einwilligung der betroffenen Personen vorliegt. Die LUKS Gruppe hat diese Einschätzung berücksichtigt.



INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstal- tungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

DeepJudge (KI für Gerichtsentscheide): praxistaugliche KI – mit lokaler Kontrolle

Im Berichtsjahr wurde mit dem Vorhaben DeepJudge ein exemplarisches KI-Projekt begleitet, das den Einsatz von Künstlicher Intelligenz in der Verwaltung anhand eines klar abgegrenzten und praxisnahen Anwendungsfalls erprobt. Ziel des Proof-of-Concepts war es, die Arbeit der Rechtsabteilung des Bau-, Umwelt- und Wirtschaftsdepartements bei der Analyse, Wiederauffindbarkeit und internen Wissenssicherung von Gerichtsentscheiden zu unterstützen. Dabei standen insbesondere die semantische Suche, ein KI-gestützter Chat sowie automatisierte Zusammenfassungen im Vordergrund.

Aus datenschutzrechtlicher Sicht war das Projekt auch deshalb bemerkenswert, weil es ursprünglich eine cloudbasierte Umsetzung vorsah. Die Datenschutzaufsicht empfahl in der frühen Projektphase jedoch, eine Lösung zu bevorzugen, die lokal (on-premises) betrieben werden kann. Dies insbesondere im Hinblick auf die Kontrolle über die Datenbearbeitung, die Nachvollziehbarkeit der Verarbeitung und die Vermeidung unnötiger Drittstaatenrisiken.

Die Empfehlung hatte eine konkrete technische Konsequenz: Für den Betrieb der Lösung war zunächst die Beschaffung geeigneter GPU-Hardware erforderlich, da entsprechende Rechenressourcen beim Kanton noch nicht verfügbar waren. Erst durch diese infrastrukturelle Vorleistung konnte das Vorhaben so umgesetzt werden, dass die Verarbeitung der Dokumente innerhalb der kantonalen Umgebung erfolgt.

Positiv hervorzuheben ist in diesem Zusammenhang, dass das ETH-Spin-off DeepJudge sein Versprechen einlösen konnte, die Lösung nicht nur als Cloud-Dienst, sondern tatsächlich auch als lokal deploybare Variante bereitzustellen. Dies ist bei modernen KI-Produkten keineswegs selbstverständlich und stellt für die Verwaltung einen wichtigen Schritt in Richtung digitaler Souveränität und risikobewusster KI-Nutzung dar.

Das Vorhaben zeigt exemplarisch, dass KI-Lösungen in der Verwaltung möglich sind, wenn sie technisch und organisatorisch so ausgestaltet werden, dass die Kontrolle über die Datenbearbeitung gewahrt bleibt und die Risiken angemessen reduziert werden können.

KVSE

Ein weiteres Projekt, das die Datenschutzbehörde auch 2025 intensiv beschäftigt hat, war die datenschutzkonforme Umsetzung der Arbeitsplätze im KVSE (Kantonale Verwaltung am Seetalplatz, KVSE). Der Kanton Luzern ist dabei am Seetalplatz in Emmen ein neues Verwaltungsgebäude zu realisieren, in welchem verschiedene Dienststellen und Organisationseinheiten von rund 30 Standorten in der Stadt Luzern zentralisiert werden sollen. Das Gebäude bietet ab 2026 Platz für über 2000 Mitarbeitende

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

der kantonalen Verwaltung. Dazu werden verteilt auf 5 Stockwerke Stand heute lediglich 1235 Standardarbeitsplätze eingerichtet, nebst Sitzungszimmern, Besprechungsbereichen und Fokusräumen. Das Gebäude ist in öffentliche, halböffentliche und interne Bereiche gegliedert.

In der Planungsphase wurde keine Risikoanalyse betreffend Datenschutz durchgeführt und die Datenschutzbehörde wurde auch hier erst später beigezogen. Dies hatte zur Folge, dass erst im Frühjahr 2024 auf Basis der zu dieser Zeit kurz vor der Baubewilligung stehenden Baupläne eine grobe Datenschutzrisikoanalyse durchgeführt und zusammen mit der Datenschutzbehörde mögliche Massnahmen herausgeschält wurden, um die identifizierten Risiken zu mitigieren. Gesamthaft betrachtet, konnte in Zusammenarbeit mit der Projektleitung bzw. der Dienststelle Immobilien aus datenschutzrechtlicher Sicht dennoch eine deutliche Optimierung der Arbeitsplatzsituation erreicht werden, insbesondere gemessen daran, was aus baulicher Sicht in diesem Zeitpunkt überhaupt noch umsetzbar war.

Bei Staatsangestellten ist beim Desksharing und Arbeiten im Grossraumbüro aus datenschutzrechtlicher Sicht Vorsicht geboten. So werden die einzelnen Dienststellen und Abteilungen nach ihrem Einzug 2026/2027 zu evaluieren haben, ob die getroffenen risikosenkenden Massnahmen als ausreichend beurteilt werden können.

Bezüglich der datenschutzrechtlichen Herausforderungen, die sich bei Desksharing und Grossraumbüros stellen, verweisen wir auf den Beitrag «Datenschutz am Arbeitsplatz», S. 13 unseres [Tätigkeitsberichts des Jahres 2023](#).

Im Zusammenhang mit dem KVSE hat die DSB 2025 darüber hinaus Beratungstätigkeit in Bezug auf das neue Postbüro und die geplante Videoüberwachung des Gebäudes geleistet.

Projekte im Jahr 2025

Neben den oben aufgeführten Vorhaben hat die DSB im Jahr 2025 weitere Projekte begleitet. Anbei finden Sie eine Auswahl der Projekte:

- Digitale Vertragsunterzeichnung (Projekt der Dienststelle Personal)
- EVEN Elektronischer Vollzug Energetischer Nachweise (Projektleitung BUWD)
- Digitale Kommission (Projektleitung GSD)
- Zentrale Opferhilfe Online (Projektleitung DISG)
- Exchange Online (Projektleitung DIIN)
- Vorabkonsultation PICAR (Projektleitung LUPOL)
- StabiLU (Projektleitung BKD)
- FrostControl (Projektleitung BUWD)
- Datenklassifizierung (Projektleitung DIIN)
- POC Ausweitung DeepJudge (Projektleitung BUWD)

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse



F. EXKURS: KÜNSTLICHE INTELLIGENZ IN DER VERWALTUNG

Studie «Lösungsansätze für die datenschutzkonforme Nutzung von GenAI in der öffentlichen Verwaltung»

Im Berichtsjahr wurde im Auftrag der DSB eine Studie zur datenschutzkonformen Nutzung generativer Künstlicher Intelligenz (GenAI) in der öffentlichen Verwaltung veröffentlicht. Die Untersuchung wurde durch das Institut für Datenanwendungen und Sicherheit (IDAS) der Berner Fachhochschule erarbeitet und dokumentiert praxisnahe Lösungsansätze, rechtliche Rahmenbedingungen, technische Möglichkeiten und organisatorische Massnahmen für den Einsatz von GenAI-Technologien in Verwaltungsprozessen.

Die Studie beginnt mit einer Bestandsaufnahme der technologischen Entwicklungen im Bereich GenAI und zeigt auf, welches Potenzial solche Systeme für die öffentliche Verwaltung bieten. GenAI-Modelle können Mitarbeitende bei komplexen Aufgaben unterstützen, indem sie etwa die automatisierte Beantwortung von Anfragen, die systematische Aufbereitung von Informationen oder die Generierung von Textinhalten ermöglichen. Gleichzeitig adressiert die Studie die spezifischen Herausforderungen, die sich beim Einsatz dieser Technologien im öffentlichen Sektor ergeben – insbesondere im Hinblick auf Datenschutz, digitale Souveränität und rechtliche Anforderungen.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstal- tungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Ein zentrales Kapitel der Untersuchung widmet sich exemplarischen Anwendungsfällen, die für Verwaltungen relevant sind. Dazu gehören der Einsatz von Chatbots zur Unterstützung des Bürgerservices, Anwendungen zur Sprach- und Protokollverarbeitung, KI-gestützte Office-Funktionen sowie Fachapplikationen, die administrative Abläufe effizienter gestalten können. Auf dieser Grundlage werden technische Optionen für die Auswahl und den Betrieb von GenAI-Modellen aufgezeigt sowie konkrete Massnahmen zur datenschutzkonformen Implementierung entlang des gesamten Lebenszyklus eines KI-Systems beschrieben.

Die Studie schliesst mit einem Set von Handlungsempfehlungen für Behörden und IT-Verantwortliche. Diese Empfehlungen umfassen die Entwicklung einer Daten- und KI-Kultur innerhalb der Verwaltung, die gezielte Weiterbildung von Mitarbeitenden, die Berücksichtigung rechtlicher Rahmenbedingungen bereits in der Konzeptionsphase, transparente Kommunikation über KI-Nutzung sowie ein systematisches Risikomanagement. Ziel ist es, GenAI-Lösungen nicht nur innovativ, sondern gleichzeitig verantwortungsvoll, rechtskonform und mit Blick auf den Schutz personenbezogener Daten zu implementieren.

KI in der Verwaltung: Chancen nutzen – Grundrechte schützen

Künstliche Intelligenz (KI) hat das Potenzial, die öffentliche Verwaltung spürbar zu entlasten und Dienstleistungen für die Bevölkerung zu verbessern. Insbesondere dort, wo Prozesse heute stark standardisiert sind oder grosse Textmengen verarbeitet werden müssen, können KI-Systeme zu effizienteren Abläufen und zu qualitativ besseren Ergebnissen beitragen.

Die DSB zeigt grundsätzlich Verständnis für den Wunsch der Verwaltung, solche Technologien einzusetzen. Der Einsatz von KI kann dazu beitragen, dass Anliegen schneller bearbeitet werden, Informationen verständlicher aufbereitet werden und Mitarbeitende mehr Zeit für komplexe oder besonders schutzbedürftige Fälle haben. Für betroffene Personen kann dies zu kürzeren Wartezeiten, konsistenteren Entscheidungen und insgesamt zu einer verbesserten Servicequalität führen.

Typische Anwendungsfelder in der Verwaltung sind beispielsweise:

- Unterstützung bei der Erstellung und Qualitätssicherung von Texten (z. B. Schreiben, Verfügungen, Standardantworten),
- automatische Zusammenfassungen von Dokumenten oder Akten,
- Übersetzungen und sprachliche Vereinfachung,
- interne Wissenssuche (z. B. in Weisungen, Gesetzestexten, Handbüchern),
- sowie Assistenzfunktionen im Bereich Protokollierung, Transkription und Gesprächszusammenfassungen.

Gleichzeitig ist festzuhalten, dass KI-Systeme – insbesondere generative KI – datenschutzrechtlich anspruchsvoll sind. Je nach Einsatzgebiet können Personendaten in grossem Umfang bearbeitet werden, teilweise auch besonders schützenswerte Per-

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website

www.datenschutz.lu.ch

35

L. Adresse

sonendaten. Hinzu kommen Risiken wie fehlende Nachvollziehbarkeit, unzureichende Zweckbindung, unbeabsichtigte Datenbekanntgaben oder eine Abhängigkeit von internationalen Cloud-Anbietern.

Aus Sicht der DSB ist daher entscheidend, dass KI-Lösungen nicht nur nach ihrem Nutzen beurteilt werden, sondern dass ihre Einführung systematisch geplant, rechtlich abgestützt und technisch sowie organisatorisch abgesichert erfolgt. Eine verantwortungsvolle KI-Nutzung ist möglich – sie setzt jedoch voraus, dass der Schutz der Persönlichkeit, die Transparenz gegenüber den betroffenen Personen und die Kontrolle über die Datenbearbeitung konsequent gewährleistet bleiben.

KI als Hilfsmittel im Tagesgeschäft: keine Generalabsolution, sondern Einzelfallprüfung

Im Berichtsjahr zeigte sich deutlich, dass Organe vermehrt den Wunsch äussern, KI-Lösungen als Hilfsmittel im Tagesgeschäft einzusetzen. Im Vordergrund stehen dabei typische Assistenzfunktionen wie das Zusammenfassen von Dokumenten, das Formulieren von Texten, die Protokollierung von Gesprächen oder die Transkription von Sitzungen.

Aus Sicht der DSB ist die grundsätzliche Rechtmässigkeit solcher Hilfsmittel in vielen Fällen nicht bestritten. Der Einsatz von KI kann – vergleichbar mit anderen digitalen Werkzeugen – dazu beitragen, Abläufe zu vereinfachen und die Bearbeitung von Anliegen effizienter zu gestalten. Entscheidend ist jedoch, dass die Verantwortung für Inhalt, Qualität und Rechtmässigkeit der Bearbeitung weiterhin beim jeweiligen Organ verbleibt.

In der Praxis zeigt sich gleichzeitig, dass es nicht auf die abstrakte Idee «KI» ankommt, sondern auf die konkrete Ausgestaltung des Hilfsmittels. Datenschutzrechtlich relevant sind insbesondere Fragen wie: Welche Daten werden tatsächlich bearbeitet? Handelt es sich um besonders schützenswerte Personendaten? Wo findet die Bearbeitung statt (lokal, in einer Cloud, in der Schweiz oder im Ausland)? Welche Zugriffsmöglichkeiten bestehen für den Anbieter? Wie werden Protokollierung, Speicherung und Löschung geregelt? Und wie wird verhindert, dass Mitarbeitende unbeabsichtigt sensible Informationen in das System einspeisen?

Dabei gilt: Je allgemeiner und unbestimmter ein Vorhaben formuliert ist, desto schwieriger wird eine tragfähige datenschutzrechtliche Beurteilung. Pauschale Aussagen wie «die Lösung soll für alles genutzt werden» oder «Mitarbeitende können beliebige Dokumente hochladen» führen regelmässig dazu, dass eine umfassende Datenschutz-Folgenabschätzung notwendig wird – häufig mit dem Ergebnis, dass die Risiken für Persönlichkeit und Grundrechte in der geplanten Form nicht ausreichend reduziert werden können.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstaltungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Die DSB zeigt Verständnis für den Wunsch nach vertrauenswürdigen, souveränen Alternativen zu grossen internationalen KI-Diensten. Ein «SwissGPT»-Ansatz kann aus Sicht des Datenschutzes eine wichtige Stossrichtung sein, insbesondere wenn Datenstandort, Governance und Zugriffskontrollen konsequent auf Schweizer Anforderungen ausgerichtet sind. Dennoch kann auch für solche Lösungen keine Generalabsolution erteilt werden: Ob ein KI-Hilfsmittel datenschutzkonform eingesetzt werden kann, entscheidet sich stets am konkreten Use Case, am Datenumfang und an den wirksam umgesetzten technischen und organisatorischen Massnahmen.

Beispiel: Einsatzarchitektur und Learnings aus «Red Ink»

Ein praktisches Beispiel dafür, wie KI-Unterstützung im professionellen Kontext datenschutz- und nutzungsorientiert ausgestaltet werden kann, zeigt das KI-Tool «Red Ink»⁶. Die Lösung ist ursprünglich in einer Anwaltskanzlei entwickelt worden und dient dazu, juristische Texte effizienter zu analysieren, zu strukturieren und zu bearbeiten.

Aus datenschutz- und governancebezogener Sicht sind mehrere Elemente hervorzuheben: Erstens zeigt der Einsatz von Red Ink, dass nicht alle Verträge mit KI-Anbieterinnen dieselbe Schutzwirkung entfalten. Eine sorgfältige Vertragsgestaltung mit klaren Verpflichtungen zu Datenverarbeitung, Datenstandort und Zugriffskontrollen ist entscheidend, wenn KI-Dienste in professionellen Umgebungen genutzt werden sollen. Zweitens setzt die Architektur des Tools auf eine Entkopplung der KI-Modelle mittels API. «Red Ink» kann verschiedene KI-Modelle anbinden, je nach Leistungsprofil, Datenschutzerfordernissen und technischer Einbettung. Diese modulare API-Anbindung erlaubt es, KI-Funktionen flexibel auszuwählen und zu integrieren, ohne sich auf ein einzelnes Modell oder einen einzelnen Anbieter festzulegen. Eine solche Architektrichtung ist aus Sicht der Verwaltung und Aufsicht besonders interessant, weil sie mehr Steuerungsmöglichkeiten und eine bessere Kontrolle über die eingesetzten Modelle eröffnet. Drittens lässt sich «Red Ink» direkt in den Arbeitsplatz der Nutzenden einbinden – zum Beispiel als Add-in in gängigen Arbeitsumgebungen – ohne dass zwingend ein separater, grosser KI-Dienst wie ein genereller Copilot verwendet werden muss. Dadurch können Mitarbeitende KI-Funktionalität nutzen, ohne intransparent oder ungefiltert mit generativen Diensten ausserhalb ihrer geschützten Arbeitsumgebung zu interagieren.

Insgesamt verdeutlicht das Beispiel, dass der erfolgreiche Einsatz von KI in der Verwaltung nicht allein von der Leistungsfähigkeit der Modelle abhängt, sondern stark von vertraglicher Absicherung, architektonischer Einbettung und organisatorischer Gestaltung. Solche praxisnahen Lösungsansätze können helfen, KI-Unterstützung datenschutzkonform, nutzerzentriert und nachhaltig umzusetzen.

Und wie bereits erwähnt, braucht es für jeden Use Case eine Datenschutz-Folgenabschätzung!

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

Token Anxiety – neue Belastungsformen im Umgang mit generativer KI

Mit der zunehmenden Verbreitung generativer KI-Systeme zeigen sich neben technischen und rechtlichen Fragestellungen auch neue arbeitskulturelle und psychosoziale Effekte. In Fachkreisen wird in diesem Zusammenhang zunehmend der Begriff «Token Anxiety» verwendet. Gemeint ist eine Form dauerhafter mentaler Anspannung, die aus der permanenten Verfügbarkeit und Nutzung KI-gestützter Systeme entstehen kann.

Generative KI ermöglicht es, Inhalte, Analysen oder Software in sehr kurzer Zeit zu erzeugen und Arbeitsprozesse erheblich zu beschleunigen. Diese Effizienzgewinne können jedoch gleichzeitig zu neuen Erwartungshaltungen führen. Nutzerinnen und Nutzer berichten vermehrt von einem Gefühl, die technologischen Möglichkeiten kontinuierlich ausschöpfen zu müssen, etwa durch das fortlaufende Starten automatisierter Prozesse, das Testen neuer Prompts oder das Überwachen laufender KI-gestützter Abläufe.

Dadurch kann sich die Struktur von Wissensarbeit verändern. Arbeit endet nicht mehr zwingend mit dem Abschluss einer einzelnen Aufgabe. Automatisierte Systeme ermöglichen es vielmehr, dass Prozesse kontinuierlich weiterlaufen. Dies kann zu einer zunehmenden Vermischung von Arbeits- und Erholungszeiten sowie zu einer dauerhaften gedanklichen Beschäftigung mit laufenden KI-gestützten Prozessen führen.

Das Phänomen macht deutlich, dass der Einsatz generativer KI nicht nur Fragen der Rechtmässigkeit, des Datenschutzes oder der Informationssicherheit aufwirft. Ebenso relevant sind organisatorische und arbeitskulturelle Auswirkungen, die sich aus der Beschleunigung digitaler Arbeitsprozesse ergeben können.

Für Organisationen, die generative KI einsetzen, wird es daher zunehmend wichtig, klare Rahmenbedingungen für deren Nutzung zu definieren. Dazu gehören transparente Einsatzregeln, realistische Produktivitätserwartungen sowie eine Nutzungskultur, die Effizienzgewinne nicht in dauerhafte Leistungs- oder Verfügbarkeitsanforderungen übersetzt. Eine verantwortungsvolle KI-Governance muss deshalb neben technischen und rechtlichen Aspekten auch die Auswirkungen auf Arbeitsorganisation und Mitarbeiterschutz berücksichtigen.

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



G. KONTROLLEN

Die DSB ist nach § 23 KDSG gehalten, die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren. Im Berichtsjahr hat die DSB eine Datenschutzkontrolle durchgeführt.

Die DSB hat sich entschieden, eine Datenschutzkontrolle der Videoüberwachung einer Gemeinde durchzuführen, bei welcher bisher keine Beratung oder Kontrolle in diesem Bereich erfolgt ist. Der Gemeinderat der kontrollierten Gemeinde hat vor rund 8 Jahren die Videoüberwachung eines Schulhauses für Schülerinnen und Schüler von der Kindergarten- bis zur Sekundarstufe und eines öffentlichen Spielplatzes mit insgesamt 4 Kameras bewilligt.

Die DSB hat sich bei ihrer Kontrolle auf die Einhaltung der gesetzlichen Vorgaben (Gesetz über die Videoüberwachung und seine Verordnung, KDSG, KDSV), insbesondere der Verhältnismässigkeit der Ausgestaltung der Videoüberwachung und der einzelnen Kameras fokussiert. Vor Ort fand nebst den Interviews eine Besichtigung der Kamerastandorte, Kameraperimeter sowie der Serverstandorte der beiden Videoüberwachungsanlagen der Gemeinde statt.

Bei der Kontrolle hat die DSB festgestellt, dass die Gemeinde eine öffentliche Liste mit den bewilligten Kamerastandorten führt und über ein Videoüberwachungsreglement verfügt, welches wichtige datenschutzrechtliche Aspekte regelt. Allerdings hat die Kontrolle auch gezeigt, dass insbesondere eine verbindliche Regelung der

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstaltungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Zugriffsprozesse und eine Protokollierung der Zugriffe fehlt. So zeigte sich im Rahmen der mit den Vertretern der verantwortlichen Organe geführten Interviews, dass die bisherigen Zugriffe auf das Videoüberwachungssystem des einen Standorts, unzulässig waren, soweit sie nicht der Ahndung von Straftaten bzw. Durchsetzung von Ansprüchen aus Straftaten durch die Strafverfolgungsbehörden dienten.

Weiter finden weder regelmässige technische Wartungen der Geräte durch die verantwortlichen Organe noch eine periodische Überprüfung der Erforderlichkeit der bewilligten Videoüberwachungsanlagen durch den Gemeinderat statt. Die Kontrolle hat gezeigt, dass bei einem Standort eine Kamera seit geraumer Zeit gar nicht mehr im Einsatz ist und eine andere aufgrund von Umbauarbeiten mittlerweile nicht mehr überwacht, was dem Schutzzweck dient. Auch beim zweiten Standort wurde festgestellt, dass eine Kamera aufgrund einer lockeren Halterung nicht mehr den bewilligten Perimeter filmt. Bei einem der Standorte fehlt überdies eine Kennzeichnung der Videoüberwachung.

Die DSB wurde im Rahmen der Kontrolle darüber informiert, dass im Zuge von Umbauten und Erweiterungen des Schulhauses eine neue Videoüberwachung mit rund 15 Kameras geplant sei, welche das Schulhausareal zukünftig rund um die Uhr überwachen solle. Die DSB nahm diese Information zum Anlass, um im Kontrollbericht die Unverhältnismässigkeit dieses undifferenzierten Vorhabens aufzuzeigen und auf wichtige datenschutzrechtliche Aspekte bei der Planung und Umsetzung der neuen Videoüberwachungsanlage hinzuweisen.

Bereits frühere Kontrollen sowie andere durch die DSB getätigte Abklärungen und Beratungen haben gezeigt, dass bei der Videoüberwachung von öffentlich zugänglichen Orten durch kommunale und kantonale Organe der Grundvoraussetzung der Verhältnismässigkeit oft zu wenig oder gar nicht Rechnung getragen wird. Überdies scheint manchen verantwortlichen Organen das Bewusstsein zu fehlen, dass es mit dem Installieren einer solchen Videoüberwachungsanlage nicht getan ist, sondern dass damit auch gesetzlich geregelte Pflichten verbunden sind. Die DSB wird deshalb auch künftig die Einhaltung der rechtlichen Vorgaben von Videoüberwachungsanlagen prüfen und gegebenenfalls von ihren Befugnissen nach § 24 KDSG Gebrauch machen, um entsprechende Massnahmen zu verfügen.

H. SCHULUNGEN UND INFORMATIONS- VERANSTALTUNGEN / VORTRÄGE

Die gezielte Aus- und Weiterbildung kantonaler und kommunaler Stellen ist zentral, um den Datenschutz flächendeckend zu gewährleisten. Durch proaktive Sensibilisierung beugen wir Grundrechtsverletzungen vor und stärken das Vertrauen in die Verwaltung. In diesem Sinne unterstützt die DSB verantwortliche Organe bei internen Schulungen.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstaltungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Ein Highlight im September 2025 war das Kaderseminar für Führungskräfte, bei dem die DSB die Gelegenheit nutzte, neu eintretende Führungspersonen in die Grundlagen des Datenschutzes einzuführen. Ergänzend dazu hielt die DSB im Berichtsjahr drei fachspezifische Kurzreferate bei verschiedenen kantonalen Verwaltungseinheiten.

I. GESETZGEBUNG UND VERNEHMLASSUNGEN

Die DSB prüft Gesetzes- und Verordnungsentwürfe von Kanton, Gemeinden und Bund im Hinblick auf ihre datenschutzrechtlichen Auswirkungen und gibt dazu Stellungnahmen ab (§ 23 Abs. 1 lit. e KDSG). Die Stellungnahme wird unabhängig, teilweise in Koordination mit privatim, der Konferenz der Schweizer Datenschutzbeauftragten, erarbeitet. Darüber hinaus ist die Beteiligung an Rechtsetzungsprojekten ein wesentlicher Bestandteil ihrer Tätigkeit (§ 23 Abs. 1 lit. b und e KDSG). Die DSB bringt sich hierzu in unterschiedliche Arbeitsgruppen sowie in laufende Gesetzgebungsverfahren ein, sofern datenschutzrelevante Fragestellungen betroffen sind.

Im Berichtsjahr nahm die DSB zu einer Reihe von Vorhaben auf kantonaler und eidgenössischer Ebene Stellung, namentlich zu den nachfolgend aufgeführten Projekten:

a) Kantonale Gesetzgebungsverfahren

Erlass eines E-Government-Gesetzes

Im Rahmen der Vernehmlassung zum E-Government-Gesetz hielt die DSB fest, dass staatliche Dienstleistungen auch künftig in nicht-elektronischer Form zugänglich bleiben sollen, da Bürgerinnen und Bürger darauf vertrauen dürfen. Sie wies darauf hin, dass elektronische Dienstleistungsangebote regelmässig mit zusätzlichen Datenbearbeitungen verbunden sind und entsprechend erhöhte Datenschutzrisiken mit sich bringen. Auslagerungen an Cloud-Anbieter wurden insbesondere im Zusammenhang mit besonders schützenswerten Personendaten kritisch beurteilt; solche Auslagerungen seien nach Möglichkeit zu vermeiden, andernfalls sei auf einschlägige Empfehlungen, insbesondere das Cloud-Merkblatt von privatim, abzustellen. Die DSB betonte zudem, dass die datenschutzrechtlichen Grundsätze in jedem Fall einzuhalten und die föderalen Zuständigkeitsordnungen zu berücksichtigen sind. Hinsichtlich des elektronischen Identitätsverwaltungssystems wurde hervorgehoben, dass unterschiedliche Vertrauensstufen unterschiedlich intensive Datenbearbeitungen nach sich ziehen, weshalb die entsprechenden Mindestanforderungen sowie die damit verbundenen Datenbearbeitungen auf geeigneter Normstufe transparent zu regeln sind.

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstaltungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

Totalrevision des Gesetzes über die Niederlassung und den Aufenthalt (NG)

Stellung nahm die DSB des Weiteren zur Totalrevision des Gesetzes über die Niederlassung und den Aufenthalt. Die Totalrevision bezweckt primär die Modernisierung in sprachlicher und inhaltlicher Sicht. Schwerpunkt bei letzterem sind die Anpassung an den bereits existierenden elektronischen Datenaustausch sowie der Verzicht auf eine physische Hinterlegung des Heimatscheins in allen Luzerner Gemeinden. Die DSB hat sich in ihrer Vernehmlassung auch zum Verordnungstext geäussert.

Aus datenschutzrechtlicher Sicht gab auf Gesetzesstufe das Verfahren betreffend Aufnahme weiterer Merkmale auf Verordnungsstufe sowie der Einbezug der DSB in dieses Verfahren Anlass zu einigen Hinweisen. Auf Verordnungsstufe hat die DSB die vorgesehene Aufnahme der Merkmale «E-Mailadressen», «Telefonnummer» und «Mobiltelefonnummer» vor dem Hintergrund der Grundsätze der Verhältnismässigkeit, der Datenrichtigkeit und der Datensicherheit kritisch beleuchtet.

Revision Kantonales Energiegesetz

Im Rahmen der Vernehmlassung zur Änderung des Kantonalen Energiegesetzes (KEng) vom Juni 2025 hat die DSB insbesondere zu § 33 KEng Stellung genommen. Sie begrüsst ausdrücklich, dass die Auskunftspflicht neu auf alle ausgedehnt wird, da dies die Vollzugsfähigkeit stärkt und zur Rechtsgleichheit beiträgt. Gleichzeitig hat sie angeregt, die datenschutzrechtlichen Anforderungen im Gesetz oder auf Verordnungsstufe zu präzisieren. Namentlich wurde auf die Notwendigkeit einer hinreichenden Rechtsgrundlage und der konsequenten Beachtung des Verhältnismässigkeitsprinzips hingewiesen. Zudem empfahl die DSB, die Zweckbindung, Datensparsamkeit und – wo möglich – Anonymisierung ausdrücklich zu verankern, Aufbewahrungsfristen klar zu regeln sowie angemessene technische und organisatorische Massnahmen sicherzustellen. Bei risikoreichen oder umfangreichen Datenbearbeitungen sei eine Datenschutz-Folgenabschätzung gemäss § 7a KDSG vorzusehen. Schliesslich wurde betont, dass die Mitwirkung durch Datenbereitstellung datenschutzkonform zu erfolgen hat und keine generelle Pflicht zur Weitergabe sämtlicher vorhandener Daten begründet.

b) Eidgenössische Gesetzgebungsverfahren

Zudem wirkte die DSB an Vernehmlassungen auf eidgenössischer Ebene mit und nahm zu mehreren bundesrechtlichen Vorlagen Stellung, darunter zu den folgenden:

- Revision des Einführungsgesetzes zum Bundesgesetz über die Krankenversicherung
- Teilrevision des Bundesgesetzes über Schuldbetreibung und Konkurs
- Revision der Postverordnung
- Verordnungsentwurf zum E-ID-Gesetz
- Erlass eines Bundesgesetzes über die Gasversorgung

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse



J. ZUSAMMENARBEIT MIT ANDEREN DATENSCHUTZSTELLEN

a) **privatim**

Der Kanton Luzern ist Mitglied von **privatim**, der Konferenz der schweizerischen Datenschutzbeauftragten. **Privatim** bezweckt, den Anliegen des Datenschutzes Nachdruck zu verschaffen. Als Konferenz aller Datenschutzaufsichtsbehörden fördert **privatim** die Zusammenarbeit unter den Schweizer Kantonen, den Gemeinden und dem Bund im Datenschutz durch ständigen Informationsaustausch und ermöglicht so den wirkungsvollen Einsatz der Ressourcen.

Privatim führt zweimal jährlich ein Plenum durch, bei dem sich die Mitglieder zwecks Informationsaustauschs in aktuellen Datenschutzfragen treffen. Diese Veranstaltungen werden abwechselungsweise durch die einzelnen Mitgliedskantone organisiert. Im Berichtsjahr konnte in St. Gallen das Frühjahressplenum durchgeführt werden, das sich mitunter auf die Gesundheitsdaten in der Cloud konzentrierte. Im Herbst trafen sich die Datenschutzbeauftragten in Bern.

Die DSB ist ausserdem in vier Arbeitsgruppen von **privatim** vertreten. Die Arbeitsgruppe «ICT» beschäftigt sich mit speziellen Informatiklösungen für die Kantone und die Anforderungen an die Datensicherheit. Die Arbeitsgruppe «Sicherheit» befasst sich mit dem Einsatz von IT-Tools im Polizeibereich, während sich die Arbeitsgruppe «Digitale Verwaltung» insbesondere mit digitalen Verwaltungslösungen befasst. Bei

INHALT

Tätigkeitsbericht 2025 Datenschutz- beauftragten des Kantons Luzern	
2	Vorwort
4	Inhalt
5	A. Gesetzlicher Auftrag
7	B. Statistische Angaben
10	C. Datenschutzverletzung
13	D. Exkurs: Allgemeine Ausführungen zur Auslagerung (Cloud)
17	E. Projekte
23	F. Exkurs: Künstliche Intelligenz in der Verwaltung
28	G. Kontrollen
29	H. Schulungen und Informationsveranstal- tungen / Vorträge
30	I. Gesetzgebung und Vernehmlassungen
32	J. Zusammenarbeit mit anderen Datenschutzstellen
34	K. Website www.datenschutz.lu.ch
35	L. Adresse

der Arbeitsgruppe «Gesundheit» werden Erfahrungen zu datenschutzrechtlichen Themen im Gesundheitsbereich ausgetauscht.

Besonders hervorzuheben ist die im Berichtsjahr von privatim veröffentlichte Resolution zur Auslagerung von Datenbearbeitungen in die Cloud. Darin wird klargestellt, dass die Auslagerung sensibler Personendaten durch öffentliche Organe in Cloud-Lösungen internationaler Anbieter zumeist als unzulässig einzustufen ist.⁷

b) Schengen Koordinationsgruppe

Die Zusammenarbeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) mit den kantonalen Datenschutzbeauftragten ist aufgrund der Schengen-Assoziierungsabkommen gesetzlich vorgeschrieben. Der EDÖB und die kantonalen Datenschutzbehörden sind verpflichtet, bei der Beaufsichtigung der Datenbearbeitungen, die in Anwendung der Assoziierungsabkommen erfolgen, aktiv zusammenzuarbeiten. Die Zusammenarbeit erfolgt über die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Schengen-Assoziierungsabkommen», an deren Sitzungen auch die DSB jeweils teilnimmt.

Jährlich finden zwei Sitzungen in Bern statt. Die DSB nahm an beiden Sitzungen teil. An diesen Sitzungen informiert der EDÖB über die Aktualitäten und Entwicklungen in der Aufsicht des Schengener-Informationssystems (SIS) und des Visa-Informationssystems (VIS). Zudem tauschen sich der EDÖB sowie die Kantone gegenseitig über durchgeführte SIS- oder VIS-Kontrollen aus.



⁷ <https://www.privatim.ch/de/publikation-resolution-zur-auslagerung-von-datenbearbeitungen-in-die-cloud/>

INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

K. WEBSITE DATENSCHUTZ.LU.CH

Im Berichtsjahr nahm die Nutzung des Internetauftritts datenschutz.lu.ch erneut deutlich zu. Gegenüber dem Vorjahr stieg die Zahl der Besucherinnen und Besucher um 22.40 %, die Seitenansichten um 15.77 % und die Downloads um 20.27 %. Im selben Zeitraum wurde der Internetauftritt laufend aktualisiert und um mehrere News, Merkblätter und fachliche Einschätzungen ergänzt. Dazu zählen namentlich Beiträge zur Auslagerung von Datenbearbeitungen in die Cloud, Microsoft 365, besonders schützenswerten Personendaten sowie GenAI und Datenschutz. Vor diesem Hintergrund ist die positive Entwicklung der Nutzungszahlen nachvollziehbar. Ebenfalls in diesen Zeitraum fällt die neue Besetzung der DSB.

Dienstleistungen	2020	2021	2022	2023	2024	2025	Entwicklung (2024–25)
Besucher Insgesamt	4'563	4'660	4'855	6'834	6'149	7'504	+ 22.40 %
Ø Besucher pro Tag	12.5	12.8	13.3	18.7	16.8	20.6	+ 22.60 %
Seitenansichten Insgesamt	15'891	13'453	13'656	17'813	15'652	18'119	+ 15.77 %
Ø Seitenansichten pro Tag	43.5	36.9	37.4	48.9	42.8	49.7	+ 16.15 %
Downloads	1'275	1'408	1'496	2'211	2'226	2'677	+ 20.27 %

Die Entwicklung zeigt, dass der Internetauftritt als Informations- und Arbeitsinstrument weiterhin stark genutzt wird. Besonders die hohen Downloadzahlen weisen auf ein anhaltendes Interesse an aktuellen, fundierten und praxisnahen Unterlagen hin. Die Website bleibt damit ein wichtiger Baustein für die Sichtbarkeit der Datenschutzaufsicht und für die niederschwellige Bereitstellung datenschutzrechtlicher Informationen.



INHALT

Tätigkeitsbericht 2025
Datenschutz-
beauftragten des
Kantons Luzern

2

Vorwort

4

Inhalt

5

A. Gesetzlicher Auftrag

7

B. Statistische Angaben

10

C. Datenschutzverletzung

13

D. Exkurs: Allgemeine
Ausführungen zur
Auslagerung (Cloud)

17

E. Projekte

23

F. Exkurs: Künstliche
Intelligenz in der
Verwaltung

28

G. Kontrollen

29

H. Schulungen und
Informationsveranstal-
tungen / Vorträge

30

I. Gesetzgebung und
Vernehmlassungen

32

J. Zusammenarbeit
mit anderen
Datenschutzstellen

34

K. Website
www.datenschutz.lu.ch

35

L. Adresse

L. ADRESSE

Datenschutzbeauftragte des Kantons Luzern

Bahnhofstrasse 15

6002 Luzern

Telefon 041 228 61 00

datenschutz@lu.ch

datenschutz.lu.ch

