Tätigkeitsbericht der Datenschutzstelle des Kantons Uri für die Zeit vom 01.01.2015 bis 31.12.2019

Die beauftragte Person für Datenschutz ist kantonales Kontrollorgan gemäss dem Bundesgesetz über den Datenschutz. In diesem Sinne nimmt sie neben anderen auch Aufgaben wahr wie die Überwachung der Anwendung der Vorschriften über den Datenschutz, Beratung von Behörden bei der Anwendung von Datenschutzvorschriften, Beratung von Privaten und allfällige Vermittlung zwischen Behörden und Privaten; Stellungnahmen zu Erlassen und zu Massnahmen, die sich datenschutzrechtlich als relevant erweisen können. Gemäss Art. 22 Abs. 2 lit. f Datenschutzgesetz[1] bildet der Landrat das behördliche und fachliche Aufsichtsorgan über die beauftragte Person im Bereich des kantonalen Datenschutzes.

I

Datenschutz, verstanden als Grundrecht der persönlichen Freiheit im Sinne von Art. 10 Abs. 2 u. Art. 13 Abs. 2 Bundesverfassung.

Bereits zur Zeit der Renaissance im 15. Und 16. Jahrhundert begann sich das Verständnis zu entwickeln, trotz vielerorts einer völlig anderen gesellschaftlichen Wirklichkeit, dass jedem Menschen, unbesehen seines Alters, gesellschaftlichen Standes, der Zugehörigkeit zu einer Ethnie oder einem Staat oder der gesundheitlichen Befindlichkeit eine unveräusserliche Würde zukommt. Unter anderem wurzelt diese abendländische Denktradition auch im Werk von Giovanni Pico della Mirandola, 1463 -1494[2], einem Repräsentanten der italienischen Renaissance, in der auch Strömungen wie die antike Stoa eine Neubelebung erfuhren und so in dieses neue Denken einflossen. In der später folgenden Epoche der Aufklärung fanden sich Denker wie Moses Mendelssohn oder Immanuel Kant, die für die Überzeugung standen, dass jedem Menschen ein je eigener Wert, ein je eigener Zweck zukommt, über den niemand, weder Private noch übergeordnete staatliche Autoritäten eigenmächtig bestimmen dürfen. Dieses Denken, das in einer der Formulierungen des berühmten kategorischen Imperativs durch Immanuel Kant in seiner philosophischen Ethik

[1] DSG UR; RB 2.2511

[2] Giovanni Pico della Mirandola, De hominis dignitate, (Über die Würde des Menschen), übersetzt u. herausgegeben von A. Buck, Meiner, Hamburg 1990

zum Ausdruck kam, hat folgenden Wortlaut gefunden: «Handle so, dass du die Menschheit, sowohl in deiner Person, als in der Person eines jeden anderen, jederzeit zugleich als Zweck an sich, niemals bloss als Mittel brauchest.»[3]. Diese kantische Maxime, aber auch allgemein die Denkrichtungen der Aufklärung des 18. Jahrhunderts, formten mit der Zeit ein neues Denken, das sich direkt auf die nachfolgende Ausgestaltung von Rechtsphilosophie und Rechtstheorie im abendländischen Raum auszuwirken begann. Es entstanden in der Folge auf je nationaler, später auch auf internationaler Ebene, die grossen Rechtssysteme, welche die Rechtsunterworfenen nicht bloss als funktionale Adressaten von Normen, als verfügbare Objekte betrachteten, sondern vielmehr ebenso als Rechtssubjekte, denen Grund- und Freiheitsrechte zukamen. Dieses Denken floss dann auch in die Schweizerische Bundesverfassung ein und fand seinen rechtlichen Ausdruck in den Grund- und Freiheitsrechten der Menschen. Art. 13 Abs. 2 BV[4] bildet ein derartiges Grundrecht, welches garantieren will, dass von Seiten von Privaten, aber auch seitens staatlicher Organe über Informationen, bezogen auf Personen, grundsätzlich nur so weit verfügt werden darf, als ein wichtiges öffentliches oder allenfalls privates Interesse dies verlangt. Dies in der Erkenntnis, dass die Verfügbarkeit über Daten, insbesondere über Personendaten, immer auch ein Stück weit eine grosse Machtakkumulation bedeuten und die persönliche Integrität eines Menschen tief eingreifen kann. Solche Überlegungen bilden die ratio legis, dass dieses durch die Verfassung gegenüber jeder Person eingeräumte Grundrecht ermöglichen soll, über die je eigenen Personendaten und Informationen so weit als möglich selber verfügen und entscheiden zu können. Bilden doch Informationen über die je eigene Person einen zentralen Bestandteil auch der persönlichen Integrität und Freiheit.

II

Strukturelle Ausgestaltung des Datenschutzes

Für Uri findet sich die wichtigste Quelle des formellen Datenschutzrechtes im kantonalen Datenschutzgesetz (DSG UR)[5]. Weitere kantonale Rechtsquellen, in welchem der Datenschutzstelle ebenfalls gewisse Funktionen zugewiesen wurden, sind das Gesetz über das Öffentlichkeitsprinzip der kantonalen

[3] Immanuel Kant, Grundlegung zur Metaphysik der Sitten, BA 67 (WB Darmstadt 1983, Kant Werke Bd. 6, S.61).
[4] SR 101
[5] RB 2.2511

Verwaltung (OeG)[6] sowie die Videoverordnung[7]. Das formelle Datenschutzrecht des Bundes ist im eidgenössischen Datenschutzgesetz[8] und in der das Gesetz konkretisierenden Verordnung (VDSG)[9] verankert. International ist die Schweiz an einen Erlass des Europarates, dessen Mitglied die Schweiz ist, gebunden, d.h. an das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (E-Konv108)[10] und deren Zusatzprotokoll[11]. Das Übereinkommen ist vor relativ kurzer Zeit in revidierter Ausgestaltung am 17./18. Mai 2018 durch den Europarat (Ministerkomitee) neu verabschiedet worden. Ebenfalls wurde im ai 2018 durch das Ministerkomitee die Ratifizierung eröffnet. Das revidierte Übereinkommen tritt in Kraft, sofern es durch mindestens 5 Vertragsstaaten genehmigt, angenommen und ratifiziert worden ist. Dies ist der Grund, dass derzeit auf der offiziellen Website des Europarates noch die in Kraft stehende Fassung aus dem Jahre 1981 zu sehen ist. Es ist davon auszugehen, dass das Parlament das neue Vertragswerk genehmigt und annimmt und die Schweiz diesen neuen revidierten Rechtserlass ratifizieren wird.

Ebenso entfaltet die Richtlinie (EU) 2016/680[12] des europäischen Parlaments und des Rates direkte Rechtskraft für die Schweiz. (Ausgeschriebene Bezeichnung: «Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Ermittlung, Verhütung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977 JI des Rates»).

Hingegen entfaltet die Datenschutzgrundverordnung (EU) 2016/679 (DSGVO)[13], welche ebenfalls in revidierter Form in Kraft getreten ist, gegenüber der öffentlichen Hand in der Regel keine direkte Rechtswirkung. Sie ist von allfälliger Relevanz für private Unternehmen oder auch Behörden, sofern ein Unternehmen oder eine Behörde oder eine Unternehmung im EU-Raum über eine feste Niederlassung verfügt, oder wenn eine Behörde oder ein Unternehmen Personen, welche im EU-Raum leben, Waren oder Dienstleistungen anbietet oder falls Personen, die im EU-Raum leben, eine

[6] RB 2.2711
[7] RB 3.8115
[8] SR 235.1
[9] SR 235.11
[10] SEV Nr. 108 (Europarat, Sammlung Europäischer Verträge – Nr. 108, Strassburg, 28.01.1981); SR 0.235.1
[11] SEV Nr. 181; SR 0.235.11
[12] ABl (EU) L 119 vom 04.05.2016, S. 89 – 131; SR 235.3
[13] ABl (EU) L 119 vom 04.05.2016, S. 1 – 88 (Verordnung (EU) vom 04.05.2016 / 679)

Internetseite einer Behörde oder eines Unternehmens besuchen und daher via Analyse-Tools deren Verhalten beobachtet werden, soweit dieses Verhalten sich im EU-Raum ereignet[14]. Wäre eine dieser drei Konstellationen gegeben, würde die DSGVO unter dem Titel «räumlicher Anwendungsbereich» auch für die öffentliche Hand direkte Rechtswirkung entfalten. Hingegen ist eine indirekte Rechtswirkung nicht gänzlich von der Hand zu weisen, sind sowohl in der DSGVO als auch in den RL 2016/680, aber auch in der E-Konv108+ doch über weiteste Strecken ähnliche datenschutzrechtliche Grundsätze verarbeitet, sorgen so für ein einheitliches Datenschutzniveau und streben einen angeglichenen Standard im gesamten EU-Raum und im Raum der Vertragsstaaten des Europarates an.

Die obgenannten Rechtsquellen betreffen das formelle Datenschutzrecht, wo die wichtigsten Grundsätze festgelegt sind. Das eigentliche materielle Datenschutzrecht ist über die gesamte Sachgesetzgebung verstreut. Dort ist festgelegt, welches die gesetzlichen Aufgaben sind, die den öffentlichen Organen und allenfalls Privaten zugewiesen wurden. Nur im Zusammenhang mit Aufgabenkatalog der öffentlichen Organe kann entschieden werden, auf welche Art die formellen datenschutzrechtlichen Grundsätze Anwendung finden.

Die kantonalen Datenschutzgesetzgebungen beschlagen datenschutzrechtlich einerseits relevante Rechtsverhältnisse, die zwischen der öffentlichen Hand (Kanton, Gemeinden, öffentlich-rechtliche Körperschaften und Anstalten, Privatpersonen, die mit öffentliche Aufgaben betraut wurden) und Privatpersonen herrschen, und anderseits Rechtverhältnisse, die öffentliche Organe untereinander, also verschiedene Behörden mit verschiedenen öffentlichen Aufgaben betreffen. Das Bundesdatenschutzrecht findet seinerseits Anwendung und die Zuständigkeit der Bundesdatenschutzstelle (EDÖB) ist gegeben soweit durch Bundesorgane, aber auch durch Privatpersonen Personendaten bearbeitet werden. In Bezug auf das Bearbeiten von Personendaten durch Privatpersonen, ohne dass sie eine öffentliche Aufgabe erfüllen, finden die kantonalen Datenschutzgesetzgebungen keine Anwendung.

[14] Verordnung (EU) 2016/679, Art. 3

III

Entwicklungen im Datenschutzrecht

Wie oben bereits erwähnt, ist aufgrund europäischer Vorgaben auch das Schweizerisches Datenschutzrecht und somit auch das Urner Datenschutzgesetz einer Revision zu unterziehen.

Der Europarat hat am 18. Mai 2018 die Revision seiner Datenschutzrechtskonvention, genannt «Konvention 108» (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten), die aus dem Jahre 1981 stammt und welche durch die Schweiz 1997 ratifiziert wurde[15],verabschiedet. Ziel der aktualisierten Konvention ist es, einen starken Rechtsrahmen gegen Missbrauch zu schaffen, gleichzeitig jedoch auch den grenzüberschreitenden Datenverkehr mit greifenden Schutzmechanismen zu sichern. Die durchgeführte Revision hält an den Bestimmungen, bezogen auf zentrale Datenschutzgrundsätze, fest. Die Revision führte jedoch relevante Neuerungen ein wie die Verpflichtung, Datenschutzverstösse durch öffentliche Organe als meldepflichtig zu erklären, eine Stärkung des Verhältnismässigkeitsprinzips bei der Datenbearbeitung gerade auch im Hinblick auf eine ausdrückliche, spezifizierte und legitime Zweckbestimmung, die Verankerung des Grundsatzes der Datenminimierung, eine Verstärkung der Rechenschaftspflicht der für die Datenbearbeitung Verantwortlichen, sowie eine Stärkung der Transparenz der Personendatenbearbeitung, um das Vertrauen in das digitale Umfeld möglichst zu erhalten sowie eine Stärkung der Kompetenzen der Aufsichtsbehörden. Aus datenschutzrechtlicher Sicht ist zu hoffen, dass das Bundesparlament die Revision dieser internationalen Datenschutzkonvention zu gegebenem Zeitpunkt im Hinblick auf eine allfällige Ratifizierung. Vorbehalte können anlässlich einer Ratifikation keine angebracht werden[16] .

Mit dem Inkrafttreten der DSGVO (Verordnung EU 2016/679) und den RL (EU) 2016/680[17] sind zwei wichtige Grundpfeiler des EU-Datenschutzrechts in Kraft getreten. Wie oben bereits erwähnt wirken sich die RL (EU) 2016/680 («Richtlinien des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und

[15] SR 0.235.1

[16] Art. 29 Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (konsolidierte Abfassung der Revision vom 18.05.2018)

[17] ABl (EU) L 119, 89ff. vom 04.05.2016

zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates») auch in der CH mit unmittelbarer Verbindlichkeit für die zuständigen öffentlichen Organe aus, welche im Bereich der Strafverfolgung, des Strafvollzuges und der Prävention in diesem Bereich tätig sind.

Ziel dieser Richtlinien bildet der Schutz der Grundrechte natürlicher Personen, insbesondere der Schutz personenbezogener Daten im Bereich von Polizei und Justiz. In diesem Bereich verpflichten die Richtlinien die Schengen-Mitgliedstaaten zur Einhaltung des in diesem Rechtserlass festgelegten Mindeststandards, lassen ihnen jedoch ausdrücklich die Möglichkeit offen, strengere Bestimmungen zu erlassen. Wesentliche Neuerungen betreffen ähnliche Regelungen wie die Neuerungen in der DSGVO, so Regelungen betreffend Informations- und Löschungspflichten; Regelungen bezüglich Beschwerden an die Datenschutzbehörden, aber auch Rechtsbehelfe gegen das Verhalten von Datenschutzbehörden; Bestimmungen über die Datenschutz-Aufsichtsorgane und deren Kompetenzen, Bestimmungen zu technischen Sicherheits-Vorkehren im Datenschutz oder Normen zur Datenschutzfolgenabschätzung. Grundsätzlich hätten die Mitglieder des Schengen-Raums nach einer Übergangsfrist von zwei Jahren, d.h. bis zum 6. August 2018 die Richtlinien in ihrem Zuständigkeitsbereich umsetzen müssen[18]. In der Schweiz ist dies bis anhin nur dem Kanton Aargau durch die Revision seines Datenschutzgesetzes fristgerecht gelungen. Der Kanton Bern hat, um die Frist einzuhalten, eigens eine Übergangsregelung, beschränkt auf den Bereich von Polizei und Justiz, im Hinblick auf die Richtlinien getroffen. Ebenso ist auf Bundesebene mit dem Erlass des Bundesgesetzes über die Schengen-Umsetzung durch die beiden Kammern am 28. September 2018 etwas verspätet die Frist eingehalten worden[19]. Hierzu ist anzumerken, dass das Parlament die Ausgestaltung dieses Gesetzes im Wesentlichen entsprechend den Prinzipien und Grundsätzen gemäss dem Leitfaden der Konferenz der Kantonsregierungen (KdK) ausführte, ein Leitfaden, der unter starker Beteiligung von privatim, der schweizerischen Vereinigung der Datenschutzbeauftragten, ausgearbeitet wurde und vor allem für die Revision der allgemeinen Datenschutzgesetzgebung vorgesehen ist. Auch der Kanton Aargau liess sich bei der Revision seiner Datenschutzgesetzgebung über weite Strecken von diesem Leitfaden leiten.

Auch das Bundesdatenschutzgesetz befindet sich derzeit in Revision. Im September 2017 richtete der BR die diesbezügliche Botschaft ans Parlament. Die

[18] Art. 63 Abs. 1 RL (EU) 2016/680; mit entsprechenden Ausnahmeklauseln in derselben Bestimmung
[19] SDSG (SR 235.3); BBl 2018 6003

Staatspolitische Kommission des Nationalrates beschloss Eintreten auf die Vorlage und sprach sich in der Folge für eine Teilung der Vorlage aus, damit die Einhaltung der Frist für die Umsetzung der RL (EU) nicht allzu lange verzögert werde und die Totalrevision des DSG[20] nicht unter Zeitdruck erfolgen muss. Allerdings weist die bundesrätliche Vorlage, gemessen an datenschutzrechtlichen Standards, wie sie seit Erlass der DSGVO im EU-Raum gelten, einige Mängel auf. So z.B. liesse sich überlegen, ob nicht Bestimmungen betr. die Löschung von Personendaten nachgebessert werden sollten oder ein Recht auf Datenportabilität aufgenommen werden sollte, ein Anliegen, das erst seit relativ kurzer Zeit in der Datenschutz-Literatur diskutiert wird - oder eine Pflicht zum Nachweis der Datenschutzkonformität durch verantwortliche Personendaten bearbeitende Instanzen statuiert werden könnte. Sinn würde eine solche Nachbesserungen deswegen machen, weil zwar die DSGVO für die öffentlichen Organe keine direkte Verbindlichkeit entfaltet, es anderseits aber auch im Interesse der Schweiz sein muss, ein dem EU-Raum absolut gleichwertiges Datenschutzniveau aufzuweisen, will sie allfälligen bürokratischen Hürden zwischen der CH und der EU, nicht nur im privaten, vielmehr auch im öffentlichen Bereich, ausweichen.

Bis jetzt kann festgestellt werden, dass die im bundesrätlichen Revisionsentwurf gemachten Vorschläge, soweit diese den öffentlichen Bereich betreffen, eher wenig umstritten sind. Zu reden geben teilweise vielmehr Vorschläge, soweit sie den privaten Bereich betreffen. Daher wurden auch schon Stimmen laut, die Datenschutzgesetzgebung gänzlich aufzuteilen und je ein Datenschutzgesetz für öffentlich-rechtliche und privatrechtliche Rechtsverhältnisse zu erlassen.[21]

Auch das Urner Datenschutzgesetz weist angesichts der internationalen Rechtsentwicklung und der rasant fortschreitenden Digitalisierung nicht nur im privaten, sondern auch im öffentlichen Bereich ganz erheblichen Revisionsbedarf auf. Der Datenschutzbeauftragte hat der Justizdirektion zuhanden des Rechtsdienstes entsprechende Revisionsvorschläge für die Ausarbeitung einer Botschaft an den Landrat unterbreitet. Auch auf kantonaler Ebene kann über weiteste Strecken dem Leitfaden der KdK wahrscheinlich gefolgt werden, drängen sich doch relativ viele Empfehlungen durch die Vorgaben der E-Konv108+ des Europarates und der RL (EU) 2016/680, aber auch durch die zu erwartende Revision des eidgenössischen DSG, soweit sie den öffentlichen Bereich betrifft, auch für die kantonale Ebene auf. Dabei bleibt

[20] Bundesgesetz über den Datenschutz; SR 235.1

[21] Vgl. Prof. Dr. Beat Rudin, Nun braucht es den zweiten Schritt, digma, 2018, Heft 1, S. 24ff.

insbesondere zu beachten, dass zwar die Kantone im Bereich des Datenschutzes grundsätzlich autonom, unabhängig vom Bund, legiferieren, ausser dass der Bund, sofern keine kantonale Bestimmungen über den Datenschutz bestehen würden, gewisse Bestimmungen des Bundes für das Bearbeiten von Personendaten im Bereich des Vollzuges von Bundesrecht für die Kantone als gültig erklären kann und ihnen vorschreiben kann, eine Datenschutzstelle einzurichten[22]. Aber auch die Kantone sind, genau wie der Bund, rechtlich an die internationalen Vorgaben von E-Konv108 und RL (EU) 2016/680, soweit diese zwingende Bestimmungen enthalten, gebunden. Auch wenn die EU-Richtlinien formal nur für den Bereich von Strafverfolgung und Justiz gelten, würde es datenschutzrechtlich eher widersinnig erscheinen, wenn ausgerechnet im Bereich ausserhalb der Strafverfolgung und des Strafvollzuges, ein weniger strenges datenschutzrechtliches Niveau gelten würde als im Strafverfolgungsbereich. Geht es doch beim Datenschutz um zentralste Grundrechte, also um den Schutz der persönlichen Integrität von betroffenen Menschen. Überdies bleibt zu beachten, dass die RL (EU) über weiteste Strecken den Grundsätzen und Prinzipien der DSGVO der EU nachgebildet sind, und somit dem Datenschutzniveau angeglichen wurden, wie es europaweit herrscht.

Digitalisierung und öffentliche Hand

Unter datenschutzrechtlichen Aspekten fällt manchmal auf, wie Argumentationsweisen sehr verschiedenartig verlaufen, je nach Interessenlage. So können, wenn einerseits raschere, effizientere und kostengünstigere Verwaltungsprozesse thematisch im Vordergrund stehen oder wenn anderseits die je eigene grundrechtliche Betroffenheit einer Person im Mittelpunkt steht, die Argumentationsweisen ganz verschiedene Stossrichtungen einnehmen. Es sind perspektivische Sichtweisen und Interessenkonstellationen, die einerseits sehr wichtige öffentliche Interessen beinhalten, anderseits aber auch sehr zentrale Rechtsgüter berühren, sich aber selten gänzlich kongruent in Übereinstimmung bringen lassen. Die Digitalisierung nicht nur des privaten, vielmehr auch des öffentlichen Bereichs bringt unbestreitbar riesige Vorteile, vermehrte Effizienz und viele Erleichterungen mit sich. Die fortschreitende Digitalisierung weckt aber andererseits ebenso unbestreitbar ein starkes, unstillbares Verlangen, einmal vorhandene Daten, und so auch Personendaten, für möglichst viele Zwecke verfügbar zu machen. Da mögen bei Einführung neuer Projekte oder anlässlich der Schaffung von gesetzlichen Grundlagen anfänglich

[22] Art. 37 DSG Bund; SR 235.1

noch so gute Grundsätze verfolgt und Versprechungen abgegeben werden: Der praktische Alltag lässt jeweils nicht lange auf sich warten und die Verfügbarkeit von vorhandenen Personendaten wird unter irgendeinem leicht zu vermittelnden Argument oder Titel auszuweiten versucht. An empirischen Beispielen würde es da wohl nicht fehlen:

Alle erinnern sich an die Abstimmung über das Referendum gegen die Einführung eines biometrischen Passes im Mai 2009. Zwar lehnte eine knappe Mehrheit der Stände den Bundesbeschluss ab, während das dazu nötige Volksverdikt (schweizerisch: 50.1% Ja zu 49,9% Nein) äusserst knapp ausfiel. Unser Kanton stimmte, gerade umgekehrt zum gesamtschweizerischen Volksverdikt, hauchdünn dem Referendum zu mit 49,21% Ja zu 50,79% Nein. Wir alle haben noch die Argumentationen der befürwortenden Kräfte für die damalige Bundes-Vorlage im Kopf, z.B. Stichworte wie »kein polizeilicher Zugriff auf die entsprechende zentrale Datenbank» usw. Es vergingen keine zwei Jahre, als im Parlament eine Motion deponiert und in der Folge vom Nationalrat wie vom Ständerat gutgeheissen wurde, die der Polizei den Zugriff auf die entsprechende zentrale Datenbank ermöglichen sollte. Es ist ein geradezu klassisches Beispiel, wie der rasante digitale Fortschritt nicht nur im privaten, vielmehr auch im öffentlichen Bereich ein exponentielles Wachstum an Verfügbarkeit von Personendaten ermöglicht und wie gleichzeitig dazu auch der Hunger nach Personendaten seitens öffentlicher Funktionsträgerschaften proportional zu diesem Wachstum wächst.[23] Ein weiteres Beispiel wäre die AHVN13. Anfänglich wurden klare gesetzliche Leitplanken eingebaut, um die Verwendung dieses zentralen Personen-Identifikators nach Möglichkeit einzuschränken.[24] Heute ist eine Revision des AHVG im Gang, dahingehend, diesen zentralen Personen-Identifikator bei begründetem Bedarf möglichst flächendeckend auf allen öffentlichen Ebenen einsetzen zu können, trotz auch gewisser Bedenken von Fachpersonen[25]. Und es gäbe weitere Beispiele zu nennen, wie Errungenschaften digitaler Projekte auch im öffentlichen Bereich den Personendatenhunger enorm anregen.

Als weiteres Beispiel möge dienen die Contact-Tracing-App, auch sie eine wunderbare Errungenschaft des digitalen Fortschritts, die sich in Zeiten von Pandemien als effizientes Instrumentarium gegen eine rasante Ausbreitung von Krankheiten einsetzen lässt und dadurch den Menschen manche Grundrechte,

[23] Vgl. auch: Prof. Dr. Beat Rudin, Digitalisierung braucht mehr als Feigenblätter, in digma, 2018, Heft 2, S. 66
[24] Vgl. Art. 50e AHVG; SR 831.10 und entsprechender Revisionsentwurf
[25] Gutachten Prof. Dr. David Basin, Risk Analysis on Different Usages of the Swiss AHV Number, (ETH Zürich, 27. September 2017)

z.B. Versammlungs- oder Bewegungsfreiheit, auch in Krisenzeiten zumindest teilweise auszuüben ermöglicht, wenn sie denn soweit als möglich unter Einhaltung von datenschutzrechtlichen Rahmenbedingungen programmiert wird und nach Beendigung einer Pandemie nicht gestützt auf jedes praktische Bedürfnis wieder eingesetzt werden darf.

IV

Beispiele aus der Beratungstätigkeit

1.

Auslagerung von Personendaten durch die Kantonspolizei zur Bearbeitung an Dritte oder andere Polizeicorps

Die Anfrage beinhaltet die Frage, wie weit es möglich (zulässig) erscheint, polizeiliche Daten an Dritte (spezialisierte Firmen), bzw. an eine andere Polizei zur Auswertung auszulagern, weil die Auswertung durch eigene Leute mangels geeigneter Infrastruktur unverhältnismässig viel Zeit in Anspruch nehmen und auch sehr hohe Kosten betreffend die Ausbildung, Infrastruktur etc. verursachen würde.

Das derzeit geltende Urner Datenschutzgesetz kennt keine Bestimmung, in welcher die Datenbearbeitung durch Dritte explizit geregelt wird, was eigentlich ein Mangel darstellt, welcher anlässlich einer künftigen Revision dringend behoben werden muss. In vielen kantonalen, aber auch in der Datenschutzgesetzgebung des Bundes ist diese Frage ausdrücklich geregelt, d.h., eine Auslagerung, bzw. ein Outsourcing unter bestimmten Bedingungen ist erlaubt, sofern es die Umstände als notwendig erscheinen lassen[26]. Aus datenschutzrechtlicher Sicht bin ich der Auffassung, dass es auch der öffentlichen Hand in Uri nicht unter allen Umständen untersagt sein kann, die Bearbeitung von Personendaten auszulagern, wenn es die Situation dringend erfordert. In gewissen Gebieten, wie z.B. im Gesundheitsgesetz, wird dies indirekt auch ausdrücklich geregelt[27], wobei allerdings die Übertragung von gesetzlichen Aufgaben mit einer Auftragsdatenbearbeitung inhaltlich nicht deckungsgleich ist. Natürlich haben die öffentlichen Organe die ihnen obliegenden gesetzlichen Aufgaben, und die damit verbundene Bearbeitung von Personendaten grundsätzlich in eigener Regie zu erfüllen, solange keine gesetzliche Grundlage eine andere Lösung ermöglicht. Aber auch wenn keine einschlägige gesetzliche Bestimmung in der Sachgesetzgebung vorhanden ist,

[26] Vgl. Art. 10a DSG Bund; SR 235.1
[27] Gesundheitsgesetz Art. 4; RB 30.2111

sollte, wenn es die Situation dringend erfordert, eine Auslagerung möglich sein.

Gestützt auf diese Annahme erscheint zwar der Wortlaut von Art. 3 Abs. 1 lit. d DSG[28] nicht direkt auf die unterbreitete Fragestellung anwendbar. Der Begriff «mit der Erfüllung öffentlicher Aufgaben betraut zu sein» ist viel umfassender als der Begriff der Auftragsdatenbearbeitung und der Gesetzgeber hat wohl nicht spezifisch an das Auslagern von Personendaten zur Bearbeitung gedacht. Bearbeiten Dritte (Privatfirmen) oder z.B. ein anderes Polizeicorps im Auftrag der Kantonspolizei Personendaten im Rahmen eines Outsourcings, so käme diesen dadurch noch kein Behördenstatus zu im Sinne von Art. 3 Abs. 1 lit. d DSG zu. Hingegen findet sich eine Strafbestimmung im Datenschutzgesetz des Kantons Uri, die so ausgestaltet ist, dass sich zur Not daraus e contrario schliessen lässt, dass ein Outsourcing nicht unter allen Umständen untersagt ist, selbst wenn es sich dabei um eine etwas gewagte Interpretation handelt. Das Urner DSG ist in seinen Grundsätzen weitgehend, soweit es den öffentlichen Bereich betrifft, dem Datenschutzgesetz des Bundes[29] nachgebildet. Dieses regelt in Art. 10a unter dem Titel „Datenbearbeitung durch Dritte“ die Frage insofern, als die Datenbearbeitung durch Vereinbarung oder Gesetz Dritten übertragen werden kann, sofern die Daten nur so bearbeitet werden, wie der Auftraggeber (das öffentliche Organ) es selber darf und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Nachdem im Urner DSG die Auftragsdatenbearbeitung bis anhin nicht explizit geregelt ist, was als eine echte Gesetzeslücke betrachtet werden darf und nicht als ein qualifiziertes Schweigen behandelt werden muss, lässt sich gestützt auf Art. 24a Abs. 1 lit. c DSG dennoch vertreten, dass das Datenschutzgesetz eine Auftragsdatenbearbeitung nicht unter allen Umständen untersagen will und unter den weiter unten ausgeführten Leitplanken eine Auftragsdatenbearbeitung möglich sein sollte.

Das Polizeigesetz des Kantons Uri regelt den Umgang mit polizeilichen Daten unter Art. 43ff. PolG (RB 3.8111) und erklärt das kantonale DSG subsidiär für anwendbar, soweit das Polizeigesetz oder die StPO (SR 312.0) nichts anderes bestimmt. Art. 44 und 45 PolG betreffen aus datenschutzrechtlicher Sicht nicht die unterbreitete Fragestellung. Soweit ich sehe, ist mit diesen Bestimmungen nicht das eigentliche Auslagern oder Outsourcing einer Datenbearbeitung gemeint, die eigentlich der Kantonspolizei obliegt. Vielmehr geht es bei diesen Bestimmungen, insbesondere bei Art. 45 PolG, um den gegenseitigen Datenaustausch in Form von Hilfestellungen bei der Erfüllung von gesetzlichen Aufgaben durch das Empfängerorgan der jeweiligen Polizeibehörde und allenfalls um Sicherheitsmassnahmen zugunsten von betroffenen privaten Personen. Aufgrund dieser Regelung im Polizeigesetz kann jedoch gesagt

[28] RB 2.2511
[29] SR 235.1

werden, dass dieses Gesetz ein Auslagern nicht a priori verbietet, indem es eine gesetzliche absolute Geheimhaltungspflicht statuieren würde.

Zieht man, wie oben erwähnt, Art. 24a Abs. 1 lit. c DSG e contrario heran, und auch mit Blick auf das DSG Bund und andere kantonale Datenschutzgesetze, so empfiehlt es sich, bei einer Auslagerung, die immer nur subsidiär erfolgen sollte, gewisse Grundsätze zu beachten, wie sie in der Datenschutzrechts-Literatur Anerkennung finden. Vorliegend geht es um Outsourcing bei der Kantonspolizei:

. Verantwortlich für die Bearbeitung von polizeilichen Daten bleibt auch bei Auslagerung grundsätzlich die Kantonspolizei, bzw. dasjenige Organ, welches innerhalb der Polizei für diese gesetzliche Aufgabe zuständig ist. Ein Auftragnehmer/Auftragnehmerin ist lediglich im Rahmen der vertraglichen Vereinbarung ermächtigt, Informationen der Kantonspolizei Uri zu bearbeiten.

. Die Kantonspolizei Uri, bzw. dessen zuständiges Organ, muss die rechtliche Verfügungsmacht über die zu bearbeitenden Daten behalten. Das bedeutet z.B., dass es dem Auftragnehmer jederzeit und ohne Begründungspflicht und ungeachtet der jeweiligen konkreten vertraglichen Situation den Zugang zu den bearbeiteten Daten verwehren können muss, bzw. die vertraglich geregelte Auslagerung widerrufen können muss. Die Polizei muss sich vorbehalten, dass sie die bearbeiteten Daten jederzeit in einem zum Voraus vereinbarten Format heraus verlangen darf und dass der Auftragnehmer sich verpflichten muss, auf Geheiss der Kantonspolizei die bearbeiteten Informationen bei sich unwiderruflich zu löschen und zu vernichten.

. Die vom Auftragnehmer bearbeiteten Informationen dürfen ausschliesslich zum vertraglich festgelegten Zweck bearbeitet werden (Art. 4 DSG). Weitere Bearbeitungen für vertragsfremde Zwecke dürfen ohne ausdrückliche schriftliche Zustimmung seitens der Kapo Uri nicht erfolgen.

. Eine Bekanntgabe von Informationen an Dritte durch den Auftragnehmer darf nicht erfolgen.

. Es versteht sich, dass ein Auftragnehmer, dessen sämtliche Mitarbeitende, und sofern vertraglich zulässig, dessen Unterauftragnehmer, im Rahmen der Vertragserfüllung einer umfassenden Geheimhaltungs- und Schweigepflicht, sei es aufgrund des Amtsgeheimnisses, sei es aufgrund einer vertraglichen Geheimhaltungspflicht, unterstehen. Bei der Kantonspolizei beziehen sich diese Geheimhaltungspflichten auf sämtliche Systeme, Prozesse und Informationen. Entsprechend müssen sie auch innerhalb des Betriebes der beauftragten Institution/Firma, auf sämtlichen Stufen, ungeachtet der hierarchischen Position, gelten. Drängt sich die Auslagerung von besonders schützenswerten

Personendaten[30] auf, so sollten Mitarbeitende des Auftragnehmers/Unterauftragsnehmers, für die Bearbeitung dieser Daten, wenn technisch möglich, dem direkten Kontroll- und Weisungsrecht der Kantonspolizei, bzw. der dortigen zuständigen Stelle, unterstellt sein.

. Beruft sich jemand auf das Öffentlichkeitsprinzip der kantonalen Verwaltung (Information auf Anfrage, Art. 6 ff. OeG)[31] und ersucht um irgendwelche Informationen, welche Daten (Personen- oder Sachdaten) betreffen, die durch einen Auftragnehmer bearbeitet werden, so sollte ausdrücklich vereinbart werden, dass das Gesuch lediglich durch die zuständige Stelle der Kantonspolizei Uri bearbeitet werden darf.

. Die Durchsetzung der Rechte von betroffenen Personen im Sinne von Art. 14ff. DSG ist, falls die verantwortliche Stelle der Kantonspolizei oder eine Beschwerdeinstanz dem Anspruch stattgibt, vom Auftragnehmer technisch zu garantieren.

. Der Auftragnehmer kennt die Pflicht der Kantonspolizei, für die vollumfängliche Sicherheit der bearbeiteten Daten im Sinne von Art. 11 DSG besorgt zu sein. Die Kantonspolizei orientiert den Auftragnehmer über die Pflichten betreffend Schutzbedarf der bearbeiteten Personendaten. Besonders schützenswerte Personendaten verlangen nach einem höheren Schutzbedarf. Der Auftragnehmer bietet Gewähr, dass er fachlich und technisch in der Lage ist, diesem Schutzbedarf der Personendaten nachzuleben. Er verfügt über ein hinreichendes Sicherheitskonzept, damit die Datensicherheit während und ausserhalb des Betriebes aufrechterhalten werden kann. Es gelten nach Möglichkeit die gängigen Sicherheitsstandards.

. Der Auftragnehmer trifft die organisatorischen Massnahmen und ist fachlich und technisch in der Lage, diejenigen Informationen und Datenbestände, die er im Auftrag der Kantonspolizei bearbeitet, von den eigenen wie von denjenigen anderer Auftraggeber, völlig zu trennen. Der Auftragnehmer verschafft gegenüber der Kantonspolizei Transparenz betreffend die Methoden und Prozesse, die er zur Einhaltung der Datensicherheit anwendet. Die Kantonspolizei hat das Recht, allfällige sicherheitsrelevante Unterlagen einzusehen und sich die betrieblichen Abläufe vorführen zu lassen.

. Stellen sich ausserordentliche Vorkommnisse ein wie beispielsweise Datenverlust, unrechtmässige Zugriffe oder Hackerangriffe, informiert der Auftragnehmer die Kantonspolizei umgehend in einem eigens dazu vorbereiteten Meldeverfahren.

---

[30] Art. 3 Abs. 1 lit. f DSG

[31] RB 2.2711

. Der Auftragnehmer verpflichtet sich, in periodischen Abständen Sicherheits-Audits nach anerkannten Standards durchzuführen. Auf Anfrage stellt er der Kantonspolizei die Berichte unentgeltlich zur Verfügung.

. Der Auftragnehmer darf Dritte zur Erfüllung des ihm erteilten Auftrages nur beiziehen, wenn die Kantonspolizei schriftlich die Zustimmung erteilt oder er die Absicht einer Erteilung eines Unterauftrages anlässlich der Vertragsverhandlungen mit der Kantonspolizei offenlegt. Ein allfälliger Unterauftragnehmer muss in der Lage sein, sämtliche Verpflichtungen, die sich für den Auftragnehmer aus dem Vertragsverhältnis mit der Kantonspolizei ergeben, zu erfüllen sowie über die fachlichen und technischen Voraussetzungen verfügen.

. Bei der Wartung und Entwicklung von Systemen des Auftragsnehmers durch Dritte leistet der Auftragnehmer Gewähr, gemäss den organisatorischen und technischen Möglichkeiten zu verhindern, dass diese Dritte Einblick in die ausgelagerten Informationen der Kantonspolizei erhalten.

. Die durch die Kantonspolizei ausgelagerten Daten dürfen grundsätzlich durch eine andere Polizei oder Dritte nur in der Schweiz bearbeitet, gespeichert und archiviert werden. Drängt sich eine Bearbeitung aus unausweichlichen Gründen im Ausland auf, so darf dies nur geschehen, wenn die Kriterien von Art. 8a DSG vollumfänglich erfüllt sind.

. Benutzt der Auftragnehmer Cloud Computing, so darf er dies nur mit Zustimmung der Polizei tun und er hat zu garantieren:

. Der Auftragnehmer informiert und dokumentiert die zuständige Stelle der Kantonspolizei schriftlich und umfassend über die verwendete Technologie, bzw. über deren Weiterentwicklung. Insbesondere informiert er die zuständige Stelle auch über sämtliche möglichen Datenbearbeitungsorte (Serverstandorte).

. Werden besonders schützenswerte Personendaten bearbeitet, dürfen diese nur mit einer umfassenden kryptographischen Sicherung in die Cloud einfliessen. Diese kryptographische Sicherung muss in jeder Phase der Bearbeitung, bis und mit Löschung und Vernichtung der besonders schützenswerten Personendaten, durch den Auftragnehmer garantiert sein. Die zu dieser Sicherung notwendigen Zertifikate (Schlüssel) verwaltet die Kantonspolizei selbst.

. Die Einhaltung der gegenseitig eingegangenen Vertragsverpflichtungen sollten mit einer vertraglich ausgehandelten Konventionalstrafe, unter Vorbehalt der Geltendmachung allfälligen weiteren Schadens, abgesichert werden.

. Es versteht sich, dass die Bezahlung einer Konventionalstrafe nicht von der Pflicht zur strengen Wahrung der Geheimhaltungspflichten befreit. Auch allfällig relevante strafrechtliche Normen werden dadurch nicht aufgehoben.

. Der Auftragnehmer sollte ausdrücklich verpflichtet werden, bei Aufhebung des Vertragsverhältnisses, unbesehen aus welchem Grund, sämtliche Bestände an bearbeiteten Informationen auf Geheiss der Kantonspolizei dieser in einem vereinbarten Format unverzüglich und unentgeltlich bedingungslos herauszugeben. Ein vorläufiger Rückbehalt darf selbst dann nicht stattfinden, wenn sich die Vertragsparteien in einem Rechtsstreit befinden sollten.

. Überdies muss die Polizei vom Auftragnehmer verlangen können, nach Auflösung des Vertrages sämtliche im Rahmen dieses Vertrages bearbeiteten Informationen unentgeltlich zu vernichten und diese Vernichtung entweder selbst, oder durch unabhängige Dritte kontrollieren zu lassen.

. Sämtliche Mitarbeitenden des Auftragnehmers oder eines allfälligen Unterauftragnehmers unterstehen auch nach Vertragsauflösung als Hilfspersonen der strengen gesetzlichen Geheimhaltungspflicht. Als anwendbares Recht gilt nur schweizerisches Recht. Als Gerichtsstand gilt der Sitz der Kantonspolizei.

2.

Anfrage einer Gemeinde betreffend Kompetenzen eines privaten Sicherheitsdienstes.

Im Zusammenhang mit dem Freizeit- und Veranstaltungsbetrieb in der Umgebung von Sportanlagen, einem Jugendlokal und Jugendtreffpunkt, dem Schulhausareal usw., d.h. an öffentlichen Örtlichkeiten einer Gemeinde, bildet es das Ziel der Gemeindebehörden, für Ordnung zu sorgen und Littering, Sachbeschädigungen und Konflikten präventiv vorzubeugen. In diesem Zusammenhang erteilte der zuständige Gemeinderat einer privaten Sicherheitsfirma einen Auftrag. In der Offerte/Auftrag (Pflichtenheft) finden sich als Schwerpunkte der Tätigkeit der Firma folgende Punkte aufgelistet: „Situation beobachten; Gespräch suchen; auf Verhaltensregeln hinweisen und durchsetzen; Konflikte verbal schlichten; eventuell Ausweise kontrollieren; Ansprechpartner der Auftraggeberin informieren oder aufbieten; wenn nötig Polizei kontaktieren; Ereignisrapport erstellen.“ In diesem Zusammenhang hat offenbar der beauftragte Sicherheitsdienst zwei schulpflichtige Jugendliche im Umgelände des Jugendlokals beobachtet, wie sie einen Joint vorbereiteten. Er hat den Vorgang fotografiert und ebenso deren ID-Ausweise fotografiert, also die Personalien aufgenommen und dem Gemeinderat die Personendaten mit dem Rapport gemeldet. Gleichzeitig hat der Sicherheitsdienst auch den Schulleiter informiert, da es sich um zwei schulpflichtige Jugendliche handelte. Der Schulleiter seinerseits informierte die Eltern der beiden Jugendlichen,

welche über die Information froh waren.

Aus diesem Ereignis ergeben sich für die Gemeindebehörden folgende Fragen:

. Darf der Sicherheitsdienst Fotos machen vom Joint, allenfalls von den Jugendlichen?

. Darf der Sicherheitsdienst Fotos machen von den Personalausweisen der beiden Jugendlichen?

. Darf die Schulleitung die ihr zugetragene Information verwenden, indem sie diese den Eltern weiterleitete?

Die Regelungen bezüglich der Tätigkeiten (Rechte und Zuständigkeiten) privater Sicherheitsdienste sind nicht in allen Kantonen einheitlich ausgestaltet. Es gibt Kantone, die ihnen teilweise (ansatzmässig) hoheitliche Funktionen, gestützt auf gesetzliche Grundlagen, übertragen. Im Kanton Uri ist dies, wie auch in vielen andern Kantonen, ausdrücklich nicht der Fall[32]. Es dürfen aufgrund dieser Bestimmung privaten Sicherheitsdiensten explizit keine hoheitlichen Befugnisse übertragen werden. Die Tätigkeit einer privaten Sicherheitsfirma stellt im Grunde ausschliesslich eine Präventivaktivität dar, die nicht in die persönliche Freiheit anderer Personen, auch nicht von Jugendlichen, eingreifen darf. Findet wirklich eine Gefährdung der öffentlichen Sicherheit statt, wo die Erfüllung von Vergehens- oder Verbrechenstatbeständen zu erwarten sind, bzw. erfüllt wurden, so kann und darf gegen Personen nur durch Benachrichtigung der öffentlichen polizeilichen Organe vorgegangen werden, es sei denn, es handle sich um eine Notstandssituation im Sinne von StGB Art. 17.[33] Eine Gewaltbefugnis in Form eines kurzfristigen Festhaltens eines Störers zu diesem Zweck ist allerdings erlaubt, jedoch nur im Rahmen des Notwehr-, Notstands- und Selbsthilferechts, dies dann, wenn Private, also nicht nur Sicherheitsdienste, gestützt auf Art. 218 StPO, Störer oder Straftäter vorläufig festhalten dürfen, um das Rechtsgut einer Person aus einer unmittelbar drohenden, nicht anders abwendbaren Gefahr zu retten. Dies jedoch nur unter der Voraussetzung, dass die Polizei nicht rechtzeitig auf den Platz kommen kann und die festzuhaltende oder abzuwehrende Person bei einem Verbrechen oder Vergehen ertappt oder unmittelbar danach angetroffen wird. Oder auch etwa in Fällen, wo die Öffentlichkeit aufgefordert wird, bei der Fahndung mitzuhelfen. Es handelt sich dabei um sogenannte „Jedermannsrechte“, d.h., ein Recht, das jedermann bei allfällig gegebenen Voraussetzungen grundsätzlich zusteht.

Vorliegend hat der Sicherheitsdienst offenbar zwei Jugendliche im Schulalter beobachten können, wie sie einen Joint drehen. Es ist offensichtlich, dass, wer

[32] Art. 59 PolG; RB 3.8111
[33] SR 311.0

einen Joint dreht, sich allenfalls, wenn überhaupt, einer Übertretung schuldig macht[34] und niemanden gefährdet. Für ein Vorgehen im Sinne von Art. 218 StPO wären in einem solchen Fall die Voraussetzungen nicht erfüllt.

In der Vereinbarung ist nun unter der Liste, welche das Auftrags-Pflichtenheft beinhaltet, auch „Eventuell Ausweise kontrollieren“ aufgeführt. Dies wäre rechtlich für eine private Sicherheitsfirma nur dann zulässig, wenn sie beauftragt wäre, allenfalls die Zugangskontrolle zu den Jugendräumlichkeiten – vielleicht anlässlich einer Veranstaltung – zu kontrollieren und die um Eintritt ersuchenden Jugendlichen auffordern würde, sich auszuweisen, beispielsweise für eine Alterskontrolle. Aber auch in einem solchen Fall wäre sie zu einer Ausweiskontrolle nur dann berechtigt, wenn die Jugendlichen freiwillig bereit wären, ihren Ausweis zu zeigen. Sind sie es nicht, dürfte eine private Sicherheitsfirma keine Personalien kontrollieren, sondern einfach die Jugendlichen abweisen, bzw. ihnen den Zugang verwehren.

Gemäss Urner Polizeirecht und auch nach dem Recht der meisten andern Kantone, handelt es sich bei der Anhaltung und Identitätsfeststellung um eine klare polizeiliche Massnahme, somit um eine hoheitliche Befugnis, welche auszuüben einer privaten Sicherheitsfirma rechtlich verwehrt ist (Art. 59 PolG).

Beobachtet eine private Sicherheitsfirma auf dem umliegenden Areal eines Jugendtreffpunktes, wo sie im Auftrag einer Gemeinde Sicherheitskontrollen durchführt, dass Jugendliche Cannabis konsumieren oder Vorbereitungshandlungen dazu treffen, darf sie wohl die Jugendlichen darauf ansprechen, sie darauf hinweisen, dass der Konsum von Cannabis grundsätzlich nach wie vor illegal ist. Aber sie darf nicht deren Personalien kontrollieren, indem sie von diesen verlangt, sich auszuweisen. Allerdings kann der Sicherheitsmann oder die Sicherheitsfrau die Polizei anvisieren und diese bitten, ihrerseits Kontrollen durchzuführen.

Auch wäre es im Sinne des Datenschutzes, aber auch im Sinne des allgemeinen Persönlichkeitsschutzes, nicht angängig, gezielt die Jugendlichen in einer solchen Situation (da lediglich eine allfällige Übertretung im Raum steht) zu fotografieren und die Bilder weiterzureichen. Denn dies liefe darauf hinaus, die Identitätsüberprüfung faktisch auf visuellem Weg vorzunehmen. Ein solches Vorgehen wäre auch durch Art. 218 StPO nicht gedeckt, da es sich um eine Übertretung handelt.

Ebenso wenig darf ein privater Sicherheitsdienst die ID-Ausweise fotografieren, es sei denn, die Jugendlichen hätten ihm die Ausweise ausdrücklich freiwillig gezeigt und ihm erlaubt, die Ausweise zu fotografieren. Voraussetzung dazu

[34] Art. 19a Abs. 1; allenfalls 19b Abs. 1 BetmG; SR 812.121

bildet jedoch, dass die Jugendlichen genau um den Umstand wissen, bzw. aufgeklärt worden sind, dass sie einem privaten Sicherheitsdienst keinen Ausweis zu zeigen verpflichtet sind. Wären sie im Vorfeld in irgendeiner Form, wenn auch nur subtil, eingeschüchtert worden, bewegt sich das Verhalten des Sicherheitsdienstes im illegalen Bereich.

Insofern ist es nicht statthaft, dass ein privater Sicherheitsdienst dem Gemeinderat die Personalien der betroffenen Jugendlichen rapportiert, selbst wenn er im Auftrag des Gemeinderates arbeitet. Zweifelsohne darf und muss der Sicherheitsdienst seinem Auftraggeber rapportieren, dass Jugendliche beobachtet wurden, wie sie im Umgelände des Jugendlokals Cannabis konsumierten oder Vorbereitungen dazu trafen. Das zu wissen liegt im gesetzlichen Interesse einer Gemeindebehörde.

Die Identitätskontrolle, d.h. die Ausweiskontrolle eines/einer Jugendlichen stellt eine Bearbeitung von Personendaten dar. Wird die Kontrolle durch einen privaten Sicherheitsdienst vorgenommen, ohne dass ein Jugendlicher freiwillig zustimmt – freiwillig bedeutet in diesem Zusammenhang, dass ein Jugendlicher im genauen Wissen um seine Rechte und Pflichten einer Kontrolle zustimmt und zwar ohne jegliche unstatthafte Beeinflussung – dann gilt eine derartige Bearbeitung von Personendaten als nicht rechtens. Art. 59 PolG verbietet ausdrücklich, dass eine private Sicherheitsfirma gegenüber Personen hoheitliche Befugnisse im Sinne von polizeilichen Massnahmen[35] ausüben oder sich aneignen darf.

Andererseits verlangt Art. 4 Abs. 1, 2 und 3 DSG,[36] dass Personendaten grundsätzlich nur gestützt auf eine gesetzliche Grundlage oder zur Erfüllung einer gesetzlichen Aufgabe und ganz allgemein nur rechtmässig bearbeitet werden dürfen. Die Überprüfung der persönlichen Identität (Ausweiskontrolle) ist, als Ausübung einer hoheitlichen Befugnis und polizeilichen Massnahme, einer privaten Sicherheitsfirma verwehrt.

Anders verhielte es sich, wenn die betreffenden Jugendlichen den Vertretern des Sicherdienstes ohnehin persönlich bekannt waren. Wenn also die Jugendlichen ihnen ohne jegliche Personenüberprüfung namentlich bekannt gewesen wären, wäre eine Meldung dieser Jugendlichen an den Gemeinderat nicht zu beanstanden. Hingegen ist eine direkte Meldung des Sicherheitsdienstes der Personalien an die Schulleitung aufgrund des von ihm wahrzunehmenden Auftrages streng genommen nicht korrekt. Zum einen erfüllt der Sicherheitsdienst einen Auftrag, der ihm vom Gemeinderat erteilt wurde. Der Gemeindeschreiber handelte wahrscheinlich in Vertretung des Gemeinderates,

[35] Art. 13ff. PolG
[36] RB 2.2511

nicht der Schulbehörden. Aufgrund der kantonalen Schulgesetzgebung erstreckt sich der Verantwortungsbereich der Schulbehörden (Schulrat, Schulleitung und Lehrerschaft) primär, sachlich wie örtlich, auf den Bereich der Schule, allenfalls auf das Schulhausareal.

Aus datenschutzrechtlicher Sicht liesse es sich hingegen vertreten, wenn eine Mitteilung seitens des Gemeinderates an die Schulleitung ergehen würde, sofern er aufgrund derartiger Feststellungen zur Überzeugung gelangen und erhebliche Indizien darauf hinweisen würden, dass ein schulpflichtiger Jugendlicher ein problematisches Freizeitverhalten, z.B. frühzeitiger und übermässiger Alkoholkonsum, oder eben Cannabis-Konsum, erkennen lässt. Dies liesse sich gestützt auf Art. 7 DSG dahingehend rechtfertigen, als in erster Linie die Schulbehörden, in Zusammenarbeit mit den Eltern, gefordert wären, wenn sich ernst zu nehmende Anzeichen eines solchen problematischen Freizeitverhaltens zeigen sollten. Dies aus der Überlegung, dass das Freizeitverhalten eines/einer schulpflichtigen Jugendlichen, soweit es die Entwicklung von deren Persönlichkeit mitberührt, zwar formal nicht das schulische Verhalten betrifft, sich jedoch pädagogisch nicht gänzlich von diesem Verhalten, und damit vom Erziehungsauftrag, abtrennen lässt.

Die Mitteilung seitens der Schulleitung an die Eltern scheint mir aus Datenschutzgründen bei der vorliegenden Konstellation nicht problematisch. Dies aus der Überlegung, dass einerseits im Kontext des gesamten Erziehungs- und Bildungsauftrages, welchen die Bildungs-Gesetzgebung sowohl einerseits den Schulbehörden als anderseits auch den Eltern auferlegt, beide Seiten zu einer konstruktiven Zusammenarbeit verpflichtet sind. Hingewiesen sei in diesem Zusammenhang stellvertretend auf Art. 47 Abs. 1 und 2 SchulG.[37] Anderseits haben alle, oder doch die allermeisten Eltern ein zentrales Interesse daran, zu wissen, nicht was alles ihre Zöglinge konkret in der Freizeit treiben – der persönliche Freiraum muss selbstverständlich gewahrt bleiben - jedoch ob das Freizeitverhalten ihrer Jugendlichen sich in einigermassen unproblematischen Bahnen bewegt. Unter diesem Gesichtspunkt ist eine Mitteilung der Schulbehörden an die Eltern, dass ein schulpflichtiger Jugendlicher beim Cannabis- oder Alkoholkonsum beobachtet wurde, datenschutzrechtlich nicht zu beanstanden.

[37] RB 10.1111

3.

Gewährung des elektronischen Zugriffs auf Steuerdaten durch die Bildungs- und Kulturdirektion

Das Amt für Steuern wurde durch die BKD angefragt, ob zwei Mitarbeiterinnen, die für die Sachbearbeitung von Ausbildungsbeiträgen zuständig sind, ein direkter Zugriff in elektronischer Form auf die relevanten Steuerdaten gewährt werden könne. Die ersuchende Behörde stützt sich bei ihrer Anfrage auf Art. 22 der Stipendienverordnung[38] und führt im Wesentlichen aus, dass es immer wieder vorkomme, dass gesuchstellende Personen unvollständige oder nicht mehr aktuelle Unterlagen einreichen würden, sodass die Behörde darauf angewiesen sei, die fehlenden Unterlagen beim Amt für Steuern anzufordern.

Das Amt für Steuern weist in seinen Erläuterungen zu dieser Anfrage darauf hin, dass im Jahre 2015 in ca. 350 Fällen im Rahmen von Art. 22 der Stipendienverordnung Auskunft an die BKD erteilt worden sei. Dabei habe sich die Auskunftserteilung hauptsächlich auf die Monate September/Oktober konzentriert.

Gestützt auf Art. 177 des Steuergesetzes[39] unterliegt die Steuerverwaltung nebst dem allgemeinen Amtsgeheimnis einer relativ strengen besonderen Geheimhaltungspflicht. Vorliegend handelt es sich datenschutzrechtlich um die Konstellation der Bekanntgabe von Personendaten an eine andere Behörde im Sinne von Art. 7 DSG[40]. Eine solche Bekanntgabe ist grundsätzlich zulässig, wenn eine gesetzliche Verpflichtung oder Ermächtigung vorliegt (Art. 22 Stipendienverordnung) oder wenn für den Datenempfänger die Bekanntgabe für die Erfüllung einer gesetzlichen Aufgabe als erforderlich erscheint. In Bezug auf die steuerrechtlichen Personendaten der gesuchstellenden Personen, allenfalls ihrer unterstützungspflichtigen Angehörigen, sind diese datenschutzrechtlichen Voraussetzungen zweifelsohne als erfüllt anzusehen. In diesem Rahmen wurden ja bis anhin auch immer Auskünfte erteilt.

Art. 8b DSG erlaubt ein Abrufverfahren, wenn die datenschutzrechtlichen Voraussetzungen, welche Art. 7 und 8 DSG vorsehen, grundsätzlich erfüllt sind. Bezüglich Art. 7 Abs. 2 sind sie vorliegend im Grunde über weite Strecken nicht erfüllt. Denn der in Art. 7 DSG erwähnte Vorbehalt einer besonderen Geheimhaltungspflicht nimmt im vorliegenden Kontext Bezug auf Art. 177 StG und bildet einen Persönlichkeitsschutz gerade auch für jene steuerpflichtigen Personen, die nicht in einem Gesuchs-Verfahren um Gewährung von Stipendien stehen, die also nicht in das Segment jener Steuerpflichtigen fallen, die um

[38] RB 10.2201
[39] RB 3.2211
[40] RB 2.2511

Ausrichtung von Studienbeiträgen ersuchen. Diese Personen besitzen ein schutzwürdiges persönliches Interesse, dass ihre Steuerdaten nur jenen privaten Personen, aber auch Amtsstellen, offenbart werden, welche sie zur Erfüllung einer gesetzlichen Aufgabe benötigen. Insofern besteht im Sinne von Art. 9 DSG auch ein öffentliches Interesse, dass die Geheimhaltungspflicht im Sinne von Art. 177 StG nur in absolut notwendigen Situationen durchbrochen wird. Art. 177 StG Abs. 5 zählt denn auch abschliessend auf, welchen Stellen bei allenfalls notwendigem Bedarf der elektronische Zugang zu Steuerdaten gewährt werden darf, was e contrario bedeutet, dass vorerst die Gewährung eines elektronischen Zugangs an weitere Stellen untersagt ist. Es liegt also eine gesetzliche Schranke vor, über welche sich auch das Amt für Steuern, ohne Revision der Bestimmung, nicht hinwegsetzen darf.

In diesem Zusammenhang muss nicht weiter darauf eingegangen werden, dass die Ermöglichung eines elektronischen Abrufverfahrens für die Erfüllung von gesetzlichen Aufgaben, welche nur die Steuerdaten einer sehr stark beschränkten Anzahl von Steuerpflichtigen erfordern, zumindest eine potentielle Durchbrechung der durch Art. 177 StG auferlegten Geheimhaltungspflicht darstellt.

Das Amt für Steuern spricht das Prinzip der Verhältnismässigkeit an und führt zwei Beispiele an, wo gegenüber kantonalen Ämtern aufgrund des Massengeschäftes und des dadurch bedingten sehr umfangreichen Mengengerüstes von Anfragen die Auskunftserteilung durch elektronischen Zugriff erledigt wird. Die beiden vom Amt für Steuern erwähnten elektronischen Zugriffsmöglichkeiten durch kantonale Ämter sind denn auch durch Art. 177 Abs. 5 StG ausdrücklich gedeckt.

Gemäss der Definition von Art. 3 Abs. 1 lit. b DSG stellt die Gewährung eines elektronischen Zugriffs eine Bearbeitung von Personendaten dar. Art. 4 Abs. 3 verlangt, dass Personendaten nur verhältnismässig bearbeitet werden dürfen. Vor dem Hintergrund dieser Bestimmung dürfte die Voraussetzung von Art. 4 Abs. 1 lit. a DSG kaum erfüllt sein, bezieht sich Art. 22 der Stipendienverordnung grundsätzlich doch nur auf die Steuerdaten der gesuchstellenden Steuerpflichtigen.

Es bleibt auch zu beachten, dass Art. 17 und Art. 19 der Stipendienverordnung die gesuchstellenden Personen zu einer detaillierten Mitwirkungspflicht anhält, diese also gemäss den informellen Instruktionen der BKD verpflichtet sind, detaillierte und aktuelle Unterlagen einzureichen. Im Übrigen ist es ihnen auch unbenommen, ihrerseits in eigener Regie die vollständigen und aktuellen Steuerunterlagen beim Amt für Steuern anzufordern. Art. 22 Stipendienverordnung verpflichtet andere Behörden, so auch die

Steuerbehörden, ausdrücklich nur soweit zur Amtshilfe, als dies sich für den Vollzug der Stipendienverordnung als notwendig erweist. Vor diesem Hintergrund ist, nebst der gesetzlichen Schranke von Art. 177 Abs. 5 StGB, ohnehin auf das erwähnte Prinzip der Verhältnismässigkeit abzustellen.

Hinsichtlich des Datenschutzes verlangt der Grundsatz der Verhältnismässigkeit, dass allgemein nur so viele Personendaten wie nötig und so wenig wie möglich bearbeitet werden sollen. Eine Massnahme gilt allgemein dann als verhältnismässig, wenn sie einerseits für die Erreichung eines im Gesetz verankerten Zweckes (Art. 1 Stipendienverordnung) sich als notwendig erweist, demnach den geringstmöglichen Eingriff darstellt und wenn sie anderseits geeignet und demnach zwecktauglich ist. Überdies soll zwischen dem Zweck und der Massnahme ein vernünftiges Verhältnis bestehen (Verhältnismässigkeit im engeren Sinn). Dieser Grundsatz gilt ganz allgemein für staatliches Handeln, also auch im Bereich der Verwaltung und verpflichtet folgerichtig das Amt für Steuern zum geringstmöglichen Eingriff in die Persönlichkeitsrechte derjenigen Steuerpflichtigen, welche bei der BKD nicht als Gesuchsteller in Escheinung treten.

Das Amt Steuern legt dar, dass das Mengengerüst der Anfragen im Zusammenhang mit Stipendiengesuchen im Vergleich mit andern elektronischen Zugriffen doch relativ bescheiden ausfällt; dass das Handling der entsprechenden Applikation „NEST“ aufgrund der Komplexität steuerrechtlicher Gegebenheiten sich als nicht ganz einfach erweist, derart, dass das Steueramt ohnehin immer wieder mit weiteren Nachfragen belastet wird, insbesondere dann, wenn eine auskunftsersuchende Behörde nicht regelmässig mit dem Abfrageprogramm befasst ist. Es kommt wie erwähnt hinzu, dass gestützt auf Art.17 und 19 der Stipendienverordnung eine detaillierte Mitwirkungspflicht für die Gesuchsteller statuiert ist, sodass es für die Gesuchsteller aufgrund der Info-Unterlagen der BKD zumutbar erscheint, möglichst in eigener Regie vollständige und aktuelle Gesuchsunterlagen beizubringen, bzw. zu vervollständigen.

Angesichts der geschilderten Umstände, der Anfragemengen, und der aufgrund der Komplexität nur relativ bedingten Entlastung des Amtes für Steuern erscheinen aus datenschutzrechtlicher Sicht die Voraussetzungen auch im Hinblick auf das Verhältnismässigkeitsprinzip als nicht erfüllt, die in Art. 177 statuierte Geheimhaltungspflicht vorliegend durch die Gewährung eines elektronischen Zugriffs zu durchbrechen.

4.

Anfrage des Kantonsspital Uri betreffend eine minderjährige Patientin

Im Kantonsspital wurde eine minderjährige, jedoch urteilsfähige Patientin behandelt. Da offenbar die Jugendliche eine nicht mehr aktuelle Krankenkasse angegeben hat, will sich das Spital bei den Eltern um die Anschrift der zuständigen Krankenkasse erkundigen, damit entsprechend Rechnungsstellung erfolgen kann. Die Mutter der Patientin hat das Spital angerufen und möchte den Grund der medizinischen Behandlung in Erfahrung bringen. Das Kantonsspital hat der Mutter vorderhand keine diesbezügliche Auskunft erteilt und möchte die Rechtslage bei der Datenschutzstelle abgeklärt wissen.

Aus datenschutzrechtlicher Sicht haben die Organe des Spitals korrekt reagiert. Art. 19c und Art. 305 Abs. 1 ZGB[41] bestimmen, dass, unter Vorbehalt der Fälle, in welchen das Gesetz die Zustimmung des gesetzlichen Vertreters vorsieht, urteilsfähige, grundsätzlich jedoch infolge Minderjährigkeit handlungsunfähige Personen, die Rechte, die ihnen um ihrer Persönlichkeit willen zustehen, selbstständig auszuüben berechtigt sind. Auch die Mehrheit der Lehre vertritt die Auffassung, dass die Liste der im höchstpersönlichen Bereich liegenden zustimmungsbedürftigen Geschäfte nicht durch Auslegung erweitert werden dürfe[42]. Das Gesetz regelt also abschliessend, welche höchstpersönlichen Rechte einer urteilsfähigen, minderjährigen Person seitens der gesetzlichen Vertretung zustimmungsbedürftig sind. Beispielhaft zu denken wäre etwa an Art. 90 Abs. 2 oder Art. 183 Abs. 2 ZGB. In Bereichen, wo die Höchstpersönlichkeit einer minderjährigen, urteilsfähigen Person im Sinne von Art. 19c Abs. 1 ZGB betroffen ist, d.h., wo es sich um Rechte handelt, die der Person um ihrer Persönlichkeit willen zustehen und daher auch ohne Zustimmung der gesetzlichen Vertretung ausgeübt werden können, ist die urteilsfähige Jugendliche zu selbstständigem Handeln berechtigt und braucht die Zustimmung der sorgeberechtigten Eltern nicht einzuholen.

Daraus folgt: Vorliegend handelt es sich um eine 16-jährige Jugendliche, welche urteilsfähig ist. Sie hat sich entschlossen, an sich im Kantonsspital eine Behandlung durchführen zu lassen. Hierbei handelt es sich um eine medizinische Behandlung, welche für die Gesundheit der Betroffenen keine weiteren Folgen zeitigt. Insbesondere bleibt dadurch die elterliche Sorge unberührt insofern, als es sich nicht um eine Behandlung handelt, welche in der Folge von den sorgeberechtigten Eltern spezifische Fürsorgemassnahmen abverlangen würde. Insofern sind die Eltern auf die Kenntnis der betreffenden Personendaten nicht angewiesen, damit sie ihrer gesetzlichen Aufgabe als Sorgeberechtigte

[41] SR 210

[42] Botschaft Erwachsenenschutzrecht BBl 2006 7001, 7095

nachkommen können. Gleichzeitig handelt es sich bei der besagten Behandlung um einen Bereich, welcher besonders schützenswerte Personendaten im Sinne von Art. 3 Abs. 1 lit. f DSG umfasst. Aus datenschutzrechtlicher Sicht dürfen solche Daten ohne ausdrückliches Einverständnis einer minderjährigen, urteilsfähigen Jugendlichen auch nicht an die sorgeberechtigten Eltern weitergegeben werden. Das geschilderte Arzt-Patienten-Verhältnis in der vorliegenden Konstellation wird vom ärztlichen Berufsgeheimnis auch gegenüber den sorgeberechtigten Eltern gedeckt und auch durch Art. 321 StGB geschützt.

Zu Recht weist das Spital auf den Umstand hin, dass Indizien eines Verbrechens oder Vergehens gegen Leib und Leben oder einer Verletzung der sexuellen Integrität nicht vorliegen, bzw. dass das medizinische Personal keine diesbezüglichen Wahrnehmungen machen konnte, welche als entsprechende Verdachtsmomente sich aufdrängen würden (Art. 36 Abs 1 lit. c GG)[43] In einem solchen Falle würde eine gesetzliche Meldepflicht seitens der zuständigen Medizinalpersonen an die Strafverfolgungsbehörden bestehen.

Das Spital kann also zu Recht auf den Datenschutz und die ärztliche Schweigepflicht verweisen. Die sorgeberechtigten Eltern bleiben dennoch verpflichtet, dem Spital die Anschrift der aktuellen Krankenkasse mitzuteilen.

5.

Anfrage vom Rechtsdienst der HotellerieSuisse; Aufbewahrungsfrist von Personendaten aus der Gästekontrolle

Der Rechtsdienst von HotellerieSuisse will eine schweizerische Übersicht über die kantonalen Bestimmungen zur Gästekontrolle in Beherbergungsbetrieben zusammenstellen. In Bezug auf Uri findet sich im Gastwirtschaftsgesetz[44] keine Bestimmung, welche die Aufbewahrungsfrist dieser Personendaten regelt.

Vorauszuschicken bleibt, dass es sich bei diesen Personendaten sehr wohl um sensitive Personendaten handeln kann. In Uri haben Personen, die einen Beherbergungsbetrieb gewerbsmässig führen, zuhanden der Kantonspolizei eine Gästekontrolle zu führen, in die sich der Gast bei seiner Ankunft einzutragen hat. Die verantwortliche Person hat sicherzustellen, dass der Eintrag durch Vorweisen eines gültigen amtlichen Ausweispapiers verifiziert werden kann.[45] Eine Frist, wie lange die Unterlagen aufbewahrt werden müssen, ist in Uri diesbezüglich, konkret bezogen auf das GWG, gesetzlich nicht explizit geregelt.

[43] RB 30.2111
[44] RB 70.2111
[45] Art. 9 Abs. 2 GWG

Nun verhält es sich so, dass es sich bei der Bestimmung von Art. 9 Abs. 2 GWG im Grunde um eine kriminalpolizeiliche Vorschrift handelt. Die privaten Betreiber von Beherbergungsbetrieben bearbeiten also die Personendaten (Gästekontrolle) grundsätzlich im Auftrag des Staates, konkret der Polizei, nehmen diesbezüglich also eine gesetzliche Aufgabe wahr.

Das Datenschutzgesetz des Kantons Uri[46] sieht in Art. 13 Abs. 1 vor, dass Datensammlungen und Personendaten, die nicht mehr benötigt werden, zu vernichten sind (unter Vorbehalt einer allfälligen Anbiete-Pflicht gegenüber dem Staatsarchiv, was vorliegend kaum relevant sein dürfte). Das will bedeuten: Auch die öffentliche Hand, welche zwecks Erfüllung einer gesetzlichen Aufgabe Personendaten bearbeitet, darf diese Daten nur solange aufbewahren, als dies für die Erfüllung der Aufgabe notwendig erscheint.

Grundsätzlich handelt es sich bei den Personendaten betreffend die Gästekontrolle in Beherbergungsbetrieben demnach um polizeiliche Daten, welche rein präventiv bearbeitet werden. Dies geht zum Beispiel aus der Formulierung des GWG des Kantons Zug, aber auch aus weiteren Gastwirtschaftsgesetzgebungen hervor. Im Kanton Zug sind die Betreiber von Beherbergungsbetrieben explizit aus „kriminalpolizeilichen Gründen“ verpflichtet, Gästekontrollen zu führen. Auch die Gastwirtschaftsgesetze von anderen Kantonen verlangen dies aufgrund der gleichen ratio legis, beispielsweise der Kanton Luzern, auch wenn dies nicht überall derart ausdrücklich ausformuliert ist. Die Gästekontrolle ist jedenfalls überall zuhanden der Polizei zu führen, so auch im Kanton Uri. Aufgrund dieser ratio legis handelt es sich aus datenschutzrechtlicher Sicht bei den Gästekontrollen eigentlich um polizeiliche Daten im Sinne von Art. 43ff. des Urner Polizeigesetzes (PolG).[47] Für polizeiliche Daten gelten grundsätzlich die Vorschriften des Datenschutzgesetzes, soweit im Polizeigesetz oder in der StPO[48] nichts anderes bestimmt wird. Bezüglich Vernichtung von polizeilichen Daten hält das PolG, in Übereinstimmung mit Art. 13 Abs. 1 DSG fest, dass sie zu vernichten sind, wenn feststeht, dass sie nicht mehr benötigt werden[49], spätestens nach einem Jahr, sofern sie nicht für ein Straf-, Zivil- oder Verwaltungsverfahren benötigt werden[50]. Wollte man an einer ausgedehnteren Aufbewahrungsfrist für die Gästekontrollen festhalten, müsste dies aus datenschutzrechtlicher Sicht ausdrücklich gesetzlich geregelt werden, so wie es zum Teil in gewissen Kantonen in der Gastwirtschaftsgesetzgebung der Fall ist, wo auch Aufbewahrungsfristen von fünf Jahren anzutreffen sind, so z.B. im Kanton

[46] RB 2.2511
[47] RB 3.8111
[48] SR 312.0
[49] Art. 46 lit. a PolG.
[50] Art.46 lit. b PolG.

Luzern.[51] Dies ist jedoch in Uri nicht der Fall. Das Aufbewahren von Personendaten gilt als Bearbeiten von Daten im Sinne von Art. 4 Abs. 1 lit. b DSG. Ein Bearbeiten von Personendaten ist nur gestattet, soweit dafür eine gesetzliche Grundlage besteht oder wenn es zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.[52] Überdies ist der Grundsatz der Verhältnismässigkeit zu beachten, was insofern von Bedeutung ist, als jeder Gast sich zu registrieren hat, ein Umstand, der nach einer kurzen Aufbewahrungsfrist ruft, insbesondere, da es sich dabei auch um sensitive Personendaten handeln kann. Des Weiteren dürfen Personendaten auch nur zu dem Zweck bearbeitet werden, zu welchem sie erhoben wurden. Aus datenschutzrechtlicher Sicht wäre es nicht gestattet, Personendaten, die gestützt auf Art. 9 GWG erhoben wurden, zu andern Zwecken zu verwenden, bzw. aufzubewahren, es sei denn, eine längere Aufbewahrungsfrist stütze sich auf eine andere gesetzliche Grundlage wie z.B. auf eine prozessuale Bestimmung in einem laufenden Verfahren gegen einen betroffenen Gast.

Zusammenfassend kann also gesagt werden, dass bei der jetzigen Rechtslage die Unterlagen der Gästekontrolle ohne anderweitige Erfordernisse nicht länger als ein Jahr aufbewahrt werden dürfen.

6.

Auskunftserteilung einer Einwohnerkontrolle gegenüber der Transportpolizei Schweiz

Die Einwohnerkontrolle einer Gemeinde richtet die Anfrage an die Datenschutzstelle, wie weit der Transportpolizei Schweiz Personalien betreffend eine in dieser Gemeinde wohnhafte Person bekannt gegeben werden dürfen?

Der rechtliche Status der Transportpolizei Schweiz stützt sich auf das BG über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr.[53] Das Gesetz bezieht sich auf die Eisenbahn-, Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen im öffentlichen Verkehr mit einer Konzession zum Personentransport. Die Sicherheitsorgane unterteilen sich in Sicherheitsdienst und Transportpolizei. Die Sicherheitsorgane können u.a. Ausweiskontrollen durchführen oder Personen, die sich vorschriftswidrig verhalten, anhalten. Die Transportpolizei kann überdies angehaltene Personen vorläufig festnehmen sowie Gegenstände beschlagnahmen. Sie verfügt demnach eindeutig über ihr durch Gesetz verliehene polizeiliche Hoheitsfunktionen. Im Bereich der Datenbearbeitung dürfen die Sicherheitsorgane folgende neben anderen Daten

[51] Gastgewerbeverordnung, § 22a (Kanton Luzern, Systematische Gesetzessammlung, 981)
[52] Art. 4 Abs. 1 DSG
[53] BGST; SR 745.2

bearbeiten: Angaben zur Feststellung der Identität einer Person.[54] Den Sicherheitsorganen, insbesondere der Transportpolizei, kommen gestützt auf diese gesetzliche Grundlage eindeutig polizeiliche Hoheitsfunktionen zu, ähnlich wie einer Kantons- oder Gemeindepolizei. Aufgrund dieser gesetzlichen Grundlage steht fest, dass die Einwohnerkontrolle im Einklang auch mit dem kantonalen Datenschutzrecht der Transportpolizei Schweiz die angeforderten Personalien bekannt geben darf und muss.[55].

7.

Bekanntgabe von Personendaten seitens der Kantonspolizei an die KESB

Die KESB ist mit der Fragestellung an die Kantonspolizei herangetreten, wie weit es möglich sei, dass die KESB bei Gefährdungsmeldungen ohne weitere Voraussetzungen an die Polizei gelangen könne, um von dieser Behörde Auskunft zu erhalten, wie weit polizeilich etwas gegen eine betroffene Person vorliegen würde, was in Bezug auf den Kindes- oder Erwachsenenschutz von Belang sein könnte. Zu denken wäre an Fragen des Inhalts, ob von einer betroffenen Person allenfalls eine Gefahr für sich selber oder für Dritte ausgehen könnte oder ob es Hinweise auf häusliche Gewalt gebe. Des Weiteren möchte die KESB wissen, in welcher Form eine solche Anfrage gegenüber der Polizei zu erfolgen hätte. Aus datenschutzrechtlicher Sicht können dazu folgende Überlegungen angestellt werden:

Eingangs ist von der Feststellung auszugehen, dass die Polizei, wie jede andere Behörde, dem Amtsgeheimnis unterliegt, welches grundsätzlich auch zwischen den einzelnen Amtsstellen und Behörden Geltung beansprucht. In Art. 7 Abs. 1 DSG ist u.a. festgehalten, dass Behörden einer anderen Behörde Personendaten bekannt geben dürfen, sofern hierfür eine gesetzliche Ermächtigung oder Verpflichtung besteht oder die Personendaten für die anfragende Behörde zur Erfüllung ihrer gesetzlichen Aufgabe erforderlich sind. Datenschutzrechtlich bildet diese Bestimmung im Zusammenhang mit der von der KESB unterbreiteten Fragestellung die Ausgangslage.

Es finden sich verschiedene gesetzliche Bestimmungen, welche die oben genannten datenschutzrechtlichen Voraussetzungen als dahingehend erfüllt erscheinen lassen, dass eine Behörde, trotz grundsätzlich bestehendem Amtsgeheimnis, Personendaten an die KESB weitergeben darf, zum Teil hierzu gar von Amtes wegen verpflichtet ist. Zu denken wäre einmal an die Bestimmung

[54] Art. 6 Abs. 1 BGST
[55] Art. 7 Abs. 1 lit. a DSG

von Art. 364 StGB[56] [57], welche ganz allgemein Personen, die dem Amtsgeheimnis oder gar einem Berufsgeheimnis im Sinne von Art. 320 oder 321 StGB unterstehen, dazu berechtigt, Meldung an die Kindesschutzbehörden zu machen. Wurde nämlich an einer minderjährigen Person eine strafbare Handlung begangen, so darf die an das Amtsgeheimnis gebundene Person oder Amtsstelle – und damit wäre auch die Polizei mitgemeint -, dies der Kindesschutzbehörde melden, sofern es im Interesse der minderjährigen Person liegt. Einerseits räumt das Gesetz der Amtsstelle ein gewisses Ermessen ein, anderseits ermächtigt das Gesetz die betroffene Behörde zu einer solchen Meldung bereits, wenn «bloss» eine strafbare Handlung vorliegt. Es braucht sich also nicht notwendig um ein Verbrechen oder Vergehen zu handeln. Dennoch darf die Meldung nur erfolgen, wenn eine strafbare Handlung mit einiger Wahrscheinlichkeit bereits begangen wurde, nicht also eine allenfalls strafbare Handlung erst bevorsteht. In der Literatur findet sich auch der Hinweis, dass eine Meldung nur erstattet werden solle, wenn dem Tatopfer dadurch nicht geschadet wird. Es trifft also den Geheimnisträger die Pflicht sorgfältiger Abwägung, wobei in der Literatur zurecht darauf hingewiesen wird, dass diesbezüglich diese Vorschrift nur schwer justiziabel erscheine. Klar erscheint hingegen unter diesem Titel, dass eine solche Meldung nicht an irgendwelche Behörden, sondern nur an die Kindesschutzbehörde - in Uri ist das die KESB - erfolgen dürfe. Vorstellbar erscheint, dass eine solche einschlägige Konstellation im Sinne von Art. 364 StGB am ehesten etwa auf dem Hintergrund häuslicher Gewalt, Kindesmissbrauch oder Kindesmisshandlung in der Verwandtschaft oder durch Dritte, oder wenn unter Umständen erhebliche Indizien in Bezug auf eine andauernde Verletzung der Fürsorge- und Erziehungspflicht im Sinne von Art. 219 StGB vorliegen oder auch im Hinblick auf die ernsthafte Gefährdung weiterer unmündiger Personen, gegeben sein könnte.[58] Art. 364 StGB beschreibt also einen Sachverhalt, ohne dass seitens der KESB eine Anfrage vorliegen würde.

Zur weiteren Diskussion der von der KESB unterbreiteten Fragestellung ist vorauszuschicken, dass die Verfahrensregeln des Erwachsenenschutzes grundsätzlich auch für das Verfahren betreffend den Kindesschutz sinngemäss Anwendung finden[59].

Art. 448 Abs. 4 ZGB hält fest, dass Gerichte und Verwaltungsbehörden unter dem Titel «Mitwirkungspflichten und Amtshilfe» die notwendigen Akten herausgeben, Bericht erstatten und Auskünfte erteilen, soweit nicht

[56] SR 311.0

[57] Art. 364 StGB wurde inzwischen aufgehoben durch Anhang Ziff. 1 des BG vom 15.12.2017, (Kindesschutz) mit Wirkung ab 01.01.2019 (AS 2018 2947; BBl 2015 3431)

[58] vgl. Stefan Trechsel, et al., Schweizerisches Strafgesetzbuch, Praxiskommentar, N 3 zu Art. 364 StGB, Zürich/St. Gallen 2008

[59] Art. 314 Abs. 1 in Verbindung mit Art. 443ff. ZGB; SR 210

schutzwürdige Interessen entgegenstehen. Es ist die bundesrechtliche Rechtsgrundlage für die Amtshilfe im Bereich des Erwachsenenschutzes[60]. Für den einschlägigen Bereich des Kindesschutzes ist in Art. 317 ZGB zusätzlich vorgesehen, dass die Kantone die geeigneten Vorschriften schaffen müssen, um die Zusammenarbeit der Behörden in den Bereichen des zivilrechtlichen Kindesschutzes, des Jugendstrafrechts und der Jugendhilfe zu sichern. Im Kanton Uri ist dies beispielsweise teilweise durch den Erlass von Bestimmungen wie Art. 21 Abs. 2 Sozialhilfegesetz[61] oder Art. 36 Abs. 1 lit. c Gesundheitsgesetz[62] geschehen, wenn auch die letztere Bestimmung eine Meldepflicht von Medizinalpersonen gegenüber den Strafverfolgungsbehörden und nicht direkt gegenüber der KESB beinhaltet. Die gestützt auf Art. 448 Abs. 4 ZGB um Amtshilfe ersuchte Behörde hat allerdings vorgängig zu prüfen, ob private Interessen Dritter oder öffentliche Interessen verletzt werden könnten und eine entsprechende Interessenabwägung vorzunehmen. Unter Umständen hat sie die entsprechenden Schutzvorkehrungen zu treffen (Bot Rev ZGB 2006 7081). Das Gesuch um Amtshilfe sollte deshalb schriftlich erfolgen und mit einer kurzen Begründung versehen sein. Sind jedoch die gesetzlichen Voraussetzungen zur Amtshilfe erfüllt, besteht anlog zur Regelung der Meldepflicht eine Pflicht zur Amtshilfe[63].

Liegt Gefahr im Verzug, Selbstgefährdung einer hilfsbedürftigen Person, d.h. ernst zu nehmende Anzeichen für suizidale Tendenzen, oder besteht die Gefahr, dass eine solche Person ein Verbrechen oder Vergehen gegen Drittpersonen begehen könnte, sodass die Gefahr einer Schädigung von deren körperlichem, geistigem oder materiellem Befinden besteht,[64] sind Amtsgeheimnisträger, und somit auch die Polizei, berechtigt, der KESB von sich aus Meldung zu erstatten. Es liegt ein Rechtfertigungsgrund im Sinne von Art. 14 StGB vor.[65]

Im Weitern sieht Art. 443 ZGB generell ein Melderecht für jedermann vor. Es haben jedoch auch gewisse Meldepflichten in diese Bestimmung Eingang gefunden. Handelt es sich um eine Person in amtlicher Tätigkeit, dann ist sie gar verpflichtet, - also nicht erst auf Anfrage hin – bei starken Indizien, die auf die Hilfsbedürftigkeit einer betroffenen Person hinweisen, bei der KESB Meldung zu erstatten. In der Literatur wird teilweise darauf hingewiesen, dass der Begriff der amtlichen Tätigkeit in diesem Kontext weit zu fassen sei. Darunter sei zu verstehen jede Tätigkeit einer Person, die als Funktion im Dienste der Öffentlichkeit gilt, selbst wenn die betreffende Person nicht in einem rechtlichen

[60] Bot Rev ZGB 2006, 7081
[61] RB 20.3421
[62] RB 30.2111
[63] CHK-D.Steck, Art. 448 ZGB, N 35ff., Handkommentar zum Schweizer Privatrecht, Schulthess, Zürich/Basel/Genf 2012
[64] Art. 453 Abs. 2 ZGB
[65] P. Breitschmid, N 1 – 5 zu Art. 453 ZGB, Handkommentar zum Schweizer Privatrecht, Schulthess 2012

Beamten- oder Anstellungsverhältnis zum Gemeinwesen steht.[66] [67] In Bezug auf die Polizei erscheint es im Lichte dieser Rechtsauffassung ohnehin klar, dass sie unter eine Meldepflicht gegenüber der KESB fällt, auch ohne deren Anfrage, sofern sie ernst zu nehmende Indizien betreffend die Hilfsbedürftigkeit einer Person feststellt. Diese Meldepflicht bedeutet jedoch noch nicht, dass die Polizei von sich aus über alles Bericht erstatten muss, was polizeilich über eine solche Person vorliegt, sofern keine Gefahr von einer solchen Person für Drittpersonen ausgeht und auch keine Indizien für eine Selbstgefährdung gegeben sind oder auch anderweitige Informationen nicht für ein allfälliges Kindes- oder Erwachsenenschutzverfahren relevant erscheinen. Art. 443 Abs. 2 Satz 2 ZGB sieht weiter vor, dass die Kantone darüber hinaus weitere Meldepflichten vorsehen können. Manche Kantone haben von dieser Möglichkeit Gebrauch gemacht, so auch Uri in Art. 25 EG/KESR.[68] Allerdings trifft diese Erweiterung der Meldepflicht die Polizei nicht wirklich, wiederholt doch Art. 25 Abs. 2 EG/KESR in Bezug auf die allgemeinen Amtspersonen lediglich das, was bereits Art. 443 Abs. 2 ZGB vorschreibt. Art. 25 EG/KESR macht, streng besehen, von einer Meldepflichterweiterung lediglich im Hinblick auf ärztliche Medizinalpersonen Gebrauch, soweit es eine allfällige Hilfsbedürftigkeit von Kindern betrifft. Erfasst ist im Grunde nur eine Ausnahmeregelung bezüglich des ärztlichen Berufsgeheimnisses, da Lehrpersonen sowie Schulleiter und Schulleiterinnen bereits aufgrund von Art. 443 ZGB meldepflichtig sind.

Weiter finden sich Meldepflichten gegenüber der KESB, die auch für die Polizei relevant sein können, in Art. 75 Abs. 2 und 3 StPO[69]. Insbesondere Absatz 3 wird diesbezüglich von Belang sein, selbst wenn keine Anfrage seitens der KESB vorliegt. Wer in diesem Zusammenhang als Strafbehörde gilt, die Staatsanwaltschaft oder auch die Polizei, sollte zwischen Staatsanwaltschaft und Polizei abgesprochen werden. Im Lichte der gesetzlichen Systematik kommen beide Instanzen in Frage. Implizit lässt sich Art. 75 StPO auch auf das Jugendstrafverfahren[70] anwenden in Verbindung mit Art. 3 Abs. 1 JStPO, während Art. 31 JStPO im Kanton Uri wohl nur für die Jugendanwaltschaft relevant ist, nachdem diese im Jugendstrafverfahren als Untersuchungsbehörde fungiert.[71]

Zusammenfassend kann aus datenschutzrechtlicher Sicht im Hinblick auf die von der KESB unterbreitete Fragestellung gesagt werden, dass wohl Art. 448 Abs. 4 ZGB sich als die einschlägige gesetzliche Grundlage erweist. Ich verstehe die

[66] Bot Rev ZGB 2006 7076;
[67] Michelle Cottier, Regula Schlauri, FamPra, 2005 760ff.
[68] RB 9.2113
[69] SR 312.0
[70] Art. 3 Abs. 1 JStPO; SR 312.1
[71] Art. 64 Abs. 1 GOG; RB 2.3221

Anfrage dahingehend, dass die KESB, wenn eine Gefährdungsmeldung an sie herangetragen wird und weil sie als Schutzbehörde der Offizialmaxime verpflichtet ist, sich routinehaft an die Polizei wenden und von dieser Auskunft über polizeiliche Vorgänge erhalten möchte, soweit solche im Zusammenhang mit einem Erwachsenen- oder Kindesschutzverfahren als relevant in Betracht fallen. Im Hinblick auf die gesetzlichen Aufgaben, welche der KESB obliegen – ein abgerundetes Bild einer allenfalls hilfsbedürftigen Person zu erhalten – erscheint dieses Anliegen mit Art. 7 Abs. 1 und 2 DSG vereinbar. Art. 453 ZGB lese ich in diesem Zusammenhang mehr in die Richtung, wo es um eine hilfsbedürftige Person geht, bei der zugleich ernst zu nehmende Indizien bestehen, dass Selbst- oder auch Fremdgefährdung ein Thema sein könnten, derart, dass gesetzlich sowohl für die KESB wie für die Polizei eine Zusammenarbeitspflicht besteht, aber auch, selbst wenn keine Anfrage seitens der KESB vorliegt, weil vielleicht dieser Behörde die betroffene Person noch unbekannt ist, die Polizei gestützt auf Absatz 2 dieser Bestimmung ohnehin berechtigt ist, der KESB Meldung zu erstatten.

Aus datenschutzrechtlicher Sicht ist zu empfehlen, dass die Korrespondenz zwischen der KESB einerseits und der Polizei andererseits in schriftlicher Form erfolgt, d.h., dass sowohl die Anfragen seitens der KESB als auch die Antworten seitens der Polizei schriftlich abgewickelt werden. Dies aus der Überlegung, dass bei solchen Konstellationen in der Regel ja ohnehin Dossiers angelegt werden. Vor allem aber auch im Hinblick auf Art. 15 DSG, wo grundsätzlich einer betroffenen Person das Recht eingeräumt wird, unter Vorbehalt entgegenstehender privater oder öffentlicher Interessen Einsicht in die sie betreffenden Personendaten zu nehmen, welche durch die Behörden bearbeitet wurden, verbunden mit der allfälligen Möglichkeit, eine Berichtigung zu verlangen[72].

8.

Bildungs- und Kulturdirektion, Ansprechstelle für Integration; Bekanntgabe von Personendaten an eine andere Behörde

Die bei der Bildungs- und Kulturdirektion angesiedelte Ansprechstelle Integration gelangt mit einer Anfrage betreffend Personendatenbearbeitung in Form von Bekanntgabe von Personendaten an eine andere Behörde im Sinne von Art. 7 Datenschutzgesetz an die Datenschutzstelle.

Art. 53 Abs. 4 AIG[73] schreibt vor, dass die kantonalen Sozialhilfebehörden

[72] Art. 17 DSG

[73] SR 142.20; neu Art. 53 Abs. 5

stellenlose, anerkannte Asylbewerber und vorläufig aufgenommene Personen bei der öffentlichen Arbeitsvermittlung zu melden haben. Gemäss Art. 10a der VO über die Integration von Ausländerinnen und Ausländern (VIntA[74] [75]) regeln die Kantone das Verfahren zur Meldung von stellensuchenden anerkannten Flüchtlingen und vorläufig aufgenommenen Personen. Dabei gilt die Meldepflicht für Personen, die gestützt auf Abklärungen als arbeitsmarktfähig gelten.

Im Kanton Uri wurde nun offenbar dieses Verfahren und die Zuständigkeit so geregelt, dass das SRK im Auftrag der Gesundheits-, Sozial- und Umweltdirektion (GSUD) zuständig ist für die Unterbringung und die wirtschaftliche und persönliche Sozialhilfe von Flüchtlingen und vorläufig aufgenommenen Personen. Des Weiteren ist das SRK im Auftrag der Bildungs- und Kulturdirektion (BKD), wo die Ansprechstelle für Integration angesiedelt ist (Amt für Volksschulen), zuständig für die sprachliche und berufliche Integration von anerkannten Flüchtlingen und vorläufig aufgenommenen Personen.

Unter Bezugnahme auf Art. 32 BG über die Arbeitsvermittlung und den Personalverleih AVG[76] bildet das Amt für Arbeit und Migration das kantonale Arbeitsamt im Sinne des AVG, und hat in dieser Funktion die Vorschriften des AVG zu vollziehen (öffentliche Arbeitsvermittlung etc.)[77].

Die Ansprechstelle unterbreitet der Datenschutzstelle nun die Frage, wie weit aus datenschutzrechtlicher Beurteilung das SRK, das im Auftrag der BKD auch für die sprachliche und berufliche Integration von betroffenen Personen zuständig ist, Personendaten von betroffenen Migranten im Sinne einer Personendatenbekanntgabe an das Amt für Arbeit und Migration, bzw. an das RAV, bearbeiten darf.

Vorliegend handelt es sich also um die Frage der Bekanntgabe von Personendaten an eine andere Behörde. Im Sinne der Legaldefinition von Art. 3 Abs. 1 lit. d DSG[78] gilt das SRK, soweit es sich mit der Unterbringung sowie sprachlichen und beruflichen Integration von Flüchtlingen und vorläufig aufgenommenen Personen befasst, als Behörde im Sinne des Datenschutzgesetzes. Datenschutzrechtlich geht es also um die Frage, wie weit das SRK Personendaten von Personen, welche sich in einem individuellen Integrationsplan befinden, an das RAV als öffentliche Arbeitsvermittlungsstelle weitergeben darf. Gemäss Art. 7 DSG dürfen Personendaten an andere Behörden – auch das Amt für Arbeit und Migration, bzw. das RAV gilt natürlich

[74] SR 142.205
[75] Inzwischen wurde diese Verordnung allerdings revidiert mit Wirkung ab dem 01.01.2019
[76] SR 823.11
[77] Art. 4 Abs. 2 lit. a u. b AMV; RB 20.2311
[78] RB 2.2511

im Sinne des DSG als Behörde – nur weiter gegeben werden, wenn hierzu eine gesetzliche Verpflichtung oder Ermächtigung besteht oder die Personendaten für die Erfüllung einer gesetzlichen Aufgabe erforderlich sind oder allenfalls, wenn es im Interesse einer betroffenen Person liegt und diese ausdrücklich zugestimmt hat oder wenn sie verhindert ist, ihre Zustimmung vorausgesetzt werden darf. Diese gesetzliche Verpflichtung scheint gestützt auf Art. 53 Abs. 6 AIG[79] und Art. 10a Abs. 2 VIntA[80] vorzuliegen.

Gemäss Art. 33a AVG sind die mit der Durchführung dieses Gesetzes betrauten Organe befugt, Personendaten und Persönlichkeitsprofile zu bearbeiten oder bearbeiten zu lassen, die sie benötigen**,** um die ihnen übertragenen Aufgaben zu erfüllen, namentlich um:

Stellensuchende zu erfassen, zu vermitteln und zu beraten;

Offene Stellen zu erfassen, bekanntzugeben oder zuzuweisen; (…).

Besonders schützenswerte Personendaten dürfen bearbeitet werden:

Über die Gesundheit und die Religionszugehörigkeit der Stellensuchenden, wenn diese Daten für die Vermittlung erforderlich sind (…)[81].

Im derzeit noch geltenden Urner Datenschutzgesetz zwar nicht explizit als Voraussetzung ausformuliert,[82] wird im BG über den Datenschutz, aber auch in andern kantonalen Gesetzgebungen und in der Lehre überwiegend verlangt, dass die Bearbeitung von besonders schützenswerten Personendaten und Personenprofilen sich auf ein Gesetz im formellen Sinne abstützen muss, eine Voraussetzung, die mit den vorliegenden Gesetzesbestimmungen des AVG als erfüllt betrachtet werden darf.

Die Arbeitsvermittlung bedingt die Zusammenarbeit diverser Behörden und Organe. Damit wird erforderlich, dass Personendaten ausgetauscht werden. Völlig unabhängig vom Umstand, ob es sich bei den Stellensuchenden um Inländer, Ausländer oder Personen mit dem Status eines anerkannten Flüchtlings oder einer vorläufig aufgenommenen Person handelt, umfassen solche Daten teilweise Informationen über Alter, Ausbildung, berufliche Laufbahn, Familienverhältnisse, teilweise gar, sofern wirklich notwendig, bis hin zu medizinischen Gutachten. Solche Daten beinhalten Informationen direkt die Persönlichkeit der Stellensuchenden betreffend, weshalb dem Datenschutz eine nicht unerhebliche Bedeutung zukommt[83]

[79] neu Art. 53 Abs. 5 AIG
[80] neu Art. 9 VIntA
[81] Art. 33a Abs. 2 AVG
[82] Vgl. Art. 4 DSG Uri
[83] Vgl. Eva-Maria Bäni, Arbeitsvermittlungsgesetz, Artikelkommentar zu Art. 33a AVG, Stämpfli-Verlag 2014

Grundsätzlich hält Art. 33a Abs. 1 AVG in allgemeiner Form fest, welche Stellen oder Organe zu welchem Zweck zur Personendatenbearbeitung befugt sind. Durch die Zweckbindung und gestützt auf das Verhältnismässigkeitsprinzip beschränkt das allgemeine formelle Datenschutzrecht,[84] aber auch das vorliegend materielle Datenschutzrecht[85] die Erhebung und Bearbeitung von Personendaten auf das, was zur Erfüllung der gesetzlichen Aufgaben, insbesondere der Arbeitsvermittlung, zwingend erforderlich ist. Dabei soll der Datenschutz, bzw. der Schutz der Persönlichkeit möglichst gewährleistet bleiben, anderseits soll laut Gesetz eine Optimierung der Arbeitsvermittlung durch institutionelle Zusammenarbeit angestrebt werden können. Darauf weist das Gesetz nicht zuletzt durch die Formulierung hin, dass die mit dem Vollzug dieses Gesetzes betrauten Organe befugt sind, die Personendaten zu bearbeiten oder auch allenfalls bearbeiten zu lassen.

Aus Art. 33a AVG ergibt sich jedenfalls, dass auch die öffentliche Arbeitsvermittlungsstelle, das heisst das Amt für Arbeit und Migration, bzw. das RAV, dem DSG und somit an die Einhaltung der tragenden datenschutzrechtlichen Grundsätze, wie sie auch in das Urner Datenschutzgesetz Eingang fanden, gebunden sind.

Konkret bedeutet dies, dass Begriffe wie Personendaten,[86] Zweckbindung und Verhältnismässigkeit,[87] besonders schützenswerte Personendaten,[88] gemäss den datenschutzrechtlichen Grundsätzen zu handhaben sind. Wie bereits erwähnt, wird für die Bearbeitung besonders schützenswerter Personendaten in der Lehre, in vielen kantonalen Datenschutzgesetzgebungen und auch im BG über den Schutz von Personendaten eine formelle gesetzliche Grundlage verlangt. Im derzeit noch geltenden Urner Datenschutzrecht ist dieser Grundsatz zwar nicht ausdrücklich erwähnt, wird aber in der Praxis anerkannt. Im Hinblick auf die Datenbearbeitung im Zusammenhang mit der öffentlichen Arbeitsvermittlung ist diese formelle gesetzliche Grundlage jedoch mit Art. 33a Abs. 2 AVG eindeutig gegeben. Gleichzeitig wird gerade durch diese gesetzliche Grundlage die Bearbeitung besonders schützenswerter Personendaten auch wieder eingeschränkt. Daten über Gesundheit oder Religionszugehörigkeit dürfen gemäss dieser gesetzlichen Grundlage zwar bearbeitet werden, aber nur, sofern diese Daten für die Vermittlung notwendig sind[89]. Überdies sind die Arbeitsvermittlungsbehörden befugt, Daten über verfügte oder vorgesehene AVIG-Massnahmen zu bearbeiten, sofern diese Daten direkt die Leistungen der

[84] Art. 4 Abs. 3 DSG
[85] Art. 33a AVG
[86] Art. 3 Abs. 1 lit. a DSG
[87] Art. 4 DSG UR; Art. 33a Abs. 1 lit. a – f AVG
[88] Art. 3 Abs. 1 lit. f DSG UR
[89] Art. 33a Abs. 2 lit. a AVG

ALV beeinflussen können.[90]

Aus dem Gesundheitszustand können sich Einschränkungen für die Arbeitsvermittlung ergeben. Es kann z.B. etwa ein bestehendes Rückenleiden einer stellensuchenden Person Probleme in bestimmten Arbeitsbereichen verursachen, z.B. auf dem Bau oder bei manchen Arbeitsstellen, wo erhebliche Lasten von Hand bewegt werden müssen. Ähnliches kann für die Religionszugehörigkeit gelten, sofern sich aufgrund dieser Bekleidungsvorschriften ergeben, die mit Sicherheitsvorschriften in einem bestimmten Einsatzbetrieb kollidieren können. Daraus ergibt sich, dass eine erfolgreiche Arbeitsvermittlung auf die Erfassung und Kenntnisnahme solcher Informationen angewiesen ist.[91]

Auch aufgrund des Verhältnismässigkeitsprinzips steht die Bearbeitung von sensiblen Personendaten unter der Bedingung der notwendigen Erforderlichkeit für die Vermittlung. Das Verhältnismässigkeitsprinzip besagt in dem vorliegenden Kontext, dass solche sensible Informationen «unbedingt» für eine erfolgreiche Vermittlung notwendig sein müssen.[92] Die Zweckbindung für solche Personendaten bedeutet, dass die Bearbeitung ausschliesslich nur für diesen Zweck, also im Hinblick auf eine erfolgreiche Vermittlung, bearbeitet werden dürfen. Auch obliegt den Arbeitsvermittlungsbehörden die Pflicht, für die Richtigkeit solcher Daten zu sorgen, bzw. diese auf ihre Richtigkeit hin zu überprüfen.

Zusammengefasst kann gesagt werden, dass die Informationen, welche in diesen Integrationsplänen enthalten sind, den Arbeitsvermittlungsbehörden aus datenschutzrechtlicher Sicht bekannt gegeben werden dürfen. Die Arbeitsvermittlungsbehörden vermögen aufgrund ihrer fachlichen Kompetenz am ehesten zu beurteilen, welche Informationen für eine anstehende erfolgreiche Vermittlung Relevanz aufweisen können. Die Arbeitsvermittlungsbehörden unterliegen ihrerseits selbstverständlich auch dem Datenschutzrecht und dürfen eine Weiterbearbeitung dieser Daten nur ins Auge fassen, soweit dies für eine erfolgreiche Arbeitsvermittlung als notwendig erscheint**.** Diese Voraussetzungen zu beurteilen fällt naturgemäss von der Sache her den Arbeitsvermittlungsbehörden leichter als dem SRK.

Finden sich allerdings in diesen Integrationsplänen Personendaten, die für jeden Laien ersichtlich im Hinblick auf ein künftiges Arbeitsverhältnis absolut keine Relevanz aufweisen, dann brauchen davon auch die Arbeitsvermittlungsbehörden keine Kenntnis zu haben. Zu denken wäre etwa an

[90] Art. 33a Abs. 2 lit. b AVG
[91] vgl. Staatssekretariat SECO, Weisungen u. Erläuterungen zum Arbeitsvermittlungsgesetz, 173
[92] Weisung SECO 173; sinngemäss auch BGE 131 II 413, E. 2.5

Informationen, die gewisse innerfamiliäre Belange betreffen, schulische Belange der Kinder oder etwa abgeschlossene medizinische Behandlungen, welche für das künftige berufliche Fortkommen keine Bedeutung aufweisen. In solchen Fällen, von denen es natürlich keine abschliessende Erwähnung geben kann, braucht der Personendatenfluss gegenüber der Arbeitsvermittlung nicht zu erfolgen. Stellen sich Grenzfälle ein, wo man sich wirklich nicht sicher ist, ob die Informationen für die Vermittlung eine Relevanz aufweisen, empfiehlt es sich, es der stellensuchenden Person zu überlassen, ob sie die Information an die Vermittlungsbehörden weitergeben will.

Grundsätzlich ist aus Sicht des Datenschutzes jedoch festzuhalten, dass Art. 33a AVG für anerkannte Flüchtlinge und vorläufig aufgenommene Personen die gleiche Bedeutung aufweist wie für andere Stellensuchende.

9.

Auskünfte von Schulsekretariaten an Dritte für allfällig geschäftliche Zwecke

Das Schulsekretariat einer Gemeinde gelangt mit der Anfrage an die Datenschutzstelle, wie weit es einer Bank, die gerne die Klassen-Adresslisten der Schülerschaft für Werbe- oder Geschäftszwecke zur Verfügung hätte, die Listen aushändigen dürfe.

Die Anfrage betrifft Art. 8 des Datenschutzgesetzes des Kantons Uri[93]. Vorausgeschickt sei, dass ein Schulsekretariat im Sinne der Legaldefinition von Art. 3 Abs. 1 lit. d DSG als Behörde gilt. Das bedeutet konkret, dass die Tätigkeit bei dieser Amtsstelle, soweit diese ein Bearbeiten von Personendaten betrifft, im Sinne von Art. 2 Abs. 1 DSG von den Bestimmungen der Datenschutzgesetzgebung erfasst wird, bzw. diesem Gesetz untersteht.

Wenn nun eine Bank an das Schulsekretariat einer Gemeinde gelangt mit der Bitte, ihr die Klassen-Adresslisten zuzustellen, so stellt sich die Frage, ob in diesem Sinne die entsprechenden Personendaten bearbeitet werden dürfen. Bearbeiten von Personendaten bedeutet auch das Bekanntgeben von Personendaten an eine andere Behörde oder an Privatpersonen.

Eine Antwort findet sich unter der Bestimmung von Art. 8 DSG: Personendaten dürfen an Private nur bekanntgegeben werden, wenn hierzu eine gesetzliche Verpflichtung oder Ermächtigung besteht oder es zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder es im Interesse der betroffenen Person liegt und diese ausdrücklich zugestimmt hat….

Diese Voraussetzungen sind vorliegend eindeutig nicht erfüllt. Auch ist keine

[93] RB 2.2511

Bestimmung in der kantonalen Schulgesetzgebung bekannt, welche die Behörden ermächtigen oder verpflichten würde, einer (juristischen) Privatperson, wie es eine Bank ist, Personendaten aus dem Schulbereich herauszugeben. Und zur Erfüllung einer gesetzlichen Aufgabe ist es vorliegend auch nicht erforderlich. Werbeinteressen von Banken oder anderen Firmen haben mit den gesetzlichen Aufgaben, denen sich die Schulbehörden widmen, keinen Zusammenhang.

Eine Mitteilung von Klassen-Adresslisten an eine private Person wie eine Bank würde überdies auch aus systematischen Überlegungen quer in der Gesetzeslandschaft liegen, weil auch den Einwohnerkontrollen die Erteilung von Auskünften über Personen gegenüber Dritten zu geschäftlichen Zwecken ausdrücklich untersagt ist.[94] Selbstredend gilt dies natürlich auch in Bezug auf Personen, die nicht die schweizerische Staatsbürgerschaft besitzen.

Die weitere Frage, welche das Schulsekretariat unterbreitet, betrifft gleichlautende Anfragen von Vereinen. Vereine wie Jugend- und Sportvereine verfolgen in der Regel nicht einen kommerziellen, sondern einen ideellen Zweck und leisten gerade im Hinblick auf eine sinnvolle Freizeitgestaltung von Jugendlichen äusserst wertvolle Arbeit. Es gibt Kantone, z.B. Zürich, wo die Auskunftserteilung bei den Einwohnerkontrollen ausdrücklich so geregelt ist, dass Daten von mehreren Personen nach bestimmten Kriterien geordnet praktisch ohne Begründung seitens einer Gesuchstellerin bekannt gegeben werden dürfen, unter der Bedingung, dass sie für einen ausschliesslich ideellen Zweck verwendet und nicht weiter gegeben werden[95]. Der Kanton Uri kennt keine derartige ausdrückliche Bestimmung. In Art. 12 Abs. 4 Gesetz über Aufenthalt und Niederlassung heisst es lediglich, dass Dritten Auskünfte in beschränktem Masse erteilt werden dürfen, soweit ein berechtigtes Interesse nachgewiesen wird. Und diese Bestimmung ist auf die Einwohnerkontrolle zugeschnitten, nicht auf den eigentlichen Schulbereich.

Allein gestützt auf Art. 8 DSG können Adresslisten von Klassen auch an Vereine nicht ausgehändigt werden. Anderseits erscheint es natürlich als verständlich und naheliegend, dass Vereine irgendwie darauf angewiesen sind, dass sie einen Weg zu den Jugendlichen finden, damit sie ihren Nachwuchs rekrutieren können. Und was liegt da näher, als eine Klassenliste eines bestimmten Jahrgangs zur Verfügung zu haben?

Damit die Schulsekretariate datenschutzrechtlich auf der sicheren Seite sind, würde ich den Schulbehörden folgendes Vorgehen vorschlagen: Die Behörden machen den Vereinen das Angebot, dass diese Werbeschreiben der Schule

[94] Art. 12 Abs. 4 Gesetz über die Niederlassung und den Aufenthalt der Schweizer; RB 1.4211
[95] Gesetz über das Meldewesen und die Einwohnerregister, Art. 19, Zürcher Gesetzessammlung 142.1

(beispielsweise den Schulleitungen und Lehrkräften, die jene Jahrgänge unterrichten, welche das Zielsegment der Jugendlichen bilden) zustellen, die dann in der Klasse von den Lehrpersonen an die Schülerinnen und Schüler abgegeben werden. Oder vielleicht lässt man einmal eine Vertreterin, einen Vertreter eines Jugend- oder Sportvereins in der Klasse auftreten, um den Verein den Jugendlichen kurz vorzustellen und Werbematerial abzugeben. Nicht gelten diese Vorschläge jedoch für Institutionen, die, wie eine Bank, einen kommerziellen Zweck verfolgen.

10.

Bekanntgabe von Personendaten seitens der KESB an eine Hochschule, Fachbereich soziale Arbeit, zwecks Durchführung eines Forschungsprojekts

Die Hochschule Luzern, Fachbereich soziale Arbeit, will ein Forschungsprojekt lancieren, welches sich mit der Thematik «Fürsorgepraxis bei Kindesvernachlässigung» befasst. Die Hochschule gelangt an die Kindes- u. Erwachsenenschutzbehörden von verschiedenen Kantonen, u.a. auch an die KESB Uri. In diesem Zusammenhang gelangt eine Dozentin der Hochschule mit dem Anliegen an die KESB, vertrauliche Einsicht in einzelne Dossiers zu nehmen, die das Thema «Kindesvernachlässigung» beinhalten. Innerhalb dieses Projektes ist vorgesehen, Einsichtnahme in Dossiers zu nehmen, die einerseits im Zeitraum 2009/2010 und anderseits im Zeitraum 2018/2019 erstellt wurden. Ziel der Forschungsarbeit bildet offenbar die Untersuchung des Begriffes «Kindesvernachlässigung», bzw. dessen Einbettung in die historische Entwicklung der normativen Handhabung dieses Begriffes. In diesem Zusammenhang ist für die Forschungsarbeit von Interesse die historische und aktuelle Rekonstruktion von bezogen auf diese Thematik sich ereignenden Diskursen zu Themen wie Familie, Erziehung und Mutterschaft, soweit sie Relevanz für den normativen Begriff der «Kindesvernachlässigung» aufweisen. Ebenso von Interesse erscheint der Einfluss des Wandels von kontextbezogenen sozialen Wertvorstellungen auf die Fürsorgepraxis. Untersuchungsthemata bilden nicht narrative Einzelschicksale, als vielmehr sich ereignende Prozessabläufe, die aus solchen Reihenuntersuchungen sich allenfalls ableitenden Regelhaftigkeiten und allenfalls ein sich daraus ergebender Wissensgewinn, welcher verallgemeinerungsfähiges Potential für künftige Prozessabläufe bereitstellt.

Weitere Bestandteile dieses besagten Forschungskonzepts bilden Interviews mit Fachpersonen und mit Bezugspersonen, die in die zu untersuchenden Prozesse

involviert sind oder waren.

Das Forschungsprojekt bildet Teil eines nationalen Forschungsprogramms (NFP 76), wird vom Schweizerischen Nationalfond finanziert und begleitet, vom SVAM befürwortet und wurde von einer externen Ethikkommission unter ethischen Aspekten beurteilt.

Die gesetzliche Grundlage für die Durchführung eines solchen Forschungsprojektes findet sich im BG über die Förderung der Forschung und der Innovation (FIFG)[96]; insbesondere in dessen Zweckbestimmung, (Art. 1), in dessen Legaldefinition (Art. 2 lit. a Ziff. 2), Geltungsbereich (Art. 3) und Forschungsorgane (Art. 4).

Aus der methodologischen Anlage des vorgesehenen Forschungsprojektes ergibt sich, dass die Durchführung des Projekts die Einsichtnahmen in Falldossiers als unumgänglich erscheinen lässt. Insofern gilt die Voraussetzung für die Bekanntgabe von Personendaten im Sinne von Art. 7 DSG[97] als erfüllt. Die Projektleitung als Vertretung der Hochschule Luzern gilt im Sinne des DSG als Behörde.[98]

Einerseits handelt es sich bei Personendaten, welche die KESB, bzw. vormals die Vormundschaftsbehörden im Zusammenhang mit dem Thema «Kindesvernachlässigung» zu bearbeiten hatten, immer um besonders schützenswerte Personendaten im Sinne von Art. 3 Abs. 1 lit. f DSG. Bei besonders schützenswerten Personendaten steht immer auch eine intensive Gefährdung des Persönlichkeitsschutzes zur Debatte, derart, dass deren Bearbeitung nur gestützt auf eine gesetzliche Grundlage und unter besonderen Vorkehren erfolgen darf. Auf der anderen Seite präsentiert die Hochschule Luzern ein Forschungsziel, welches im Interesse der Öffentlichkeit und auch im Interesse der Erfüllung der künftigen gesetzlichen Aufgaben durch Eltern, durch die KESB und durch weitere Instanzen, denen pädagogische Aufgaben obliegen, steht.

Im Fokus dieser Thematik steht in diesem Zusammenhang Art. 10 DSG. Personendaten dürfen für nicht personenbezogene Zwecke - dies ist vorliegend gemäss Forschungsanlage der Fall, da Prozessabläufe, nicht aber biographische Narrative im Mittelpunkt stehen - insbesondere für Forschung…..bearbeitet werden, wenn sie anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt und die Ergebnisse so veröffentlicht werden, dass keinerlei Rückschlüsse auf direkt oder indirekt betroffene Personen möglich sind. Für die Durchführung des Projekts ist angesichts dieser besonders schützenswerten Personendaten

[96] SR 420.1
[97] RB 2.2511
[98] Art. 3 Abs. 1 lit. d DSG

und Art. 451 ZGB[99] folgendes Vorgehen zu empfehlen:

. Den am Projekt beteiligten Personen werden nur solche Dossiers unterbreitet, die inhaltlich auch wirklich einen klaren Bezug zum Thema des Forschungsprojektes aufweisen, d.h., wo es um die Frage der Kindesvernachlässigung ging oder geht.

. Es wird in einer gegenseitigen Vereinbarung klar definiert, welche Personen Einblick in nicht anonymisierte Personendaten erhalten. Jegliche Weitergabe an Drittpersonen, auch innerhalb der Hochschule, ist untersagt.

. Es ist zwischen der KESB und dem Projektteam zu vereinbaren, in welcher Form die Einsicht erfolgt (in Räumen der Amtsstelle? Allfällige Kopien? etc.)

. Die am Forschungsprojekt beteiligten Personen erheben Personendaten in nicht anonymisierter Form nur so weit, als dies sich für die Erreichung des Forschungszieles als zwingend notwendig erweist.

. Die an der Forschungsarbeit beteiligten Personen verpflichten sich gegenüber der KESB, sämtliche verwendeten Datenträger (in Papier- oder digitaler Form), die Personendaten enthalten, derart zu sichern, dass keine unbefugten Personen Zugriff zu diesen Personendaten erhalten.

. Die an der Forschungsarbeit beteiligten Personen verpflichten sich gegenüber der KESB, sämtliche im Zusammenhang mit dieser Forschungsarbeit erhobenen Personendaten auf allen Arten von Datenträgern zu löschen, bzw. zu vernichten, sobald es der Fortgang der Forschungsarbeit erlaubt.

. Die an der Forschungsarbeit beteiligten Personen verpflichten sich gegenüber der KESB, keine der erhobenen Personendaten für einen andern Zweck zu verwenden als für das im vorliegenden Forschungsprojekt umschriebene Forschungsziel.

. Die am Forschungsprojekt beteiligten Personen verpflichten sich gegenüber der KESB, die Forschungsarbeit in einer Form zu publizieren, die keinerlei Rückschlüsse auf betroffene Personen zulässt.

. Wenn die KESB dem Anliegen der Beteiligten am Forschungsprojekt nachkommt und involvierte Personen für ein Interview mit den Forschenden vermittelt, empfiehlt es sich, dass vorgängig gegenüber den Betroffenen eine klare Instruktion erfolgt betreffend Inhalt und Zweck der Projekts, der Freiwilligkeit des Interviews, der Wahrung der Anonymität etc., derart, dass die befragten Personen genau wissen, zu was sie die Zustimmung erteilen.

[99] SR 210

11.

Installation von Video-Kameras in Abstandszellen der Polizei

In den Abstands-Zellen auf den Werkhöfen und in der Ankenwaage wurden durch die Kantonspolizei Video-Überwachungsanlagen installiert. Grundsätzlich kommt für diesen Sachverhalt einerseits das PolG[100], anderseits das kantonale Datenschutzgesetz[101] zur Anwendung. In Bezug auf polizeiliche Personendaten kommt das Datenschutzgesetz subsidiär zur Anwendung. Finden sich also im Polizeigesetz und in der Schweizerischen Strafprozessordnung keine speziellen Bestimmungen, gelangt das DSG und dessen Grundätze zur Anwendung. Der Strafprozessordnung lassen sich sachverhaltsbezogen keine einschlägigen Bestimmungen entnehmen, die für diese Frage als lex specialis gelten würden. In Art. 44 PolG ist festgehalten, dass die Kantonspolizei Daten bearbeiten und Datenbearbeitungssysteme aufbauen kann, soweit dies als notwendig und zweckmässig erscheint, um ihre Aufgaben zu erfüllen. Diese Bestimmung reicht jedoch nicht aus, um eine Abstands-Zelle mittels einer Videoüberwachungsanlage durchgehend überwachen zu lassen. Gemäss derzeit geltendem kantonalem Recht kommt diesbezüglich sehr wohl das DSG im Grundsatze zur Anwendung.

In Art. 4 DSG sind die wichtigsten Grundsätze festgehalten, denen nachgelebt werden muss, wenn seitens der Behörden Personendaten bearbeitet werden. Das Überwachen einer Person in einem Raum/Abstandszelle mittels einer Video-Überwachungsanlage ist eine klassische Art einer Bearbeitung von Personendaten und stellt einen massiven Eingriff in die persönliche Integrität einer betroffenen Person dar. Es handelt sich im Übrigen um eine Art von Personendatenbearbeitung, wo sehr rasch auch besonders schützenswerte Personendaten im Sinne von Art. 3 Abs. 1 lit. f DSG berührt sein können. Besonders schützenswerte Personendaten dürfen durch Behörden nur bearbeitet werden, wenn dafür entweder eine gesetzliche Grundlage besteht oder das Bearbeiten von Personendaten für die Erfüllung einer gesetzlichen Aufgabe auch wirklich als notwendig erscheint. Dabei darf Art. 4 Abs. 1 lit. b nicht allzu extensiv ausgelegt werden, denn der Grundsatz der Verhältnismässigkeit verlangt, dass eine Bearbeitung nur im Rahmen der Notwendigkeit und der Geeignetheit für die Erfüllung einer gesetzlichen Aufgabe erfolgen darf. Gemäss polizeilicher Darstellung sind alle vier Zellen im Werkhof Göschenen von einer durchgängigen Video-Überwachung betroffen. Aus datenschutzrechtlicher Sicht bestehen ganz erhebliche Zweifel, ob mit einer durchgehenden Videoüberwachung aller dieser Zellen, im Hinblick auf alle Personen, die vorübergehend darin festgehlten werden und sich dort aufhalten, einerseits das

[100] RB 3.8111
[101] RB 2.2511

notwendige Erfordernis für die Erfüllung einer polizeilichen Aufgabe beachtet wird und anderseits dem Verhältnismässigkeitsprinzip nachgelebt wird. Ist dem aber nicht so, dann erweist sich eine durchgehende Überwachung als klar rechtswidrig.

Es bleiben in diesem Zusammenhang verschiedenste Fragen offen. So müsste etwa in folgenden Punkten Klarheit bestehen: In welchem Ausmass werden diese Zellen benutzt? Welche Zwecke mit der Benutzung einer Abstandszelle werden verfolgt? Das können wahrscheinlich sehr verschiedene sein? In welchen Situationen erweist sich allenfalls eine durchgehende Überwachung als notwendig? (Zu denken wäre an eine Situation, wo eine in einer Zelle festgehaltene Person unter suizidaler Gefährdung leidet?) Wie sind die Zellen räumlich ausgestaltet und welche räumlichen Teile einer Zelle liegen im Fokus der Videokamera? Welche Personen sollen oder müssen, wenn sie sich in der Zelle befinden, überwacht werden? Wann ist die Überwachungsanlage aktiviert? Wie findet die Information der betroffenen Personen betreffend die Überwachung statt? Wie gestaltet sich eine Auswertung einer allfälligen Überwachung? Handelt es sich um eine Echt-Zeit-Auswertung? Wann und unter welchen Voraussetzungen erfolgt eine Speicherung der Video-Daten? Unter welchen Voraussetzungen und durch wen darf eine nachträgliche Auswertung stattfinden? Nach welchem Zeitablauf muss eine Löschung der Daten erfolgen? Welche technischen/organisatorischen Massnahmen sind vorgesehen, um eine unbefugte Bearbeitung und Auswertung zu verhindern? Gibt es einen Situationsplan betreffend die Standorte der Kameras und der räumlichen Fokusbereiche? Bestehen Massnahmen, die die Wirksamkeit überprüfen, um den gesetzlich zulässigen Rahmen abzugrenzen?

Aus datenschutzrechtlicher Sicht müsste in Bezug auf solche Fragen Klarheit bestehen, damit eine Überwachung als rechtmässig angesehen werden kann. Eine generelle durchgehende Überwachung a priori aller Personen, die in einer Abstandszelle untergebracht sind, liesse sich datenschutzrechtlich nicht legitimieren.

Gestützt auf Art. 22 Abs. 2 lit. c DSG sollte die Datenschutzstelle vor der Installation vorgängig konsultiert werden, gehört es doch zum Aufgabenbereich der Aufsichtsperson, Stellung zu nehmen zu Massnahmen, auch technischer und organisatorischer Art, die für den Datenschutz von erheblicher Relevanz sind.

12.

Das Swisscom-Projekt «Schulen ans Internet»

Die Swisscom unterbreitet den Schulen im Rahmen der Initiative «Schulen ans Internet» eine Lösung, die einen sicheren Zugang ins Internet gewährleisten soll. Jugendlichen soll innerhalb des Schulbetriebes der Zugriff auf relevante Inhalte zum Schutz der Jugend, die von den Schulen und Kantonen vorgängig festgelegt werden, verwehrt werden. Swisscom macht geltend, dass bei der von ihr entwickelten Lösung dem Anliegen des Jugendmedienschutzes, dem Schutz vor gefährlichen Inhalten und dem Datenschutz Genüge getan werde. Die sich aufdrängende Frage dabei ist, dass Swisscom, um die Filterung sicherzustellen, einerseits ein Subunternehmen beizieht, anderseits den verschlüsselten Datenverkehr aufbricht, sodass die entschlüsselten Daten Dritten zugänglich werden. Unter der Voraussetzung, dass die Schülerschaft nicht mit eigenen Geräten arbeitet, sondern mit solchen, die der Schule gehören, die also nur im schulischen Bereich eingesetzt werden, sind im Zusammenhang mit dem Angebot der Swisscom-Dienstleistung folgende Angaben, aber auch Zusicherungen, von Bedeutung und folgende Punkte zu beachten:

- Zscaler (das beigezogene Subunternehmen) hat seinen Sitz in den USA, wo kein ebenbürtiges Datenschutzniveau herrscht wie im EU-Raum oder in der Schweiz, was zweifelsohne ein gewisses Risiko beinhaltet.

- Zscaler als Subunternehmen sichert gegenüber der Swisscom die Einhaltung der in der Schweiz geltenden gesetzlichen Vorgaben zum Datenschutz sowie der Vorgaben, welche der EDÖB machte, zu. Diese vertragliche Zusage gegenüber Swisscom durch das Subunternehmen trägt zu einer gewissen Risikominderung bei.

- Zscaler ist dem SWISS-U.S.Privacy Shield Framework beigetreten. Auch dieser Umstand trägt zu einer Risikominderung bei.

- Swisscom bestätigt und stellt sicher, dass alle anwendbaren gesetzlichen Verpflichtungen auch auf das Subunternehmen Zscaler übertragen werden.

- Um den Zugang zum Internet in der Schule gemäss jugendrechtlichen Kriterien sicherzustellen, wird die Übertragungsverschlüsselung aufgebrochen (SSL Inspection).

- Nach einer Überprüfung durch Proxy wird mittels zertifizierter Technologie die Verschlüsselung wieder vollzogen.

- Es erfolgt diese SSL-Inspection nur im Zuge einer ausdrücklichen Einwilligung seitens der jeweils betroffenen Kantone.

- Dem Kanton steht die Möglichkeit offen – dies scheint wichtig – Listen von URL-

Zugängen zu erstellen, wo die URL-Verschlüsselung nicht aufgebrochen wird, also keine SSL-Inspection stattfindet (Whitelists). Damit wird ein Prozess implementiert, der es den Schulen/Kantonen ermöglicht, Listen von Websites festzulegen, wo durch Zscaler keine Entschlüsselung vorgenommen wird.

- Unter datenschutzrechtlichen Aspekten ist von besonderer Bedeutung, dass Swisscom, bzw. das involvierte Subunternehmen Zscaler nicht die Person, also den konkreten User identifiziert, auch wenn dies theoretisch schulintern offenbar dennoch möglich wäre (Überprüfbarkeit bestimmter User zu einem bestimmten Zeitpunkt).

- Unter datenschutzrechtlichen Aspekten erscheint auch als sehr wichtig: Es wird vertraglich zugesichert, dass Zugriffe auf Log-Daten ausschliesslich zu Zwecken der Service-Erbringung durch das Subunternehmen erfolgen. Und mindestens ebenso wichtig: Es wird garantiert, dass diese Zugriffe in einem Audit-Log überprüfbar protokolliert werden.

- Ganz entscheidend auch: Es wird ein nachprüfbares Berechtigungskonzept erstellt. Die jeweiligen Administratoren und Administratorinnen werden autorisiert, also in der Person definiert. Nur ganz bestimmte Leute werden als Administratorinnen/Administratoren zugelassen. Diese werden sorgfältig ausgewählt und haben in regelmässigen Abständen Schulungen zu absolvieren und Auszüge aus Straf- und Betreibungsregister beizubringen.

- Ganz wichtig aus datenschutzrechtlichen Überlegungen auch: Die Inhalte der aufgebrochenen HTTP- und HTTPS-Verbindungen werden nicht gespeichert. Es werden nur Proxys eingesetzt, die selber über keinen physischen Speicherplatz verfügen.

Am Log-Server werden nachfolgende Daten gespeichert:

- IP-Adresse, von welcher der Internet-Zugriff erfolgte; Zeitpunkt des Zugriffs; anvisierte URL-Adresse; als Metadaten URL-Kategorie, Browserversion sowie der Entscheid gemäss den Filterregeln «erlaubt/blockiert».

- Den jeweiligen Kantonen steht die Möglichkeit offen, in Form von Listen festzulegen, welche Inhaltskategorien und URLs von einer Filterung ausgenommen werden sollen, und ebenso ganz wichtig, die Möglichkeit, ein selbst gewähltes Zertifikat für die Entschlüsselung einzusetzen.

Aufgrund dieser Zusicherungen erscheint es aus datenschutzrechtlichen Überlegungen vertretbar, wenn die Bildungs- und Kulturdirektion, Amt für Volksschulen, sich an diesem Projekt beteiligt.

Unabdingbare Voraussetzung, dass diesem Projekt zugestimmt werden kann, bildet allerdings die Verpflichtung, dass sowohl die Schülerschaft als auch alle

Lehrpersonen, welche im Schulbereich für die Nutzung des Internets unter den oben erwähnten Rahmenbedingungen in Frage kommen, eingehend informiert werden, sodass sie wissen, dass die Verschlüsselung ihrer gewählten Internet-Verbindungen unter Umständen aufgebrochen und überprüft werden.

Da es im Grunde die gesetzliche Aufgabe einer Schule darstellt, innerhalb des Schulbetriebes und im Zusammenhang mit dem Unterricht dafür besorgt zu sein, dass seitens der Schülerschaft keine unrechtmässigen Internet-Zugriffe erfolgen, handelt es sich beim vorliegenden Projekt, bzw. bei der Filtrierung der Internet-Verbindungen durch die Swisscom, um eine Auftragsdatenbearbeitung durch die Swisscom, wobei die Swisscom diese Auftragsdatenbearbeitung mit Hilfe eines Subunternehmens, der Firma Zscaler, wahrnimmt. Mit andern Worten: Es wird eine gesetzliche Aufgabe, die den zuständigen Schulbehörden obliegt, in Form von Personendatenbearbeitungen einem Dritten übertragen.

Daher wäre es aus datenschutzrechtlicher Sicht wünschenswert, dass die Auftragserteilung in Form eines schriftlichen Vertrages erfolgen würde, wo zumindest folgende Punkte fixiert werden:

- Swisscom müsste zustimmen, dass ihrerseits, bzw. seitens des ihr gegenüber verantwortlichen Subunternehmens Zscaler die technischen Konditionen nicht ohne das vorgängige ausdrückliche Einverständnis des Kantons geändert werden dürfen.

- Swisscom gibt die Garantie ab, dass sie in der Lage ist, jederzeit überprüfen zu können, dass das Subunternehmen Zscaler die gesetzlichen Anforderungen, die nach schweizerischem Datenschutzrecht verlangt sind, auch wirklich einhält.

- Swisscom geht nicht ohne vorheriges ausdrückliches Einverständnis der zuständigen kantonalen Behörden in dieser Sache ein Vertragsverhältnis mit einem andern Subunternehmen ein.

- Swisscom garantiert, dass sie das Berechtigungskonzept von Zscaler einsehen und dieses in Bezug auf die Zusicherungen, welche von Zscaler der Swisscom gegenüber abgegeben werden, überprüfen kann.

- Die Swisscom garantiert, dass die durch Zscaler vorgenommene Audit-Log-Protokollierung durch Swisscom jederzeit eingesehen und überprüft werden kann.

- Die Swisscom kann garantieren, dass die vom Kanton definierten Whitelists auch wirklich beachtet werden.

13.

Muss kantonales Recht im Hinblick auf eine anstehende El-Revision unter datenschutzrechtlichen Aspekten angepasst werden?

Das Amt für Gesundheit gelangt mit der Anfrage an die Datenschutzstelle, wie weit kantonales Recht im Hinblick auf eine anstehende EL-Revision unter datenschutzrechtlichen Kriterien angepasst werden sollte?

Eine Anpassung des kantonalen Rechts im Hinblick auf datenschutzrechtliche Überlegungen erscheint im Zusammenhang mit der bevorstehenden EL-Reform nicht zwingend notwendig, aber sehr empfehlenswert. Art. 65f. Bundesgesetz über die Krankenversicherung (KVG)[102] verpflichtet die Kantone, Versicherten, die in bescheidenen wirtschaftlichen Verhältnissen leben, Prämienverbilligungen zu gewähren. Den Kantonen wird dadurch eine gesetzliche Aufgabe auferlegt. Gestützt auf diese gesetzliche Grundlage ist in der kantonalen Verordnung zum BG über die Krankenversicherung[103] unter Art. 2 Abs. 1 lit. d festgehalten, dass der Regierungsrat die Vollzugsbestimmungen zur Prämienverbilligung im Sinne von Art. 65 KVG erlässt. In Art. 10 der VO zum BG über die Krankenversicherung ist weiter in Nachachtung von Art. 65f. KVG festgehalten, dass der Kanton Versicherten in bescheidenen wirtschaftlichen Verhältnissen Prämienverbilligung gewährt. Art. 10a enthält die gesetzliche Grundlage, dass die mit der Prämienverbilligung betrauten Personen im Abrufverfahren auf Steuerdaten zugreifen dürfen, soweit dies zum Vollzug der Prämienverbilligung als notwendig erscheint. Gestützt auf Art. 11 hat der Regierungsrat die näheren Bestimmungen über die Prämienverbilligung zu erlassen, namentlich Bestimmungen über die Anspruchsvoraussetzungen und die Bemessungsgrundlagen. Art. 12 unterstellt alle Personen, die in irgendeiner Form mit dem Vollzug der sozialen Krankenversicherung zu tun haben, also auch mit dem Vollzug der Prämienverbilligung betraute Personen, einer ausdrücklichen Schweigepflicht gegenüber Dritten.

Im entsprechenden Reglement[104], welches der Regierungsrat in Ausführung von Art. 2 Abs. 1 lit. d der VO zum BG über die Krankenversicherung erlassen hat, wird in der Zweckbestimmung (Art. 1) implizit auf die ursprüngliche gesetzliche Grundlage (Art. 65 KVG) verwiesen. Art. 20 regelt, gestützt auf das Bundesrecht, den Datenaustausch zwischen Kanton und Versicherern, wobei in Uri bekanntlich das Amt für Gesundheit als die Stelle bestimmt wurde, an welche die Versicherer gestützt auf Art. 106b und Art. 106c der VO über die Krankenversicherung[105] i.V.m. Art. 20 PVR ihre Daten liefern. Gemäss Art. 21 Abs.

[102] KVG; SR 832.10
[103] RB 20.2202
[104] PVR; RB 20.2213
[105] KVV; SR 832.102

2 PVR hat die Sozialversicherungsstelle Uri jeweils dem Amt für Gesundheit eine Bestandsliste aller Personen, welche Ergänzungsleistungen zur AHV/IV beziehen, zukommen zu lassen. Diese Regelung ist gemäss derzeit noch geltendem Recht eine naheliegende Norm, ist das Amt für Gesundheit doch auf diese Informationen im Zusammenhang mit der Prüfung der Anspruchsvoraussetzungen und den Bemessungsgrundlagen für Prämienverbilligung notwendig angewiesen. Wenn ich das richtig sehe, ist der Datenfluss innerhalb des Kantons zwischen dem Amt für Gesundheit und der Sozialversicherungsstelle (SVS) gemäss geltendem Recht mehrheitlich ein einseitiger, d.h., der Datenaustausch fliesst gemäss Art. 21 PVR in der Hauptsache lediglich von der SVS zum AfG. Soweit ich sehe, hat die Regelung in Art. 21 Abs. 2 PVR damit zu tun, dass nach derzeit noch geltendem Bundesrecht (Art. 10 Abs. 3 lit. d BG über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung[106] in der Ergänzungsleistungs-Berechnung immer ein Pauschalbetrag für die obligatorische Krankenversicherung als Ausgaben anerkannt wird. In der vorgesehenen Revision dieser Bestimmung ist dies offenbar ebenfalls so, jedoch nur, sofern dieser jeweils festgesetzte Pauschalbetrag die tatsächliche Prämie nicht übersteigt, da andernfalls die tatsächliche Prämie als Ausgabenbestandteil anzuerkennen ist. Was als «tatsächliche Prämie» zu verstehen ist, ist im Revisionsvorschlag zu ELV unter Art. 16d festgehalten.

Tritt diese Regelung betreffend Ausgaben für die Berechnung der Ergänzungsleistung dereinst in Kraft, dann ist klar, dass nicht nur das AfG für die Berechnung der Prämienverbilligung auf die Personendaten der Versicherten angewiesen ist, sondern auch die SVS für die Berechnung der Ergänzungsleistungen, auf welche Daten das AfG seinerseits wiederum für die Berechnung der Prämienverbilligung angewiesen ist.

Nachdem in Uri die Versicherer ihre Daten dem AfG zur Verfügung stellen müssen, ist es datenschutzrechtlich korrekt, dass unter dem Regime der dereinst neuen Regelung das AfG diese Daten auch der SVS zur Verfügung stellt. In Bezug auf die Weitergabe dieser Krankenkassenprämiendaten seitens des AfG an die SVS, soweit diese zur Prüfung der Anspruchsvoraussetzungen und Berechnung der Ergänzungsleistungen notwendig sind, ist dieser Datenfluss durch Art. 7 DSG[107] abgedeckt. Grundsätzlich reichen aus Sicht des Datenschutzes die bestehenden Bestimmungen des PVR aus.

Dennoch erscheint es empfehlenswert, eine kleine Ergänzung im PVR in Hinblick auf die Revision des ELG/ELV anzubringen. Dies aus nachfolgenden

[106] ELG; SR 831.30
[107] RB 2.2511

Überlegungen:

In Art. 20 Abs. 2 PVR heisst es, dass die von den Versicherern dem AfG gelieferten Daten nur für die Anspruchsprüfung und die Auszahlung der Prämienverbilligung verwendet werden dürfen. Diese Klausel beschlägt einen allgemein anerkannten Grundsatz des Datenschutzrechts, nämlich der Zweckgebundenheit von Personendaten im Hinblick auf deren Bearbeitung. Im Urner DSG ist dieser Grundsatz unter Art. 4 Abs. 3 Satz 2 festgehalten. Im Grunde kommt dieser Klausel in Art. 10 Abs. 2 PVR eigentlich nur deklaratorische Bedeutung zu, da Behörden grundsätzlich immer verpflichtet sind, die durch sie erhobenen Personendaten nur im Hinblick auf den dafür vorliegenden gesetzlichen Zweck zu bearbeiten, für den sie erhoben wurden. Auch die Behörden dürfen Personendaten nie auf Vorrat erheben. Aufgrund der neuen ins Auge gefassten Regelung könnte man datenschutzrechtlich argumentieren, dass auch ohne Überarbeitung von Art. 20 Abs. 2 PVR der Zweck, für den die Personendaten bei den Versicherern erhoben wurden, auch mit einer Weitergabe an die SVS Uri immer noch abgedeckt wäre, da die SVS diese Personendaten für die Anspruchsprüfung und Berechnung der Ergänzungsleistungen benötigt, diese aber wiederum dem AfG zur Verfügung stehen müssen, um die Voraussetzungen für die PV zu prüfen und diese zu berechnen.

Um jedoch vollends Klarheit zu schaffen und auf der sicheren Seite zu sein, erscheint es datenschutzrechtlich dennoch als empfehlenswert, diese Bestimmung zu ergänzen. Als Vorschlag könnte vielleicht dienen:

«…Die Daten dürfen zur Anspruchsprüfung und zur Zahlung der Prämienverbilligung verwendet werden. Ebenso dürfen sie, soweit dies für den Vollzug des ELG/ELV sich als notwendig erweist, der SVS Uri übermittelt werden.»

Es ist dem Datenschützer nicht bekannt, wie gross das Massengeschäft betreffend Ergänzungsleistungen ist, derart, dass sich eine elektronische Übermittlung, bzw. ein Abrufverfahren wirklich aufdrängt. Es wird nicht so umfangreich sein wie die Prüfung der Prämienverbilligung. Dennoch: Sollte das Geschäft jedoch wirklich sehr umfangreich sein, derart, dass es einen riesigen Mehraufwand bedeuten würde, wenn die Ausgleichskasse für jedes einzelne Prüfverfahren beim AfG die entsprechenden Daten anfragen müsste, so wäre aus datenschutzrechtlicher Sicht gegen ein elektronisches Abrufverfahren nichts einzuwenden, da die Voraussetzungen gemäss Art. 7 DSG als erfüllt gelten[108]. Natürlich immer unter der Voraussetzung, dass verlässliche technische und organisatorische Sicherheitsmassnahmen getroffen werden.

[108] Art. 8b DSG

Sofern es sich also um ein Massengeschäft handelt, derart, dass sich eine elektronische Lösung aufdrängt, möchte ich vorschlagen, vielleicht eine sinngemässe Bestimmung in das Gesetz über die Ergänzungsleistungen zur AHV/IV (RB 20.2421) aufzunehmen:

« Die mit dem Vollzug des ELG/ELV bei der Ausgleichskasse betrauten Personen können mittels eines Abrufverfahrens beim Amt für Gesundheit auf die notwendigen Krankenversicherungsdaten greifen.»

14.

Bekanntgeben von Verfügungen seitens Sozialdienste an weitere Gemeindebehörden

Ein Urner Sozialdienst gelangt mit der Anfrage an die Datenschutzstelle, wie weit Verfügungen der Sozialbehörde (Entscheide im Einzelfall betreffend Art und Ausmass der öffentlichen Sozialhilfe) einer Gemeindekanzlei, bzw. dem Gemeinderat zuzustellen sind?

Gestützt auf die Gemeinde-Gesetzgebungen haben sich mehrere Gemeinden zusammengeschlossen und übertrugen die Aufgaben, welche die KV und das Sozialhilfegesetz[109] [110] im Bereich des Sozialwesens den Einwohnergemeinden übertrug, gestützt auf die Gemeindesatzungen einem gemeinsamen regionalen Sozialrat. Der Vertrag wurde in den Gemeinden durch die je zuständigen Organe genehmigt. Der regionale Sozialrat gilt für die dem Vertrag beigetretenen Einwohnergemeinden als die zuständige Sozialhilfebehörde im Sinne von Art. 8 des Sozialhilfegesetzes. Die gesetzlichen Aufgaben, die dem regionalen Sozialrat als Sozialhilfebehörde obliegen, werden in Art. 10 des Gesetzes umschrieben.

Gemäss dieser Bestimmung kommen dem regionalen Sozialrat neben verschiedenen weiteren Obliegenheiten die Aufgaben zu, das Sozialwesen in den Gemeinden zu leiten; die Budget- und Finanzverantwortung des Sozialwesens der jeweiligen Gemeinde zu übernehmen; den Sozialdienst zu beaufsichtigen und ihn in seiner Arbeit zu unterstützen. Überdies sind durch die regionale Sozialhilfebehörde laut Art. 35 allfällig bestehende Rückerstattungsansprüche zugunsten einer betroffenen Wohnsitzgemeinde unter Beachtung der gesetzlichen Verjährungsfrist mit anfechtbarer Verfügung geltend zu machen.

Ebenso haben die Vertrags-Gemeinden einen gemeinsamen Sozialdienst im Sinne des Sozialhilfegesetzes eingerichtet. Dem Sozialdienst obliegt laut Gesetz

[109] RB 1.1101
[110] RB 20.3421

in erster Linie der Vollzug der Sozialhilfe im Einzelfall. Hierfür überträgt ihm das Gesetz neben andern Funktionen die Aufgaben der Abklärung der persönlichen und wirtschaftlichen Sozialhilfe; der Beratung und Betreuung von Menschen in persönlichen, sozialen und materiell schwierigen Lebenslagen; der Entscheid über die Art und das Ausmass der öffentlichen Sozialhilfe im Einzelfall; die Klienten-Administration sowie die Sozialberichterstattung zuhanden der Sozialhilfebehörde über Umfang und Inhalt der Fälle und deren Problemlagen.

In Art. 20 des Gesetzes sind die Grundsätze festgehalten, gemäss denen die Sozialhilfe zu gestalten ist, so u.a. vor allem auch die Achtung der persönlichen Integrität der hilfesuchenden Person. In Art. 21 wird explizit auf eine Schweigepflicht verwiesen, dahingehend, dass alle, die mit dem Vollzug des Sozialhilfegesetzes betraut sind – das sind in erster Linie die Sozialhilfebehörde und der Sozialdienst - oder zum Vollzug beigezogen werden, über die Verhältnisse einer hilfesuchenden Person, über deren Akten – wozu nicht zuletzt auch Verfügungen und Entscheide sowie deren ausführliche Begründungen gehören – und über die Verhandlungen in den Behörden Stillschweigen zu bewahren ist. Dabei handelt es sich nicht einfach lediglich um einen deklaratorischen Hinweis auf das ohnehin geltende Amtsgeheimnis, sondern um eine besondere gesetzliche Schweigepflicht im Sinne von Art. 7 Abs. 2 Datenschutzgesetz[111]. Gemäss Art. 21 Abs. 2 Sozialhilfegesetz dürfen anderen Behörden und Dritten Auskünfte und Akteneinsicht in Einzelfälle nur gewährt werden, wenn die entsprechenden Voraussetzungen des Datenschutzgesetzes erfüllt sind.

Aus der Sozialhilfegesetzgebung geht hervor, dass die Sozialhilfebehörde die Aufgaben erfüllt, die die Kantonsverfassung dem Sozialrat überträgt (Art. 113 KV[112]; Art. 9 Sozialhilfegesetz). Der Sozialdienst hat seinerseits die Sozialhilfe im Einzelfall zu vollziehen (Art. 10a Sozialhilfegesetz). Als Behörden im Sinne von Art. 3 Abs. 1 lit. d DSG, die mit direkten Vollzugsaufgaben im Hinblick auf Einzelfälle betraut sind, gelten demnach der regionale Sozialrat als zuständige Sozialhilfebehörde für die Vertrags-Gemeinden und Kontrollinstanz des Sozialdienstes, und anderseits der Sozialdienst mit seinen fachspezifischen Aufgaben wie Abklärung, Betreuung, Begleitung usw. sowie als verfügende Instanz über die Art und das Ausmass der Sozialhilfe im Einzelfall.

Wie bereits erwähnt, gilt gemäss Art. 8 des Sozialhilfegesetzes der Sozialrat in einer Gemeinde als Sozialhilfebehörde. Gibt es keinen Sozialrat und ist in der Gemeindesatzung nichts anderes bestimmt, dann übernimmt der Gemeinderat in einer Gemeinde die Aufgaben, welche der Sozialhilfebehörde, bzw. dem Sozialrat obliegen. Wurde in der Gemeindesatzung jedoch eine andere Lösung

[111] RB 2.2511
[112] RB 1.1101

getroffen, d.h. wurden die Aufgaben, die das Sozialhilfegesetz im Bereich der öffentlichen Sozialhilfe den Einwohnergemeinden überbindet, einer regionalen Behörde übertragen, dann fungiert der Sozialrat als Vollzugsbehörde im Hinblick auf das Sozialhilfegesetz, und zwar in Bezug auf sämtliche Vertrags-Gemeinden, und keine andere örtliche Gemeindebehörde. Dies geht auch deutlich aus Art. 4 des durch die beteiligten Gemeinden abgeschlossenen Vertrages hervor. Es ist auch der regionale Sozialrat, und nicht ein Gemeinderat, dem die Aufsicht über den regionalen Sozialdienst zusteht, dies auch in Bezug auf die Einzelfälle, die in finanzieller Hinsicht je eine konkret betroffene Wohnsitzgemeinde belasten können.

Unter datenschutzrechtlichen Überlegungen wäre es also nicht korrekt, wenn der Sozialdienst die Entscheide gemäss Art. 10a lit. f mit vollem Inhalt direkt den jeweiligen Gemeinderäten, bzw. den Gemeindekanzleien zustellen würde. Der regionale Sozialrat kann die Verfügungen den betroffenen Gemeinden, bzw. den Gemeinderäten soweit zur Kenntnis bringen, als die betroffene Wohnsitzgemeinde durch die finanziellen Auswirkungen eines Einzelfalles tangiert und belastet wird. Im finanzpolitischen Bereich haben die Gemeinderäte ja auch spezifische gesetzliche Aufgaben wahrzunehmen, sodass eine Bearbeitung von Personendaten im Umfang dieser Aufgaben als mit dem Datenschutzrecht konform erscheint (Art. 7 DSG).

Dies bedeutet jedoch nicht, dass den Gemeindekanzleien oder Gemeinderäten die Verfügungen im Sinne von Art. 10a lit. f Sozialhilfegesetz mit ihrem vollständigen Inhalt zur Kenntnis gebracht werden dürfen, da in derartige Verfügungen, insbesondere in die entsprechenden Begründungen, Informationen einfliessen, die erfahrungsgemäss als besonders schützenswerte Personendaten im Sinne von Art. 3 Abs. 1 lit. f DSG zu werten sind. Angesichts der in Art. 21 Abs. 2 Sozialhilfegesetz festgeschriebenen besonderen gesetzlichen Geheimhaltungspflicht und des Umstandes, dass für die Weiterleitung der vollständigen Verfügungen an die Gemeindekanzleien im Sinne von Art. 10a lit. f Sozialhilfegesetz die Voraussetzungen von Art. 7 Abs. 1 und 2 DSG nicht erfüllt sind, dürfen unter datenschutzrechtlichen Aspekten Informationen betreffend Klienten nur soweit weitergeleitet werden, als dies für die gesetzliche Handhabung der finanziellen Auswirkungen auf eine Wohnsitzgemeinde unter dem Titel von Art. 37 Sozialhilfegesetz zwingend erforderlich erscheint, es sei denn, eine betroffene hilfesuchende Person erteilt in voller Kenntnis der Umstände ihr ausdrückliches Einverständnis, dass ein Entscheid gemäss Art. 10a lit. f Sozialhilfegesetz der Gemeindekanzlei, bzw. dem Gemeinderat vollumfänglich zur Kenntnis gebracht wird.

Anders verhielte es sich, wenn eine Verfügung mit Verwaltungsbeschwerde angefochten wird und die Satzung einer Gemeinde, bevor der Regierungsrat

gestützt auf die Verordnung über die Verwaltungsrechtspflege[113] als Beschwerdeinstanz angerufen werden kann, ein gemeindeinternes Rechtsmittel bereitstellt, wie es Art. 46 Sozialhilfegesetz als Möglichkeit vorgesehen ist. In einer derartigen Konstellation wäre dem zuständigen Gemeinderat eine Verfügung mit ihrem vollen Inhalt zur Kenntnis zu bringen, was durch eine betroffene hilfesuchende Person, die sich beschwert fühlt und einen Entscheid des Sozialdienstes anfechten will, ohnehin zu geschehen hätte. Dies gilt aber nur für den Fall, als eine Verfügung auch wirklich angefochten wird.

15.

Digitalisierung der Schulenderhebungen

Die Bildungs- und Kulturdirektion, Abteilung Berufs- und Studien- und Laufbahnberatung, legt der Datenschutzstelle das Konzept der Digitalisierung der Schulenderhebung vor. Im Zusammenhang mit den Rahmenbedingungen dieses Konzeptes werden aus datenschutzrechtlicher Sicht insbesondere die folgenden Punkte begrüsst:

- Alle Informationen fliessen unter einer SSL-Verschlüsselung.

- Das Datensicherheitskonzept ist derart ausgestaltet, dass die Zugangsberechtigungen der einzelnen Personenkategorien an klar geregelte Passwortanforderungen gebunden sind (Art. 10 DSG).

- Der Zugang zu den Datensätzen wird nur registrierten Personen ermöglicht und wird differenziert gemäss Funktion und Stellung (gesetzlichen Aufgaben der zugangsberechtigten Personen) ausgestaltet (Art. 7 DSG).

- Zugangsberechtigte Personen auf Seiten des Betreibers und der Berufsberatung werden der ausdrücklichen Verpflichtung unterworfen, alle in diesem Zusammenhang zur Kenntnis genommenen und bearbeiteten Personendaten mit Verschwiegenheit zu behandeln und auch das datenschutzrechtliche Gebot der Zweckgebundenheit zu beachten (Art. 4 Abs. 3 DSG). Dasselbe gilt auch für die an der Plattform-Administration beteiligten Personen.

- Der Betreiber macht sich zum Grundsatz, die Sicherheit der Datenplattform gegen allfällige Cyber-Angriffe nach Möglichkeit zu gewährleisten (Art. 10 DSG).

- Besonders wichtig: Der Server der Datenplattform befindet sich in der Schweiz. Die betroffenen Personendaten werden nach Schulabschluss anonymisiert und der jährliche, für die Öffentlichkeit bestimmte Bericht wird in anonymisierter

[113] VRPV; RB 2.2345

Form ins Netz gestellt (Art. 11 DSG)**.**

Gestützt auf die dargelegten Rahmenbedingungen des geplanten Vorhabens und angesichts der Art der Personendaten, die auf dieser Plattform bearbeitet werden, sind die datenschutzrechtlichen Kriterien für das geplante Projekt als erfüllt zu betrachten.

V

Beratungs- und Auskunftstätigkeit

In der Berichtszeitspanne fanden in ausführlicher schriftlicher Form 185 Beratungen gegenüber Privaten und Behörden statt. Hinzu kommen relativ viele mündliche Auskünfte, die aufgrund telefonischer Anfragen gegeben wurden.

VI

Mitberichte/Vernehmlassungen

Die Datenschutzstelle hat auch eine Reihe von Stellungnahmen, Mitberichten und Vernehmlassungen verfasst im Zusammenhang mit dem Erlass von Reglementen, Verordnungen oder Gesetzen in verschiedenen Rechtsgebieten. Die Stellungnahmen erfolgten immer nur beschränkt auf datenschutzrechtliche Aspekte.

VII

N-SIS-Kontrolle

Im Rahmen der Schengen-Verpflichtungen, welche die Schweiz mit dem Abschluss des Assoziierungsabkommens mit der EU betreffend die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes[114] eingegangen ist, sind die Mitgliedstaaten verpflichtet, bei den Endnutzern des Schengen-Informationssystems (SIS) Datenschutzkontrollen durchzuführen. Bei den periodisch durchzuführenden Inspektionen der Schengener-Kontrollbehörden, die auf nationaler Ebene stattfinden, bilden die durch die nationalen Datenschutzbehörden durchgeführten Kontrollen jeweils ebenfalls Gegenstand der Schengen-Evaluationen. Der Datenschutzbeauftragte hat bei der Kantonspolizei im Jahre 2017 eine Kontrolle in Bezug auf die Nutzung des Schengener-Informationssystems durch die Kantonspolizei durchgeführt. Das methodische Vorgehen wurde so gewählt, als beim fedpol die Logfiles über eine

[114] SR 0.362.31

Zeitspanne von einer Woche betreffend die Abfragen der Kantonspolizei durch den Datenschutzbeauftragten angefordert wurden. Die Woche wurde so ausgewählt, dass sie relativ zeitnah der durchzuführenden Kontrolle lag, sodass die in die Kontrolle einbezogenen Beamten sich auch einigermassen an die Abfragen erinnern können. Aus der sehr grossen Menge von Logfiles wurden eine gewisse Anzahl von Abfragen stichprobeweise ausgewählt (nur Personen- , keine Fahrzeugabfragen), dem Polizeikommando zugestellt mit dem Ersuchen, sie den betreffenden Polizeibeamtinnen und Polizeibeamten zur Stellungnahme vorzulegen und dazu kurz begründend Stellung nehmen zu lassen.

Es konnte festgestellt werden, dass innerhalb dieser Kontrolle den antwortenden Polizeibeamten klar war, dass auf jede RIPOL-Abfrage hin digitalisiert gleichzeitig immer auch eine Abfrage über das Schengener-Informationssystem erfolgt, bzw. im Schengener-Informationssystem abgeglichen wird. Die betroffenen Personen vermochten ihre Abfragetätigkeit nachvollziehbar zu begründen und der Datenschützer gewann den Eindruck, dass das Polizeipersonal sehr wohl in Bezug auf die Datenschutzproblematik sensibilisiert ist und keine willkürlichen Abfragen erfolgten. Auch konnte sich der Datenschützer überzeugen, dass aufgrund der Funktionen und des Aufgabenbereichs, welche die stichprobemässig befragten Personen, welche die Abfragen tätigten, bei der Polizei ausüben und wahrnehmen, die Zugriffsberechtigung zu den Informationssystemen zurecht besitzen.

VIII

Öffentlichkeitsgesetz

Im Zusammenhang mit dem Gesetz über das Öffentlichkeitsprinzip der kantonalen Verwaltung[115] erfolgten vereinzelt telefonische mündliche Anfragen, die auch mündlich beantwortet wurden. Im Zusammenhang mit dem Öffentlichkeitsgesetz erfolgen beim Datenschützer relativ wenige Anfragen. Wie viele Anfragen bei direkt betroffenen Amtsstellen erfolgen, derart, dass eine direkte Einigung erfolgt und Einsichtsgesuchen stattgegeben oder zumindest teilweise stattgegeben wird, ist dem Datenschützer nicht bekannt. Grundsätzlich ist die Datenschutzstelle ja nur involviert, wenn zwischen Gesuchsteller und einer Amtsstelle Uneinigkeit herrscht.

Ein Einigungsverfahren wurde in der Berichtszeit durchgeführt. Eine Privatperson ersuchte um Einsicht in verschiedene Unterlagen einer Tourismusorganisation, die einerseits Aufgaben gestützt auf Gemeindegesetz erfüllt, anderseits aber auch seitens des Kantons als Tourismusorganisation

[115] OeG; RB 2.2711

anerkannt ist und teilweise über kantonale Mittel verfügt, indem sie auch kantonale öffentliche Aufgaben wahrnimmt. Die Differenzen zwischen der Privatperson einerseits und der Tourismusorganisation andererseits drehten sich anfänglich um die Frage, wie weit das Öffentlichkeitsgesetz auf den konkreten Sachverhalt Anwendung findet, ist unser OeG in seinem Geltungsbereich doch nur auf Behörden des Kantons, oder auf Dritte, soweit sie öffentliche Aufgaben erfüllen, die ihnen vom Kanton übertragen wurden, zugeschnitten. Der Datenschützer vertrat bei der konkret gegebenen Konstellation die Rechtsauffassung, dass das Öffentlichkeitsgesetz Anwendung findet, dies in der Überlegung, dass einerseits das OeG auch private Dritte als Behörden im Sinne des Gesetzes definiert, sofern sie kantonale öffentliche Aufgaben wahrnehmen,[116] und dass andererseits das kantonale Tourismusgesetz[117] sowie das Tourismusreglement[118] die besagte Tourismusorganisation als solche im Sinne des Gesetzes anerkennt, ihr kantonale öffentliche Aufgaben überträgt und sie teilweise auch mit Mittel ausstattet.

Um in den Status der Anerkennung zu gelangen, müssen laut Tourismusgesetz gewisse Voraussetzungen erfüllt sein. So muss eine Tourismusorganisation neben der Erfüllung weiterer Vorgaben über genügend finanzielle Mittel verfügen[119] und sie muss glaubhaft machen können, dass ihre anderweitigen Einnahmen für die Erfüllung dieser Aufgaben ohne öffentliche Gelder drei Viertel des für die Region berechneten Kantonsbeitrages gemäss Art. 16 erreichen. Präzisiert wird diese Bestimmung in Art. 5 Abs. 1 des Tourismusreglementes, wo ausgeführt ist, dass eine Tourismusorganisation durch Vereinbarungen, Absichtserklärungen und/oder Erfahrungswerte glaubhaft zu machen hat, dass ihre Einnahmen, ohne öffentliche Einnahmen nach dem Tourismusgesetz, drei Viertel des für die Region berechneten Kantonsbeitrages nach Art. 16 des Tourismusgesetzes erreichen. Des Weiteren wird in Art. 5 Abs. 3 des TourR ausdrücklich festgehalten, dass wenn eine Gemeinde mehr als den gesetzlich vorgesehenen Beitrag bezahlt, weil sie beispielsweise von den touristischen Leistungsträgern und von Dritten eine Abgabe zur Förderung des Tourismus einzieht, dann zählt der Betrag, welcher den gesetzlichen Gemeinde-Beitrag übersteigt, ebenfalls zu den Einnahmen der Tourismusorganisation dazu.

Das bedeutet im Grunde, dass die Beherbergungsgebühren, welche von den Zahlungspflichtigen eingezogen werden, zwar primär gestützt auf Gemeinderecht erhoben werden, dass jedoch anderseits die nämlichen Beherbergungsgebühren, sofern sie der Tourismusorganisation, insbesondere

[116] Art. 2 Abs. 2 lit. b OeG
[117] TourG; RB 70.2411
[118] TourR; RB 70.2415
[119] Art. 8 Abs. 1 lit. b TourG

allenfalls über den gesetzlichen Gemeindebeitrag hinaus, weitergeleitet werden, als Teil von deren finanziellen Mitteln und Einnahmen im Sinne des kantonalen Tourismusgesetzes gelten. Sie bilden damit einen integrierenden Bestandteil für die Erfüllung der Voraussetzung, als Tourismusorganisation durch den Kanton anerkannt zu werden. Damit lässt sich ohne Zwang sagen, dass die Tourismusorganisation auch im Hinblick auf die Verwendung der Beherbergungsgebühren nicht nur als Leistungserbringer im Auftrag der betroffenen Gemeinden wirkt, sondern ebenso eine gesetzliche Aufgabe im Auftrag des Kantons wahrnimmt.

Es fand schliesslich eine Einigungs-Zusammenkunft statt und der Privatperson wurde in Teile der von ihr anbegehrten Unterlagen Einsicht gewährt.

IX

Privatim und Zentralschweizer Datenschutzstellen

Der Datenschutzbeauftragte nimmt, wenn es ihm terminlich möglich ist, auch regelmässig an den Frühjahrs- und Herbsttagungen von privatim, der Vereinigung der Schweizer Datenschutzbeauftragten teil. Im Jahre 2017 wurde die Herbsttagung auf Einladung des Kantons Uri im Rathaus in Altdorf durchgeführt. Diese Tagungen dienen der fachlichen Meinungsbildung, der Weiterbildung und des Informations- und Erfahrungsaustausches. An den Tagungen werden jeweils aktuelle Probleme, die den Datenschutz betreffen, erörtert in Form von Fachreferaten und anschliessenden Diskussionen. Auch wurden innerhalb von privatim vor Jahren fünf fachliche Arbeitsgruppen gebildet. Mitglieder sind die meisten Kantone sowie einige Städte. Gerade für eine kleine Datenschutzstelle, wie sie im Kanton Uri besteht, erweist sich die Mitgliedschaft bei privatim als wichtig und nützlich.

Auch findet ein regemässiger Gedankenaustausch mit den Datenschutzstellen der Zentralschweizer Kantone statt.

X

Veranstaltungen

In der Berichtszeit hat eine Veranstaltung stattgefunden. Die Datenschutzstelle wurde von der KESB Uri für ein Referat angefragt. Die Kinder- und Erwachsenenschutzbehörde führt alljährlich eine Instruktions- und Weiterbildungsveranstaltung mit privaten Beiständinnen und Beiständen durch. Für die im Herbst 2018 geplante Veranstaltung wurde der Datenbeauftragte von der KESB eingeladen, eine Einführung zu geben in die wichtigsten

datenschutzrechtlichen Aspekte und Fragestellungen, die sich anlässlich auch einer Mandatsführung durch eine Privatperson ergeben können. Das Referat behandelte in komprimierter Form die wichtigsten grundrechtlichen Fragestellungen, in welche der Datenschutz eingebettet ist; die Strukturierung der gesetzlichen Regelung des formellen Datenschutzes in der Schweiz; zentrale datenschutzrechtliche Begriffe und Grundsätze. Das Hauptgewicht um die Ausführungen drehte sich um das materielle Datenschutzrecht, soweit es sich für eine Mandatsführung im Kindes- und Erwachsenenschutzrecht als relevant erweist, wie Bestimmungen Art. 413ff. ZGB; Art. 443f. ZGB. Es entwickelte sich anschliessend eine rege Fragerunde.

XI

Revision des kantonalen Datenschutzgesetzes

Wie bereits oben dargestellt ruft die abgeschlossene Reform des Datenschutzrechts im europäischen Raum auch nach einer Revision des Datenschutzrechts in der Schweiz, und zwar auf Bundes- wie auf kantonaler Ebene. So besteht auch in Bezug auf das Urner Datenschutzrecht erheblicher Revisions-Bedarf. Der Datenschutzbeauftragte hat zuhanden der Justizdirektion eine Reihe von Revisionsvorschlägen unterbreitet und sich dabei vor allem an den neuen, für die Schweiz verbindlichen RL (EU) 2016/680 und an der revidierten EKonv108+ orientiert, die, sofern das Parlament und weitere Staaten die Genehmigung für die Ratifizierung erteilen wird, was zu hoffen ist, in Kraft treten wird, sofern fünf Vertragsstaaten es genehmigen und in der Folge ratifizieren werden.

Daraus resultiert, dass das Urner Datenschutzgesetz aufgrund der sich ereignenden Rechtsentwicklung ebenfalls in vielen Punkten als überholungsbedürftig erscheint. Nebst einigen Begriffserweiterungen drängt sich eine Revision, bzw. Einführung erweiterter Bestimmungen auf in den Bereichen der Auftragsdatenbearbeitung, der Vorabkonsultation, der Datenschutzfolgenabschätzung, der Datensperrung, des grenzüberschreitenden Datenverkehrs, allfälliger Abrufverfahren, insbesondere wenn besonders schützenswerte Personendaten betroffen sind, in Bereichen allfälliger automatisierter Entscheidungsverfahren, Rechte von betroffenen Personen, Meldepflichten bei Datenschutzverletzungen oder etwa im Bereich von Regelungen betreffend die Stellung der Datenschutzbeauftragten.

XII

Ausblick

In den letzten Jahren fanden zwischen dem Datenschutzbeauftragten einerseits und der Koordinationsstelle Organisationsentwicklung und E-Government sowie dem Kanzleidirektor-Stellvertreter/Informationsbeauftragen andererseits in regelmässigen Abständen Zusammenkünfte statt, bei denen der Datenschützer im Rahmen der E-Government-Strategie über die anstehenden Projekte informiert und instruiert wurde. Für die Datenschützer sind derartige Zusammenkünfte sehr wertvoll, wird der Datenschutzbeauftragte doch diesbezüglich sehr informativ auf dem neuesten Stand gehalten. Er erhält so die Möglichkeit, sich auch anderweitig kundig zu machen, wie es um den Verlauf der Entwicklung von E-Government steht und wo sich allenfalls Schwachstellen ereignen könnten. Der Datenschutzbeauftragte weiss diese Informationssitzungen sehr zu schätzen.

Es ist jedoch nicht von der Hand zu weisen, dass auch im Bereich der öffentlichen Hand und ausserhalb des eigentlichen Rahmens von «E-Government» die rasch voranschreitende Digitalisierung auch vor der eigentlichen Verwaltungstätigkeit nicht Halt macht. Auch von der Verwaltung wird eine speditive, effiziente und kostengünstige Arbeitsweise erwartet und diese Anforderungen rufen in der heutigen Zeit sehr bald nach digitalen Projekten, teilweise auch sehr komplexer Art. Dies ist auch der Grund, dass sowohl anlässlich der Revision des europäischen wie nationalen Datenschutzrechts praktisch überall Bestimmungen betreffend einer Datenschutzfolgenabschätzung eingeführt werden, die vor allem dann greifen sollen, wenn in einem Verwaltungs-Bereich neue digitale Technologien zur Bewältigung von gesetzlichen Aufgaben eingeführt werden sollen. Dies ruft nach Ressourcen, die auch eine technische IT-Kompetenz beinhalten. Eine seriöse datenschutzrechtliche Beurteilung solcher Projekte erfordert im Grunde, dass auch die technischen Prozesse digitalen Inhalts eines solchen Projektes genau verstanden werden, um in eine Beurteilung miteinfliessen zu können. Die Datenschutzstellen grösserer Kantone verfügen bereits jetzt teilweise über derartige personelle Ressourcen. Im Hinblick auf diese Entwicklung müssten sich kleine Kantone wie Uri überlegen, wie sie vielleicht in Zusammenarbeit mit andern Kantonen derartige personelle Ressourcen im eigentlichen technischen IT-Bereich bereitstellen können, sodass sie anlässlich einer allenfalls anstehenden Datenschutzfolgenabschätzung im Hinblick auf die Einführung neuer komplexer IT-Technologien ebenfalls personelle Ressourcen für die technische Beurteilung abrufen könnten. Der derzeitige Datenschutzbeauftragte des Kantons Uri wäre jedenfalls in dieser Hinsicht überfordert.

Altdorf, den 5. Juni 2020

Karl Stadler, Datenschutzbeauftragter