Tätigkeitsbericht 2022

Datenschutzbeauftragter des Kantons Graubünden

Datenschutzbeauftragter des Kantons Graubünden

RA Thomas Casanova · Kornplatz 2 · 7001 Chur
Telefon 081 256 55 58 · dsb@staka.gr.ch

Impressum
Gestaltung / Druck: Casutt Druck & Werbetechnik AG, Chur
Gedruckt auf Cyclus Recycling-Papier aus 100% speziell sortierten Druckerei- und Büroabfällen

Inhalt

I. Vorwort

KI/AI

Im Bereich Informatik beherrschte im Jahr 2022 der Begriff künstliche Intelligenz (KI) bzw. artificial intelligence (AI) die Medien. Das zu Microsoft gehörende Unternehmen OpenAI lancierte ein KI-Modell namens ChatGPT (GPT steht für Generative Pre-trained Transformer, ein generierender vortrainierter Transformator). Auf Knopfdruck generiert der Chatbot je nach spezifischer Aufgabe einen eigenen Text, wobei auf eine riesige und vielfältige Datenbank zurückgegriffen wird, die vorher eingelesen wurde. Es entsteht der Eindruck, die Texte seien von Menschenhand geschaffen. Indessen beruhen die Algorithmen auf einem Sprachmodell, das menschlichen Denkmustern nachgebildet wird. Somit können künftige Aussagen aus vergangenen Werten vorhergesagt werden. Der Input wird also so verarbeitet, dass der Output einen menschlichen Anschein hat.

Die Entstehung von KI geht bis ins Jahre 1955 zurück. Die Idee, dass der Mensch eine Maschine bauen könnte, die intelligentes Verhalten zeigt, ist natürlich viel älter. In den Nachkriegsjahren und mit dem Beginn des Computerzeitalters wurden Mustererkennungs- und Expertensysteme entwickelt und verfeinert. KI-Systeme stehen denn auch schon seit geraumer Zeit im Einsatz, sei es in der Diagnose von Krankheiten, Suchmaschinen, Texterkennung, maschinellem Übersetzen usw. Einen regelrechten Hype erfuhr KI mit der breitangelegten Öffnung von ChatGPT. Die Möglichkeiten von KI im alltäglichen Umgang mit Daten wurden einer breiten Bevölkerungsschicht plakativ veranschaulicht. Es verwundert deshalb nicht, dass neben der Bevölkerung auch die Politik auf KI aufmerksam wurde. In Italien wurde ChatGPT beispielsweise vorübergehend verboten.

KI in einer breiten praktischen Anwendung wird unser Leben verändern. Welche Berufsgruppen durch KI gefährdet sind, lässt sich heute nicht abschätzen. Dabei gehen auch die Ansichten der Fachleute auseinander. Betroffen sind wir indessen alle von dieser Entwicklung, und wir können uns ihr auch nicht verschliessen. Es gilt, sich mit KI auseinander zu setzen und ihr mit einer gesunden Skepsis zu begegnen. Eine grundsätzliche Ablehnung ist nicht zielführend und wird die Weiterentwicklung auch nicht verhindern.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Allgemeines

1. Neues Datenschutzgesetz und Wirksamkeit von Datenschutzerklärungen

(verfasst von MLaw Elena Liechti)

I. Entstehung des Datenschutzrechts

Das Datenschutzrecht ist als Reaktion auf das Sammeln und Bearbeiten von Personendaten durch staatliche Behörden entstanden.[1] Das Datenschutzrecht der Schweiz nahm seinen Anfang in einzelnen Kantonen und gelangte dann, nach langwierigen Gesetzgebungsprozessen mit dem Erlass des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG, SR 235.1) zu einem ersten Abschluss. Mit dem Beitritt der Schweiz am 2. Oktober 1997 zum Europäischen Übereinkommen zum Schutz der Menschen bei der automatisierten Verarbeitung von personenbezogenen Daten und durch bereichsspezifische Einzelregelungen (v.a. im Ausländer-, Sicherheits- und Sozialversicherungsbereich) wurde das Datenschutzrecht verfestigt. Die Unterzeichnung der bilateralen Verträge mit der EU führte zudem dazu, dass sich die Schweiz immer mehr am EU-Datenschutzrecht orientierte.[2]

Das heutige Datenschutzrecht ist einerseits im Bundesgesetz (DSG) geregelt, welches auf Private und Bundesbehörden anwendbar ist. Die Kantone haben eigene Datenschutzgesetze, die auf kantonale Behörden anwendbar sind. Im Kanton Graubünden ist dies das Kantonale Datenschutzgesetz vom 10. Juni 2001 (KDSG, BR 171.100), die letzten Änderungen traten am 1. Januar 2019 in Kraft.

II. Grundsätze des bestehenden Datenschutzrechts

Das Datenschutzrecht bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Personendaten bearbeitet werden. Als Personendaten gelten Angaben, die sich auf eine bestimmte oder zumindest bestimmbare natürliche oder juristische[3] Person beziehen,

---

[1] *FLORENT THOUVENIN/NADJA BRAUN BINDER, (2022), Transparenz durch Datenschutzerklärungen von Behörden, in: Zeitschrift für Schweizerisches Recht (ZSR); 5-29.*

[2] *RAINER J. SCHWEIZER, (2009), Hintergrund und Überblick, in: Die Revision des Datenschutzrechts (Forum Europarecht); 30.*

[3] *Mit dem neuen Datenschutzrecht (revDSG vgl. Ziffer C) wurde der Geltungsbereich des DSG auf die Bearbeitung von Personendaten natürlicher Personen eingegrenzt, bis zum 1. September 2023 sind auch juristische Personen noch vom Geltungsbereich des DSG erfasst. Juristische Personen geniessen aber auch nach dem Inkrafttreten des revDSG weiterhin den Schutz durch Art. 28 ff. ZGB, das UWG, das URG sowie die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnisse (vgl. MATTHIAS R. SCHÖNBÄCHLER, (2023), Zum neuen Schweizer Datenschutzrecht in: Zeitschrift des bernischen Juristenvereins (ZBJV), S. 180. Im Folgenden zitiert als SCHÖNBÄCHLER S.*

so etwa Name, Geburtsdatum, Adresse, Telefonnummer, IP-Adresse oder ein Fingerabdruck. Eine natürliche Person ist bestimmbar und wird betroffene Person, wenn sie direkt oder indirekt identifiziert werden kann. Daher sind auch Äusserungen, Video- und Bildaufnahmen, Korrespondenz oder Registerauszüge Personendaten. Bearbeiten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mittel und Verfahren. Das Gesetz zählt Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgegeben, Archivieren, Löschen oder Vernichten von Daten auf.[4]

Das Datenschutzrecht legt fest, unter welchen Voraussetzungen eine Datenbearbeitung zu einer Persönlichkeitsverletzung führt und in welchen Fällen eine Persönlichkeitsverletzung gerechtfertigt sein kann. Zu den zentralen Grundsätzen des Datenschutzes gehört, dass Personendaten nur rechtmässig bearbeitet werden dürfen. Ihre Bearbeitung muss nach Treu und Glauben erfolgen und hat verhältnismässig zu sein, sprich es dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und erforderlich sind. Sodann dürfen Personendaten nach den Grundsätzen der Zweckbindung und Transparenz nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft und nur so verarbeitet werden, dass es mit diesem Zweck vereinbar ist.[5]
Aus diesen Grundsätzen ergibt sich auch, dass Daten vernichtet oder anonymisiert werden müssen, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Ferner verlangt der Grundsatz der Richtigkeit ein Vergewissern über deren Richtigkeit und angemessene Massnahmen zur Berichtigung oder Löschung unrichtiger oder unvollständiger Daten. Schliesslich müssen Inhaber von Daten dem Risiko von Datenschutzverletzungen durch geeignete Massnahmen vorbeugen.[6]

---

[4] *SCHÖNBÄCHLER, S. 176.*

[5] *SCHÖNBÄCHLER, S. 28 F.*

[6] *SCHÖNBÄCHLER, S. 29.*

III. Das revidierte Datenschutzgesetz

Mit dem totalrevidierten Datenschutzgesetz soll der Datenschutz an die technologischen Entwicklungen angepasst werden und das schweizerische Datenschutzniveau soll sich dem europäischen Standard annähern.[7] Dabei werden insbesondere die Transparenz von Datenbearbeitungen verbessert und die Selbstbestimmung der betroffenen Personen über ihre Daten gestärkt. Gleichzeitig soll die Totalrevision der Schweiz erlauben, bereits bestehendes EU-Recht zu ratifizieren (Datenschutzübereinkommen SEV 108), umzusetzen (Schengen-relevante Richtlinie (EU) 2016/680 über den Datenschutz in Strafsachen) und sich insgesamt den in der EU geltenden Anforderungen im Bereich Datenschutz anzunähern. Diese Annäherung und die Ratifizierung des revidierten Übereinkommens SEV 108 sind zentral, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig ohne weitere Hürden möglich bleibt.[8]

Das Parlament hat die Vorlage des Bundesrates vom 15. September 2017 zur Totalrevision des DSG (E-DSG) in zwei Etappen aufgeteilt. In einer ersten Etappe wurde ausschliesslich die schengen-relevante EU-Richtlinie 2016/680 umgesetzt. Dazu wurde – übergangsweise – ein neues Schengen-Datenschutzgesetz (SDSG, SR 235.3) geschaffen, welches am 1. März 2019 in Kraft getreten ist.[9]

In der zweiten Etappe wurde die «eigentliche» Totalrevision des DSG beraten.[10] Das neue Datenschutzgesetz (revDSG) und die neue Datenschutzverordnung (DSV) sowie die neue Verordnung über Datenschutzzertifizierungen (VDSZ) treten am 1. September 2023 in Kraft.

---

[7] *Bundesamt für Justiz, Oktober 2022, Totalrevision des Datenschutzgesetzes (DSG), S.1. Im Folgenden zitiert als BJ-D-12643401/222, S.*

[8] *https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html, zuletzt besucht am 22.05.2023.*

[9] *BJ-D-12643401/222, S. 3.*

[10] *BJ-D-12643401/222, S. 3.*

IV. Bedeutung der Transparenz

Das Datenschutzrecht unterliegt einer grundrechtlichen Prägung. Es soll insbesondere das Recht auf Privatsphäre (Art. 13. Abs. 1 der Schweizerischen Bundesverfassung BV, SR 101) und das Recht auf Schutz vor Missbrauch der persönlichen Daten gemäss Art. 13 Abs. 2 BV geschützt werden. Nach ständiger Rechtsprechung des Bundesgerichts umfasst Art. 13 Abs. 2 BV das Recht auf informationelle Selbstbestimmung. Die Gewährleistung eines solchen Rechts wird auch in der Lehre als Teilgehalt des Rechts auf Schutz vor Missbrauch der persönlichen Daten fast einhellig erkannt.[11]

Die Ausübung des Grundrechts auf informationelle Selbstbestimmung setzt voraus, dass die betroffenen Personen um die Bearbeitung ihrer Personendaten wissen. Dieses Wissen umfasst nicht nur den blossen Umstand der Datenbearbeitung, sondern auch Informationen über die Art der bearbeiteten Daten, den Zweck der Bearbeitung und die verantwortliche Behörde sowie allfällige Empfänger der Personendaten. Da informationelle Selbstbestimmung ohne diese Informationen nicht möglich ist, kommt dem Grundsatz der Transparenz der Datenbearbeitung, der auch als Grundsatz der Erkennbarkeit bezeichnet wird, ein hoher Stellenwert zu.[12]

Die Steigerung der Transparenz durch erhöhte Informationspflichten war ein zentrales Ziel für die Revision des Datenschutzrechts.[13] Zwar wird der Grundsatz der Transparenz im revDSG nicht explizit erwähnt, dies ändert jedoch nichts an dessen Geltung.[14] Der Grundsatz der Transparenz wird in der Informationspflicht (Art. 19 ff. revDSG) und dem Auskunftsrecht (Art. 25 ff. revDSG) konkretisiert.[15]

---

[11] *THOUVENIN/ BINDER, S. 13 F.*

[12] *THOUVENIN/ BINDER, S. 14.*

[13] *Botschaft revDSG 7050.*

[14] *THOUVENIN/ BINDER, S. 16.*

[15] *Die kantonalen Datenschutzgesetzte regeln die Datenbearbeitung durch kantonale Behörden. In den kantonalen Erlassen sind diese Rechte und Pflichten ebenfalls verankert.*

Die Regelung der Informationspflicht sieht vor, dass die Verantwortlichen die betroffenen Personen angemessen über die Bearbeitung der Daten informieren müssen (Art. 19 Abs. 1 Teilsatz 1 revDSG). Der Begriff «angemessen» ist auslegungsbedürftig. Nach dem Wortgebrauch her bedeutet er, dass die Information den Verhältnissen entsprechend zu erfolgen hat. Dies gilt für Inhalt und Umfang der Information, ebenso wie für die Adressaten und die Zugänglichkeit. Das bedeutet allerdings nicht, dass den Betroffenen die Informationen zugestellt oder aktiv angezeigt werden müssen (bspw. per E-Mail oder durch ein Pop-up-Fenster auf einer Website). Vielmehr genügt es, wenn die betroffenen Personen auf einfache Weise selbst auf die Informationen zugreifen können, so bspw. auf eine Datenschutzerklärung die auf einer Website zugänglich gemacht wird.[16]

Die Informationen sollten, sofern sie sich nicht an Fachpersonen richten, in einfacher Sprache abgefasst sein und für die betroffenen Personen leicht auffindbar und zugänglich sein.[17]

Es kann also festgehalten werden, dass weder der Grundsatz der Transparenz noch die Informationspflicht oder das Auskunftsrecht verlangen, dass die zur Schaffung von Transparenz erforderliche Information in einer bestimmten Form vermittelt wird. Es ist eine Form zu wählen, die dem Zweck einer transparenten Datenbearbeitung gerecht wird. Auch Bundesorgane sind daher frei, das geeignete Mittel zu wählen, um die Transparenz ihrer Datenbearbeitungen zu gewährleisten. Dasselbe muss für die kantonalen Behörden gelten.[18]

In der Praxis spielen Datenschutzerklärungen eine immer grössere Rolle. Damit soll der Informationspflicht nachgekommen und Transparenz geschaffen werden. Es lohnt sich daher, das Mittel der Datenschutzerklärung genauer zu betrachten. Dabei wird das Augenmerk auf die Datenbearbeitung der kantonalen Behörden gerichtet, zumal diese durch das kantonale Recht und den kantonalen Datenschützer zu überwachen sind.

---

[16] *THOUVENIN/ BINDER, S. 17.*

[17] *THOUVENIN/ BINDER, S. 17.*

[18] *THOUVENIN/ BINDER, S. 21.*

V. Datenschutzerklärungen

a) Informationspflicht im kantonalen Recht

Die Informationspflicht für Bundesbehörden ist in Art. 19 revDSG geregelt. Für die kantonalen Behörden ist das jeweilige kantonale Recht ausschlaggebend. Im bündnerischen Datenschutzgesetz wird in Art. 2 KDSG auf die Vorschriften des Bundes für Bundesbehörden verwiesen. Damit gilt Art. 19rev DSG sinngemäss auch für kantonale Behörden.

Die Kantone sind aufgrund ihrer verfassungsrechtlich garantierten Organisationsautonomie kompetent den Datenschutz im kantonalen öffentlichen Bereich, also für kantonale Behörden und Verwaltungsstellen, selbstständig zu regeln. Dabei sind die Kantone jedoch an die bundesrechtlichen Vorgaben und somit insbesondere zur Wahrung des Rechts auf informelle Selbstbestimmung gebunden.[19] Zudem verlangt das Datenschutzübereinkommen SEV 108 eine aktive Information über das Beschaffen von Personendaten. Diese Informationspflicht war zuvor lediglich für sensitive Personendaten vorgesehen. Diese Anforderungen müssen auch von den Kantonen umgesetzt werden.[20]

b) Nutzen von Datenschutzerklärungen

Wie bereits erwähnt, ist die Datenschutzerklärung ein weltweit anerkanntes und verbreitetes Mittel für das Schaffen von Transparenz.[21] Auch kantonalen Behörden steht es frei Datenschutzerklärungen für die Herstellung der Transparenz einzusetzen. Jedoch ist fraglich, wie diese ausgestaltet sein sollen, sodass auch ein effektiver Nutzen entsteht und Betroffene in verständlicher und gleichzeitig genügend konkreter Weise über die Datenbearbeitung informiert werden.

---

[19] *DOMINIKA BLONSKI, (2022), Was bedeutet die Revision für die kantonalen Datenschutzgesetze?, in: Die Revision des Datenschutzgesetzes des Bundes, S. 93.*

[20] *BLONSKI, S. 100.*

[21] *THOUVENIN/ BINDER, S. 22.*

Es kommt oft vor, dass beim Besuch einer Website der Nutzer mittels Pop-up-Fenster zur Einverständniserklärung der Allgemeinen Geschäftsbedingungen (AGB) aufgefordert wird. Ähnlich verhält es sich mit den sogenannten Cookies, mit denen u.a. Personendaten erhoben werden. Ein Grossteil der Internetnutzenden wird die diesbezüglichen Bedingungen (u.a. AGB's und Datenschutzerklärung) nicht durchlesen, sondern es wird ohne effektive Kenntnis den Bedingungen die Zustimmung erteilt. Dies dürfte u.a. auch darauf zurückzuführen sein, dass die Erklärungen meist sehr ausführlich gehalten sind, teilweise auf AGB's verwiesen wird (oder umgekehrt) und die Erläuterung für juristische Laien kaum verständlich sind. Der exzessive Gebrauch von Datenschutzerklärungen könnte daher als Feigenblatt für die Durchsetzung der Informationspflicht missbraucht werden.

Es stellt sich daher die Frage, wie Datenschutzerklärungen ihrem Sinn und Zweck, nämlich die Transparenz von Datenbearbeitungen herzustellen, gerecht werden können. Dabei bietet es sich an, anstatt den betroffenen Personen alle Informationen in Textform in einem einzigen oder allenfalls mehreren Dokumenten zur Verfügung zu stellen, ein differenzierter Ansatz zu verfolgen, der meist als «layered approach» bezeichnet wird. Ausgehend von der Erkenntnis, dass die meisten Betroffenen Datenschutzerklärungen nicht lesen, werden Betroffenen auf zwei oder drei Ebenen unterschiedlich detaillierte Informationen zugänglich gemacht. Auf einer ersten Ebene finden sich Angaben zu den wichtigsten Eckpunkten der Datenbearbeitungen, bspw. mithilfe von Symbolen, die es den Betroffenen erlauben, sich innert weniger Sekunden einen Überblick zu verschaffen. Auf einer zweiten Ebene werden die Datenbearbeitungen in kurzen Texten mit einfachen Worten erklärt und auf einer dritten Ebene finden sich detaillierte und technisch hinreichend präzise Informationen. Alle drei Ebenen bilden zusammen die Datenschutzerklärung. Gemeinsam vermögen sie eine hohe Transparenz zu gewährleisten, indem sie dem Bedürfnis nach rascher, einfacher sowie detaillierter und technischer Information zugleich Rechnung tragen. Zumindest für diejenigen Personen, die sich für die Bearbeitung «ihrer» Personendaten interessieren, sind Datenschutzerklärungen damit ein geeignetes Mittel, um die gesetzlich geforderte Transparenz sicherzustellen.[22]

[22] *THOUVENIN/ BINDER, S. 23 F.*

2. *Einführung von Microsoft 365 in der kantonalen Verwaltung*

I. Ausgangslage

Zahlreiche Kantone befassen sich mit der Einführung von M365 in den jeweiligen Verwaltungen. Im Zusammenhang damit sind eine Vielzahl von Spezialisten befragt, Gutachten erstellt und Prüfungen vorgenommen worden. Darin wird erkennbar, dass die Einführung von M365 nicht trivial sondern höchst anspruchsvoll ist. In Graubünden sind die Vorarbeiten abgeschlossen worden und die Regierung hat sich grundsätzlich positiv für die Umsetzung ausgesprochen. Es bleiben aber verschiedene Fragen ungeklärt.

Prüfung Einzelnoten

Es soll ein Portal für die Lehrbetriebe und für die Berufsschule eingeführt werden, woraus die Prüfungseinzelnoten hervorgehen. Im Datenschutzrecht bildet die Einhaltung des Prinzips der Verhältnismässigkeit einen Eckpfeiler des Persönlichkeitsschutzes. In Art. 4 Abs. 2 DSG und in Art. 2 Abs. 1 DSG wird ausdrücklich auf die Anwendung des Grundsatzes hingewiesen. Ob dieses Prinzip eingehalten wird, kann nicht generell bestimmt werden. Es ist in jedem Einzelfall eine Prüfung vorzunehmen. Die Prüfung muss nach objektiven Kriterien erfolgen.

Folgende Kriterien spielen eine Rolle:

1. Die Datenbearbeitung muss für die Erreichung des verfolgten Zweckes geeignet sein.
2. Die Datenbearbeitung muss für die Erreichung des verfolgten Zweckes das mildeste Mittel darstellen und damit erforderlich sein, so dass Daten nur dann und nur insoweit bearbeitet werden dürfen, wenn bzw. wie dies zur Erfüllung des Zwecks objektiv notwendig ist.
3. Schliesslich muss die Datenbearbeitung für die Betroffenen in Anbetracht des Zwecks und der verwendeten Mittel zumutbar sein, so dass zwischen der Datenbearbeitung und dem damit verbundenen Eingriff in die Privatsphäre ein angemessenes Verhältnis bestehen muss.

Im Zusammenhang mit dem Schutz der Persönlichkeit der Lernenden und der Mitteilung der Einzelnoten an die Betriebe und die Berufsschule, wird das Recht auf Schutz der Persönlichkeit höher gewichtet als die Kenntnisnahme der Noten. Denn für die adäquate Begleitung eines Lernenden ist es nicht erforderlich, jederzeit unaufgefordert die Einzelnoten weiterzuleiten, zumal diese Daten noch Änderungen erfahren können. Es ist jedoch möglich, in speziellen Einzelfällen den Lehrbetrieb mit den Einzelnoten zu bedienen. Eine standardmässige Übermittlung wird aber abgelehnt.

Verwaltungsdaten sollen in Zukunft an eine Drittfirma (Microsoft) geliefert und dort gespeichert werden. Damit verliert der Kanton zumindest teilweise die Herrschaft über die eigenen Daten. Allein schon diese Tatsache ist mit einem erhöhten Risiko verbunden. Eine Auslagerung ist nur möglich, wenn die vertraglichen, technischen und organisatorischen Voraussetzungen erfüllt sind.

II. Cloud-Computing

Wie in der Datenschutzabklärung des Amtes für Informatik (AFI) festgehalten wurde, handelt es sich bei M365 grundsätzlich um eine Informations- und Datenauslagerung. Es kann festgehalten werden, dass dies aus datenschutzrechtlicher Sicht grundsätzlich möglich ist. Selbstredend resultieren aus einer Auslagerung von Daten erhöhte Risiken im Bereich Datenschutz. Es muss bei solchen Diensten in technischer Hinsicht eine sichere Übertragung (data in transit) und Speicherung (data in rest) gewährleistet werden. Eine auf dem aktuellen Stand der Technik stehende Verschlüsselung ist

unabdingbar. In diesem Zusammenhang stellt sich immer die Frage, wer im Besitz des Schlüssels sein soll. Idealerweise sollte der Schlüssel beim Datenherr verbleiben. Aus technischer Sicht kann dies nicht in jedem Fall gewährleistet werden. Hinsichtlich der Qualität des Schlüssels wird explizit auf das Merkblatt «Cloudspezifische Risiken und Massnahmen» von privatim verwiesen.[1] Unabhängig von der Definition der Daten darf der Schlüssel nur beim Cloud-Anbieter aufbewahrt werden, wenn sich dieser vertraglich verpflichtet, ihn nur mit ausdrücklicher Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind in jedem Fall zu protokollieren. Es sind Massnahmen zum Schutz des Schlüssels vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung zu treffen.

Im vorgenannten Merkblatt werden die wesentlichen Risikobereiche genannt, welchen ein besonderes Augenmerk gewidmet werden muss, nämlich anwendbares Recht, Orte der Datenbearbeitung und Vertraulichkeit/Geheimnisschutz.

Mit Bezug auf die Vertragsgestaltung konnten durch die Schweizerische Informatikkonferenz (SIK) und privatim wesentliche Verbesserungen erreicht werden. Dabei erscheint wesentlich, dass die Daten in der Schweiz gespeichert werden und Schweizer Recht zur Anwendung kommt. Darüber hinaus muss der Kanton die Einhaltung der vertraglichen Pflichten kontrollieren können. Auf die Vertraulichkeit bzw. dem Geheimnisschutz wurde bereits oben hingewiesen. Gemäss Datenschutzabklärung sollen geheime Daten, aber auch Informationen, welche von den Ämtern als kritisch oder besonders schützenswert in Bezug auf die Risiken eingestuft werden, lokal verarbeitet werden. Die Einstufung der jeweiligen Daten soll den Ämtern überlassen werden. Dieses Vorgehen birgt die Gefahr in sich, dass innerhalb des Kantons nach unterschiedlichen Kriterien Kategorien geschaffen und angewendet werden. Auf Grund der Tatsache, dass einzelne Ämter nicht über die erforderlichen Fachkenntnisse verfügen, drängt sich eine Katalogisierung auf. Zumindest muss den einzelnen Ämtern seitens des AFI eine Richtlinie vorgegeben werden, woraus hervorgeht, gestützt auf welche Kriterien die Einteilung der Daten erfolgen soll. Mit einer solchen Massnahme kann eine «unité de doctrine» erreicht werden.

---

[1] *https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf.*

III. CLOUD Act

a) Allgemeines

Grundsätzlich ist festzuhalten, dass die Vereinigten Staaten von der Liste der vertrauenswürdigen Staaten genommen worden sind. Mithin wurde festgehalten, dass in den USA kein rechtstaatlich berechenbarer Datenschutz und ein schwer kalkulierbares Risiko besteht und die Behörden durch Einflussnahme auf die dort ansässigen Muttergesellschaften den Datenschutz in Europa und der Schweiz übergehen.

b) Verhältnis CLOUD Act und DSG

Datenbearbeitungen gestützt auf den CLOUD Act müssen als heikel qualifiziert werden und zwar mit Bezug auf die Rechtmässigkeit, die Transparenz, die Verhältnismässigkeit und die Zweckgebundenheit.

Mögliche Rechtfertigungsgründe, damit eine Datenbearbeitung nicht als widerrechtliche Persönlichkeitsverletzung gilt, sind die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine durch Gesetz gerechtfertigte Datenbearbeitung. In Bezug auf weitere, aus datenschutz- und grundrechtlicher Sicht wichtige Kernanliegen erweisen sich Datenbearbeitungen gestützt auf Herausgabeanordnungen als problematisch. Wesentlich ins Gewicht fallen hier insbesondere die unter dem CLOUD Act fehlenden Zugangs-, Berichtigungs- und Löschrechte der betroffenen Person, aber auch das Fehlen von Rechtschutzmöglichkeiten sowie von verfahrensrechtlichen Garantien.

Die Regierung des Kantons Zürich bezog sich kürzlich auf die Methode Rosenthal, als sie die Migration von Personendaten auf M365 zuliess. Die Stadt Zürich stützte sich wenig später auf ein Gutachten der Anwaltskanzlei Laux Lawyers. Die Aussagen im Gutachten erstaunen insbesondere hinsichtlich der Anwendung von amerikanischem Recht durch den Geheimdienst. In Anbetracht der Tatsache, dass die Bürgerinnen und Bürger nicht wählen können, wem der Kanton die Daten anvertraut, ist es geboten, nach Alternativen zu suchen. Die Datenschutzbeauftragte des Kantons Zürich postuliert eine Government-Cloud, die von den öffentlichen Institutionen gemeinsam aufgebaut und betrieben wird. Eine andere Lösung könnte auch darin bestehen, ein Unternehmen zwischen den Kanton und Microsoft zu schalten. Entsprechende Produkte werden bereits angeboten.

c) Schlussfolgerungen

Es kann festgestellt werden, dass die Auslagerung von Daten an ein US-amerikanisches Unternehmen grundsätzlich einer grenzüberschreitenden Datenbekanntgabe in die USA gleichkommt, selbst wenn die Daten in der Schweiz gespeichert werden. Bekanntlich weist die USA ein tieferes Datenschutzniveau auf als die Schweiz. Ein hinreichender Schutz der Daten ist deshalb nicht vollumfänglich gewährleistet.

Den datenschutzrechtlichen Unzulänglichkeiten kann nur bedingt begegnet werden. Es kann ein risikobasierter Ansatz gewählt werden. Bei der Beurteilung wird darauf abgestellt, wie hoch die Wahrscheinlichkeit eines behördlichen Zugriffs ist. Diese Wahrscheinlichkeit ist mit Wahrscheinlichkeitswerten zu beziffern. Beim risikobasierten Ansatz geht es allerdings nicht nur um die Gesetzeslage. Entscheidend ist bei diesem Ansatz, ob bzw. mit welcher Wahrscheinlichkeit die ausländischen Behörden die gesetzlichen Zugriffsmöglichkeiten im konkreten Fall anwenden. Diese Beurteilung ist mangels Kenntnisse der konkreten Parameter schwierig, zumal über Recherchen der Geheimdienste keine Publikationen greifbar sind. Eine solche Auslagerung kann bedingt als rechtlich zulässig qualifiziert werden, solange die geschätzte oder berechnete Wahrscheinlichkeit eines Datenzugriffs durch US-Behörden einen als vertretbar erachteten Wert nicht überschreitet. Zweifel an dieser Schlussfolgerung sind indessen nicht von der Hand zu weisen. Der EDÖB hat im Zusammenhang damit auf den Gesetzeswortlaut hingewiesen, wonach sich keine Hinweise finden für einen risikobasierten Ansatz zur Gewährleistung eines angemessenen Schutzes. Immerhin erachtet er einen risikobasierten Ansatz nicht als zwingend ausgeschlossen.[2] Rechtliche Vorbehalte bleiben. Werden also Personendaten mittelbar in die USA ausgelagert, werden potentiell Bestimmungen zum grenzüberschreitenden Datentransfer verletzt. Die Inkaufnahme einer solchen Verletzung und der damit verbundenen Risiken ist schlussendlich eine politische Entscheidung. Es gilt abzuwägen, ob das Risiko einer Verletzung in Kauf genommen werden soll.

---

[2] *EDÖB: Stellungnahme zur Datenschutzrisikobeurteilung der SUVA zum Projekt Digital Workplace «M365».*

Zusammenfassend kann festgestellt werden, dass ein Datentransfer an ein US-amerikanisches Unternehmen aus datenschutzrechtlicher Sicht als problematisch zu qualifizieren ist. Der Entscheid, ob dennoch Daten bei einem US-amerikanischen Unternehmen gespeichert werden, bedarf somit einer intensiven Überprüfung, insbesondere der Wahrscheinlichkeit eines Zugriffs durch US-amerikanischer Behörden. Es ist letztendlich ein politischer Entscheid, der vorzugsweise von der Regierung in Kenntnis der Risiken zu fällen ist.

IV. Abhängigkeiten

Mit der Einführung von M365 begibt sich der Kanton in sehr grosse Abhängigkeit von Microsoft. Folgerichtig muss bereits heute eine Exit-Strategie erarbeitet werden. Abhängigkeiten bergen immer Gefahren in sich, seien diese technischer oder finanzieller Natur. Allein schon aus diesem Grund sind alternative Möglichkeiten zu prüfen und in die Entscheidfindung mit einzubeziehen. Bekanntlich ist die Marktmacht von Microsoft aktuell schon sehr hoch. Mit dem Übergang zu M365 akzentuiert sich die Stellung von Microsoft zusätzlich markant. Monopole schlagen sich mittelfristig im Preis eines Produktes nieder. Vor dem Hintergrund, dass sich eine Vielzahl von Kantonen und der Bund mit denselben Fragen beschäftigt, sollte eine gemeinsame Strategie, welche insbesondere auch den Ausstieg zum Inhalt hat, verfolgt werden. Gewisse Verbesserungen konnten in der Vergangenheit erreicht werden. Diese genügen aber nicht.

V. Zusammenfassung

Die Kardinalfrage beschlägt die Datenbekanntgabe trotz Bestehen des CLOUD Acts. Es ist nicht absehbar, dass die EU oder die Schweiz eine Änderung dieses Gesetzes erreichen kann. Die Anwendbarkeit des CLOUD Acts kann nicht geprüft und abgeschätzt werden. Eine einwandfreie rechtskonforme Lösung erscheint fraglich. Es verbleibt deshalb an den politischen Entscheidträgern zu beurteilen, ob dennoch M365 umfassend eingeführt werden soll.

III. Fälle aus der Praxis

1. Aushändigung von Dokumenten der Exekutive

In einer Gemeinde wandte sich ein Mitglied des Gemeindeparlaments als Privatperson an den Gemeindevorstand und verlangte gewisse Verträge zur Einsicht. Eine Auskunft wurde verweigert. Danach wurde geprüft, welche Daten im Zusammenhang mit der Ausübung der parlamentarischen Rechte weitergegeben werden dürfen.

In einer ersten Phase muss abgeklärt werden, ob das Datenschutzgesetz anwendbar ist. Art. 1 Abs. 4 KDSG verweist betreffend die Ausschlussgründe auf das DSG. Gemäss Art. 2 Abs. 2 lit. b DSG ist das DSG nicht anwendbar auf Beratungen in den Eidgenössischen Räten und in den parlamentarischen Kommissionen. Heruntergebrochen auf die Gemeindeebene kommt das KDSG nicht zur Anwendung für die Beratungen des Gemeindevorstandes und des Gemeinderates. Diese Ausnahme gilt indessen nur, soweit die Parteien im Rahmen der laufenden Beratung für das Parlament tätig sind. Mit dem Begriff Beratungen wird verdeutlicht, dass es um die aktive Phase der parlamentarischen Arbeit geht. Nach Abschluss der Beratungen ist das DSG als auch das KDSG anwendbar (Beat Rudin in: Baeriswyl/Pärli, Stämpflis Handkommentar zum DSG, Art. 2, Note 25). Es kann festgehalten werden, dass für den Parlamentsbetrieb die einschlägigen Bestimmungen für diese Organe massgebend sind. Wird nun eine Motion, ein Postulat oder eine Interpellation im Rahmen der parlamentarischen Tätigkeit eingebracht, handelt es sich um ein aktives Geschäft. Vorab sind folgerichtig die kommunalen gesetzlichen Vorgaben zu konsultieren. Aus diesen lassen sich keine Erkenntnisse über die spezifische Handhabung des Datenschutzes erkennen. Somit ist auf allgemeine Grundsätze abzustellen.

Nutzung von Schülerfotos

Das Recht auf das eigene Bild ist Teil des Rechts auf persönliche Freiheit. Ein Freiheitsrecht kann nur eingeschränkt werden, wenn eine gesetzliche Grundlage besteht oder die betroffene Person dazu einwilligt. Fotos und Videos dürfen daher grundsätzlich nur aufgenommen werden, wenn die oder der Urteilsfähige oder die Eltern damit einverstanden sind. Mit dem Einverständnis muss auch klar sein, wofür die Aufnahmen verwendet werden sollen. Es macht einen Unterschied, ob eine Fotografie in einem Publikationsorgan oder weltweit im Internet veröffentlicht werden soll. Zudem muss die Einwilligung aktiv erfolgen. Eine Formulierung «ohne ihren Widerspruch» genügt nicht.

Ohne Einwilligung dürfen Bilder aufgenommen werden, wenn eine der folgenden Voraussetzungen erfüllt sind:

- Die abgebildete Person fügt sich in die Umgebung ein und ist nicht gezielt im Fokus;
- Bilder mit mehreren Teilnehmenden an einem schulischen Anlass, die fragliche Person ist nicht optisch hervorgehoben und wird als Teil der Menschenansammlun wahrgenommen.

Zu vermeiden ist auf jeden Fall den Namen der auf den Bildern erkennbaren Personen zu nennen. In diesem Fall ist auf alle Fälle das ausdrückliche Einverständnis einzuholen.

In Art. 12 BV wird auf den Schutz der Privatsphäre ausdrücklich hingewiesen. Ausfluss davon sind die einschlägigen Bestimmungen im ZGB (Art. 27 ff. ZGB). Es wird insbesondere darauf hingewiesen, dass Daten ohne Zustimmung oder überwiegender privater oder öffentlicher Interessen nicht bekannt gegeben werden dürfen. Der Gemeindevorstand hat folgerichtig eine Interessenabwägung vorzunehmen. Wenn er der Ansicht ist, dass die privaten Interessen auf Geheimhaltung höher zu gewichten sind als die öffentlichen Interessen auf Bekanntgabe, ist diese Haltung durchaus datenschutzkonform.

Hinzuweisen ist auf die Geschäftsprüfungskommission (GPK). Die GPK besitzt eine umfassende Kontrollkompetenz. Sie kontrolliert beispielsweise die Tätigkeit des Gemeindevorstands und der Verwaltung. Die GPK besitzt ein gesetzliches Einsichtsrecht. Sollte also die GPK die Auffassung vertreten, es bestünde Handlungsbedarf im Zusammenhang mit den erfragten Informationen, kann sie nach Einsicht in die konkreten Daten einen entsprechenden Bericht verfassen. Die Kompetenzen der GPK gehen über diejenigen der Mitglieder des Gemeinderates hinaus.

Zusammenfassend kann festgestellt werden, dass aus datenschutzrechtlichen Überlegungen der Gemeindevorstand befugt ist, einem Auskunftsbegehren einer Parlamentarierin oder eines Parlamentariers nicht vollumfänglich Folge zu leisten. Dieses Gremium kann die privaten Interessen auf Geheimhaltung höher gewichten als das öffentliche Interesse auf Bekanntgabe.

2. Einsicht in das Stimmregister

Ein Bürger fragt an, ob eine Partei Einsicht in das Stimmregister nehmen darf.

Art. 5 Abs. 2 des Gesetzes über politische Rechte (GPR) besagt, dass das Stimmregister den Stimmberechtigten zur Einsicht offensteht. Art. 32 des Gesetzes über die Einwohnerregister und weitere Personen- und Objektregister (ERG) demgegenüber erlaubt es den Gemeinden, auf Anfrage Auskunft über Name, Jahrgang und Adresse einzelner Personen, die im Einwohnerregister geführt werden, zu geben. Werden diese Daten ausschliesslich für ideelle Zwecke verwendet und nicht an Dritte weitergegeben, so können sie listenmässig bekanntgegeben werden (Art. 32 Abs. 1 ERG). Weitere Daten über einzelne im Einwohnerregister geführte Personen kann die Gemeinde mitteilen, wenn ein berechtigtes Interesse glaubhaft gemacht wird (Art. 32 Abs. 2 ERG). Die systematische Weitergabe von Daten zu wirtschaftlichen Werbezwecken ist verboten. Die Gemeinde regelt die Einzelheiten der Datenbearbeitung insbesondere bezüglich der Datenverwendung, der Zugriffsberechtigung, des Berichtigungsverfahrens, der Aufbewahrungsdauer und Löschung der Daten, der Datenweitergabe und des Auskunftsrechtes (Art. 32 Abs. 6 ERG).

Ein Vergleich dieser beiden Bestimmungen (Art. 5 Abs. 2 GPR und Art. 32 ERG) legt den Schluss nahe, dass das Stimmregister nicht die gleiche «Öffentlichkeit» geniesst wie das Einwohnerregister und damit Zurückhaltung bei Anfragen geboten ist, respektive eine solche negativ zu beantworten ist. In Literatur und Rechtsprechung konnte nichts Konkretes zu Art. 5 Abs. 3 GPR gefunden werden. Doch legt bereits eine grammatikalische Auslegung der Gesetzesbestimmung den Schluss nahe, dass das Stimmregister nicht für Sammelanfragen von Parteien zugänglich sein soll, sondern eben nur für die jeweils Stimmberechtigten öffentlich ist. Einzelne Stimmberechtigte können dabei im Rahmen von spezifischen Anfragen Auskunft darüber verlangen, ob sie selber im Stimmregister geführt werden oder ob eine andere Person stimmberechtigt oder wählbar ist. Diese Folgerung wird durch ein Urteil des Verwaltungsgerichtes des Kantons Zug vom 30. März 2016, Ziffer 4a ff. (GVB 2016 Seite 98) bestätigt.

Alternativ könnte eine Sammelanfrage mittels einer Auskunft über das Einwohnerregister geprüft werden. Das Verwaltungsgericht Zug hat sich mit diesen – nicht einfachen – Fragen im Urteil ausführlich auseinandergesetzt. Hinzuweisen betreffend das Thema Sammelanfragen von Parteien ist auf den Tätigkeitsbericht 2015 Seite 17.

3. Externe Meldestelle für Meldung von Missständen

Im Gesetz über das Arbeitsverhältnis der Mitarbeitenden des Kantons Graubünden (Personalgesetz, PG) ist neu ein Art. 47a eingeführt worden. Danach können Mitarbeitende in gutem Glauben und guten Treuen Missstände anonym einer Meldestelle melden. Die Regierung bezeichnet eine Meldestelle ausserhalb der Verwaltungsorganisation, welche die Aufgaben nach dieser Bestimmung fachlich kompetent, selbstständig, unabhängig und weisungsungebunden sowie unter Wahrung des Datenschutzes und der Geheimhaltung erfüllt. Es kann somit festgestellt werden, dass für die Errichtung einer Meldestelle ausserhalb der kantonalen Verwaltung eine gesetzliche Grundlage besteht.

Der Kanton möchte mit zwei Treuhandunternehmen, welche einerseits die Missstände, andererseits die Persönlichkeitsverletzungen bearbeiten, einen Vertrag abschliessen, wobei die technische Übermittlung lediglich über eine Gesellschaft läuft. In Anbetracht der Tatsache, dass vornehmlich besonders schützenswerte Personendaten übermittelt werden, ist eine Schutzbedarfsanalyse gemäss der Weisung «IKT-Sicherheit in der kantonalen Veraltung» durchzuführen.

Die Vertragsentwürfe wurden dem DSB zur Prüfung vorgelegt. Dabei ist aufgefallen, dass die allgemeinen Vertragsbestimmungen (AGB) nicht auf das konkrete Vertragsverhältnis mit dem Kanton Graubünden abgestimmt worden sind. Für die Meldestelle gilt das kantonale Datenschutzgesetz, da sie eine kantonale öffentliche Aufgabe übernimmt. Ein in den AGB aufgenommener Bezug auf europäisches Recht ist irrelevant. Es genügt durchaus, wenn die Erklärung Bezug auf das KDSG als auch das DSG und seine Verordnungen nimmt. Da die zu beauftragenden Unternehmen international tätig sind, findet sich eine Vielzahl von Bestimmungen, die sich auf internationale Sachverhalte beziehen. Diese Bestimmungen sind zu streichen. Es muss ohnehin ein Anliegen des Kantons sein, dass keine Daten an Dritte weitergegeben werden, geschweige denn ins Ausland. Die Bestimmung, wonach eine allgemeine Genehmigung für den Beizug von Auftragsarbeit erteilt wird, ist insofern zu ändern, wonach Dritte nur mit ausdrücklicher Zustimmung

Aktenversand

Es bestehen keine gesetzlichen Vorgaben, dass Unterlagen mit einem bestimmten Inhalt per Einschreiben versendet werden müssen. Grundsätzlich verantwortlich für den sicheren Transport der Unterlagen an die Betroffenen ist das jeweilige Amt. Ein eingeschriebenes Paket oder ein eingeschriebener Brief dient lediglich der Beweisbarkeit. Eine eingeschriebene Sendung wird grundsätzlich gleichbehandelt wie eine normale Postsendung. Der Unterschied besteht darin, dass eine eingeschriebene Sendung bereits am nächsten Werktag zugestellt wird, eine elektronische Sendungsverfolgung möglich ist und die Auslieferung nur gegen Unterschrift erfolgt. Insofern ist die Übermittlung per Einschreiben sicherer. Es liegt jedoch im Entscheidungsbereich des Amtes über die Art und Weise des Versands zu entscheiden. Der Datenschutzbeauftragte kann einem Amt nicht vorschreiben, bestimmte Korrespondenzen per Einschreiben vor-zunehmen, obwohl es durchaus verständlich erscheint, dass sensible Daten möglichst sicher übermittelt werden.

des Kantons Graubünden beigezogen werden dürfen. Bei Beendigung des Auftragsverhältnisses ist lediglich eine Sperrung der Verarbeitung vorgesehen. In diesem Fall sind die Daten zu löschen bzw. zu retournieren, sofern keine gesetzlichen Aufbewahrungsfristen dagegensprechen. Auch unter dieser Prämisse sollte es möglich sein, die bearbeiteten Falldokumente zurückzuerstatten. Zumindest müssten die Dokumentenkategorien konkret bezeichnet werden, welche von Gesetzes wegen beim Unternehmen zu verbleiben haben.

AGB's haben sicher ihre Berechtigung. Mit Bezug auf die konkrete Umsetzung sind sie in der Regel wenig hilfreich, sofern ein Unternehmen ein breites Betätigungsfeld abdeckt. Vielmehr sollen individuelle Bestimmungen die Zusammenarbeit regeln. Dadurch ist Gewähr geboten, dass bei üblichen Fragen sich Antworten aus dem Vertragstext ergeben, im Wissen, dass auch bei umfassenden Formulierungen Konflikte nicht vermieden werden können.

4. ICD-10 Code

Ein Spital fragt an, in welcher Form der ICD-Code (Diagnosecode) an Versicherer weitergegeben werden darf.

Eine Rückfrage bei anderen Kantonen hat ergeben, dass die Übermittlung von ICD-Codes unterschiedlich gehandhabt wird. Massgebend ist grundsätzlich Art. 42 Abs. 3 KVG, wonach der Leistungserbringer verpflichtet ist, eine detaillierte und verständliche Rechnung auszustellen und alle Angaben weiterzugeben, die erforderlich sind, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung zu überprüfen. Bereits im Jahre 2001 befasste sich der Bundesrat mit dem ICD-Code. Auf eine Interpellation hin antworte er unter anderem wie folgt: «Das im Datenschutzgesetz verankerte Verhältnismässigkeitsprinzip verbietet indes, mehr als die tatsächlich erforderlichen Personendaten zusammenzutragen, insbesondere bei besonders schützenswerten Daten. Somit bedeutet Art. 42 KVG, dass ein Versicherer lediglich verlangen darf, dass auf den Arztrechnungen eine allgemeine, zur Bearbeitung gewöhnlicher Fälle erforderliche Diagnose anzugeben ist. Sollte dies nicht ausreichen, so kann er nachträglich – gegebenenfalls über einen Vertrauensarzt – eine genauere Diagnose einfordern. Es wäre unverhältnismässig die Leistungserbringer zu verpflichten, auf den Arztrechnungen systematisch einen Diagnosecode aufzuführen, der detaillierte Angaben zum Gesundheitszustand der versicherten Person erteilt.»

Der DSB des Kantons Zürich hält in seinem Tätigkeitsbericht 2004 fest: «Die Weisung aus dem Jahre 1997 sieht vor, dass der zweistellige ICD-10-Diagnosecode den Versicherer bekannt gegeben wird. Auch damals war diese Regelung nur im Sinne einer Übergangslösung gedacht, fand aber nie eine verbindliche Regelung auf gesamtschweizerischer Ebene.»

Im Zusammenhang mit der Einführung von SwissDRG hat sich privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, im Jahre 2011 mit der Thematik befasst. Privatim hielt in einem Positionspapier fest: «Weitere medizinische Daten sind für die Vergütung nach Fallpauschalen in der Regel nicht notwendig. Somit ist die systematische Weitergabe von detaillierten Haupt- und Nebendiagnosen (Codierung nach ICD-10) sowie Prozeduren bzw. Eingriffscodes (Codierung nach CHOB) nicht verhältnismässig.» Im gleichen Jahr äussert sich der EDÖB dahingehend, dass eine systematische Übermittlung von Diagnose- und Prozeduren-Codes im Rahmen der Rechnungsstellung nur erfolgen könne, wenn der Grundsatz der Verhältnismässigkeit strengstens eingehalten werde. Er regte an, eine einheitliche Lösung für die ganze Schweiz

anzustreben. Es dürfe nicht sein, dass die Daten der Patientinnen und Patienten je nach Kanton anders behandelt werden.

Bis heute hat sich an der Ausgangslage grundsätzlich nichts geändert. Eine einheitliche Lösung fehlt weiterhin. Die Bekanntgabe lediglich des zweistelligen ICD-10-Codes ist buchstäblich erodiert. In Anbetracht der Tatsache, dass in verschiedenen Kantonen bereits der vierstellige ICD-10-Code übermittelt wird und vor dem Hintergrund der einheitlichen Anwendung der ICD-10-Codes kann ein Beharren auf den zweistelligen Codes in der Praxis nicht mehr durchgesetzt werden. Wenn nun im konkreten Einzelfall der vierstellige Code verlangt wird, soll dieser ausschliesslich über den vertrauensärztlichen Dienst zugestellt werden.

Vorgehen bei delinquentem Verhalten von Heimbewohnern

Zwischen Betreuungspersonen und betreuten Personen besteht ein Vertrauensverhältnis. Beim Verdacht auf eine strafbare Handlung durch Heimbewohner oder -bewohnerinnen besteht grundsätzlich ein Anzeigerecht und keine Anzeigepflicht. Im Rahmen einer Interessenabwägung ist somit abzuklären, ob in einem konkreten Einzelfall eine Anzeige erfolgen soll. Gemäss Art. 301 StPO ist jede Person berechtigt, Straftaten bei einer Strafverfolgungsbehörde schriftlich oder mündlich anzuzeigen. Art. 26 Abs. 2 EGzStPO hält fest, dass Mitarbeitende einer Behörde zur Anzeige berechtigt sind, wenn sie in ihrer amtlichen Tätigkeit Kenntnis von einer von Amtes wegen zu verfolgenden strafbaren Handlung Kenntnis erhalten.

Es ist zu unterscheiden zwischen Antrags- und Offizialdelikten. Bei Antragsdelikten wird in der Regel keine Anzeige erstattet, währenddessen es bei Offizialdelikten eher umgekehrt ist. Selbst bei Offizialdelikten resultiert daraus nicht zwingend eine Anzeigepflicht. Zielführend wird es sein, wenn intern ein Katalog für Delikte festgelegt wird, die in der Regel nicht angezeigt werden und für Delikte die zu einer Anzeige führen. Indessen soll immer im Einzelfall unter Berücksichtigung der besonderen Umstände entschieden werden.

Schliesslich ist zwischen dem KVG- und dem Unfallbereich zu unterscheiden. Im Bereich UVG kommt die Untersuchungsmaxime zur Anwendung. Der Versicherer hat Anspruch auf eine umfassende Information. Anders hingegen bei privaten Unfallversicherungen, für welche das VVG zur Anwendung gelangt. In diesem Bereich bedarf es einer Zustimmung der versicherten Person. Folgerichtig ist in solchen Fällen die Zustimmungserklärung für die Weiterleitung der Gesundheitsdaten an den Versicherer erforderlich. In Notfällen kann die Einverständniserklärung im Nachgang eingeholt werden.

5. Art. 63a EGzZGB, Kindesschutzmassnahmen

Art. 63a Abs. 4 EGzZGB lautet: «Die Inhaber der elterlichen Sorge beteiligen sich an den Kosten von Kindesschutzmassnahmen im Umfang des von der Schweizerischen Konferenz für Sozialhilfe definierten Elternbeitrags, mindestens aber mit CHF 10.00 pro Tag. Sind sie dazu wirtschaftlich nicht in der Lage, kommt das Gemeinwesen für den Elternbeitrag auf, welches für die öffentlich-rechtliche Unterstützung der Inhaber der elterlichen Sorge zuständig ist.» Insofern stellt sich die Frage, in welchem Fall eine Mitteilung an die Gemeinde betreffend Kindesschutzmassnahmen zu erfolgen hat. Massgebend für die Umsetzung der vorgenannten Bestimmung ist der Bundesgerichtsentscheid 8C_25/2018 und der Entscheid des Kantonsgerichtes Graubünden vom 21. November 2021 (ZK1 21 27). Das Bundesgericht hält fest, dass bei der Umsetzung von Massnahmen das Kindswohl an erster Stelle kommt. Kindsschutz soll rasch, nachhaltig und fachlich korrekt, mit minimalem Eingriff in Elternrechte und Familienstrukturen erfolgen. Administrative Massnahmen dürfen das Kindswohl nicht gefährden. Im konkreten Fall führte die von der Sozialbehörde verursachte Verzögerung von mehreren Monaten letztlich dazu, dass den betroffenen Kindern die notwendige Betreuung in einem Hort nicht zu kamen. Mithin stellte das Gericht fest, dass eine administrative Massnahme die rasche Umsetzung der bundesrechtlich angeordneten KESB-Massnahmen nicht verhindern oder über Gebühr verzögern darf. Gestützt auf das Urteil des Bundesgerichtes hielt das Kantonsgericht in seinem Entscheid fest: «Nach der neusten bundesgerichtlichen Rechtsprechung ist es nicht mehr zulässig, unabhängig von den finanziellen Verhältnissen die Massnahmekosten vorerst dem Inhaber der elterlichen Sorge zu überbinden. Vielmehr ist es das Gemeinwesen – entgegen der bisherigen Praxis des Kantonsgerichtes – gehalten, die Massnahmekosten vorerst zu übernehmen, um deren zügige und effiziente Umsetzung sicherzustellen.»

Das Kantonsgericht hält somit fest, dass nicht unabhängig von den finanziellen Verhältnissen die Massnahmekosten vorerst dem Inhaber der elterlichen Sorge überbunden werden dürfen. Folgerichtig kann jedoch bei Kenntnis der finanziellen Verhältnisse sehr wohl eine Überbindung erfolgen. Ist also ein Elternteil in der Lage für die Massnahmekosten aufzukommen, kann die KESB diese Kosten bei den Inhabern der elterlichen Sorge einfordern. Dieses Vorgehen darf nur nicht dazu führen, dass eine adäquate Massnahme der KESB nicht durchgeführt werden kann, da – wie bereits ausgeführt – das Kindswohl immer im Vordergrund stehen muss. Die KESB kann also bei ordentlichen finanziellen Verhältnissen bei den Inhabern der elterlichen Sorge die Kostenbeteiligung einfordern. Wenn sich jedoch die Betroffenen dagegen wehren bzw. sich dagegen aussprech-

en, ist unverzüglich die Bevorschussung beim Gemeinwesen zu verlangen. Dieses Vorgehen deckt sich mit der Formulierung in Art. 63a Abs. 4 EGzZGB, wonach das Gemeinwesen für den Elternbeitrag aufkommt, wenn die Inhaber der elterlichen Sorge dazu nicht in der Lage sind.

Das Bundesgericht hat das Kindswohl als verfassungsrechtlich geschütztes und grundlegendes Grundrecht erklärt. Wenn durch einfache Massnahmen ein Datenfluss zwischen KESB und Gemeinde verhindert werden kann, kann dieses Vorgehen durchaus dem Kindswohl dienen. Gerade in kleinen Gemeinden ist die Gefahr der unberechtigten Weitergabe von Daten der KESB latent vorhanden und dadurch können nicht nur die Persönlichkeitsrechte der Inhaber der elterlichen Sorge, sondern auch diejenigen der Kinder (und damit das Kindswohl) betroffen sein. Es sind deshalb alle Massnahmen vorzukehren, welche die Verbreitung von Daten der KESB einschränken. Kommt hinzu, dass Daten der KESB als Massnahmen der sozialen Hilfe im Sinne von Art. 3 lit. c Ziff. 3 DSG als besonders schützenswerte Personendaten qualifiziert werden. Diese sensiblen Daten sind entsprechend zu behandeln.

In Anwendung der datenschutzrechtlichen Vorgaben und auch der bundesgerichtlichen Rechtsprechung ist es nicht zu beanstanden, wenn in unproblematischen Fällen die Kostenbeteiligung vorerst bei den Inhabern der elterlichen Sorge eingefordert wird. Dieses Vorgehen darf aber in keinem Fall zu einer Verzögerung der eingeleiteten Massnahmen führen. Wenn sich also ein Elternteil bereit erklärt, für die Kosten aufzukommen, muss das Gemeinwesen nicht eingeschaltet werden. Lösungsorientiert können jeweils die errechneten Kosten bei den Inhabern der elterlichen Sorge angefordert werden mit dem Hinweis, dass im Bestreitungsfalle der Beitrag über das Gemeinwesen bevorschusst wird.

6. Herausgabe von Daten

Eine Person verlangt bei einer sozial tätigen Stiftung (Kinderheim) die Herausgabe ihrer Akten aus den Jahren 1984 – 1992. Die Stiftung teilte mit, dass die Daten vernichtet worden seien.

Es stellt sich die Frage, wie lange Personalakten bzw. Akten über Bewohner und Bewohnerinnen aufbewahrt werden müssen. Üblicherweise werden Akten im privaten Bereich nach 10 Jahren entsorgt und vernichtet. Dies hängt mit gesetzlichen Verjährungsfristen zusammen. Während dieser Phase von 10 Jahren haben die Betroffenen die Möglichkeit, ihre Akten einzusehen und sich aushändigen zu lassen. Es besteht jedoch keine Verpflichtung einer Institution, die betroffene Person anzufragen, ob deren Daten vernichtet werden dürfen. Es ist deshalb nicht zu beanstanden, wenn die Stiftung nach Ablauf der Verjährungsfrist ihre Akten entsorgt und vernichtet.

In der Anfrage wurde das Staatsarchiv erwähnt. Die Aufgaben des Staatsarchivs des Kantons Graubünden sind im kantonalen Gesetz über die Aktenführung und Archivierung sowie der dazugehörigen Verordnung legiferiert (GAA). In diesem Gesetz werden die Aktenführung und Archivierung von Unterlagen durch Behörden geregelt. Darunter fallen auch Stiftungen. Gemäss Art. 6 GAA bieten diese Institutionen nach Ablauf der Aufbewahrungsfrist die Unterlagen dem Archiv an. Das Archiv übernimmt archivwürdige Unterlagen. Verantwortlich dafür ist das Staatsarchiv. Für dieses Archivgut bestehen Schutzfristen (vgl. Art. 10 GAA). Die Schutzfrist beträgt ordentlicherweise 30 Jahre und bei Archivgut mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen 50 Jahre. Sie beginnt mit Abschluss eines Geschäftes zu laufen. Gemäss Art. 11 GAA haben Personen einen Anspruch auf Zugang zu dem sie betreffenden Archivgut. Wenn also im Staatsarchiv Graubünden Unterlagen über eine Person archiviert werden, können diese durch dieselbe eingesehen werden.

Alle Unterlagen, deren Aufbewahrungsfrist abgelaufen ist und die nicht archivwürdig sind, werden nach 10 Jahren nach Abschluss des Falles endgültig vernichtet. Es ist also durchaus möglich, dass die verlangten Akten aus dem Jahre 1984 – 1992 nicht mehr vorhanden sind. Die Stiftung war berechtigt, diese Akten zu vernichten.

IV. Statistik

Wer \ Was	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung	2						1	
DVS	3							
DJSG	14		1		5			
EKUD	2		1					
DFG	2		3					
DIEM	1							
öff. rechtliche Anstalten	6		2		1			
Gerichte								
Regionen	1							
Gemeindeverbände								
Gemeinden	23		1					
Bürgergemeinden								
Juristische Personen	6							
Private Personen	42		2					
Andere	1		1			4	3	4
Total	103	0	11	0	6	4	4	4

VI. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
AFI	Kantonales Amt für Informatik
AGB	Allgemeine Geschäftsbedingungen
AI	artificial intelligence
a.M.	anderer Meinung
Art.	Artikel
B	Botschaft
BBl	Bundesblatt
BG	Bundesgesetz
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
Bl	Blatt
BR	Bündner Rechtsbuch
BV	Bundesverfassung
bzw.	beziehungsweise
DIEM	Departement für Infrastruktur, Energie und Mobilität
DFG	Departement für Finanzen und Gemeinden
DJSG	Departement für Justiz, Sicherheit und Gesundheit
DSB	Datenschutzbeauftragter
DSG	Bundesgesetz über den Datenschutz
DVS	Departement für Volkswirtschaft und Soziales
EDOEB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EGzStPO	Einführungsgesetz zur Strafprozessordnung
EGzZGB	Einführungsgesetz zum Zivilgesetzbuch
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister
etc.	et cetera
f./ff.	folgend/folgende
GAA	Gesetz über die Aktenführung und Archivierung
GPK	Geschäftsprüfungskommission
GPR	Gesetz über die politischen Rechte
GR	Graubünden
Hrsg.	Herausgeber
ICD-Code	Diagnosecode (International Statistical Classification of Diseases and Related Health Problems)
i.V.m.	in Verbindung mit
KDSG	Kantonales Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde
KI	Künstliche Intelligenz
KV	Kantonsverfassung
lit.	litera
N	Note
OR	Obligationenrecht
PG	Personalgesetz
RB	Rechtsbuch
Rz	Randziffer
S	Seite
SIK	Schweizerische Informatikkonferenz
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
u.a.	unter anderem
usw.	und so weiter
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
vgl.	vergleiche
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch
Ziff.	Ziffer