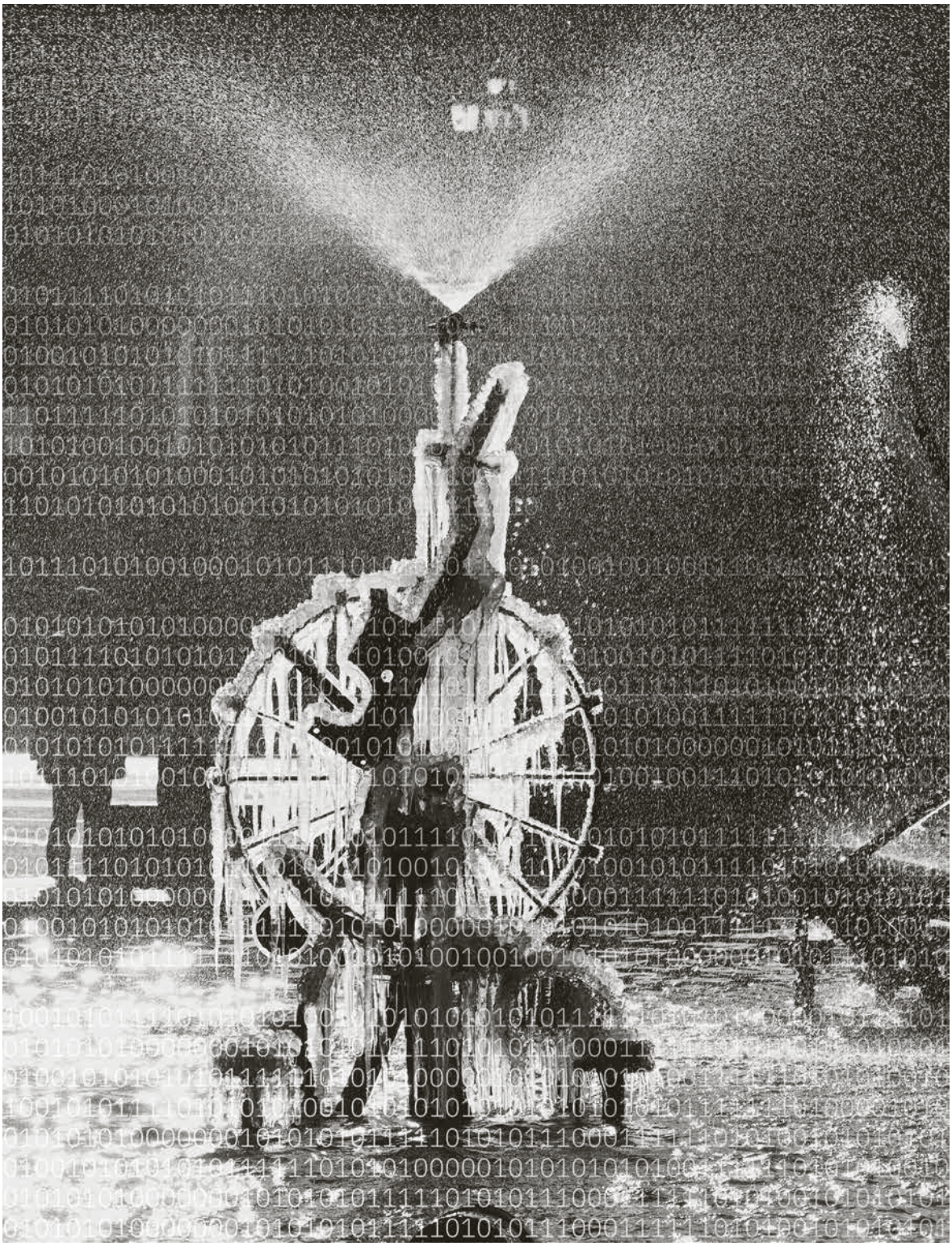
Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat



’20
’21

Inhaltsübersicht

Einleitung

Trends

Der Datenschutzbeauftragte erstattet der Wahlbehörde periodisch Bericht über seine Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht (§ 50 IDG).

Fotokonzept: Tinguely-Brunnen
Fotos: B. Rudin

Jahresüberblick

Fälle

Anhang

Einleitung 2020–2021: Corona und Cloud

Wiederum aus Ressourcengründen legt der Datenschutzbeauftragte einen schriftlichen Tätigkeitsbericht für zwei Jahre vor – jährlich hat er aber in Hearings bei der Geschäftsprüfungskommission des Grossen Rates des Kantons Basel-Stadt mündlich Rechenschaft abgelegt. Die beiden Jahre lassen sich auch bezüglich der thematischen Schwergewichte gut zusammenfassen: Corona und Cloud.

2 C

Ausstieg – Einstieg Zwei C-Themen standen in diesen beiden Jahren im Vordergrund: die Corona-Pandemie und die Cloud – wenn auch mit unterschiedlichem Blickwinkel: Beim ersten Thema sucht man aus der Corona-Pandemie *raus*zukommen – beim zweiten in die Cloud *rein*zukommen.

Corona

Aufgabenerfüllung unter Pandemie-Bedingungen Die Covid-19-Pandemie hat die beiden Berichtsjahre stark geprägt. Auf der einen Seite mit dem Bemühen des Datenschutz-Teams selber, seine Aufgabe zugunsten der Grundrechte der Menschen in unserem Kanton auch unter erschwerten Pandemie-Bedingungen weiter zu erfüllen – auf der anderen Seite bei der Unterstützung der öffentlichen Organe (Verwaltungsstellen wie Bildungsinstitutionen), ihre Dienstleistungen mit digitaler Unterstützung weiterhin anbieten zu können. In diesem Zusammenhang wurden – in enger Zusammenarbeit mit den Datenschutzaufsichtsstellen v.a. in den Kantonen Basel-Landschaft, Bern und Zürich – Tools und Anwendungen für Home-Office und Distance-Schooling in Bezug auf ihre Datenschutzkonformität beurteilt.

Gesundheitsdaten Natürlich hatten aber auch viele Fragestellungen im Zusammenhang mit den Bemühungen, die Pandemie zu bewältigen, eine datenschutzrechtliche Seite. Der Umgang mit Covid-19-spezifischen Personendaten (wie Testresultate und Impfstatus) etwa hat den DSB stark beschäftigt. Auch hier gab es eine starke kantonsüberschreitende Dimension, etwa wenn Bundesstellen Vorgaben gemacht oder Tools empfohlen haben, die datenschutzrechtliche Prüfung aber erst den Kantonen überlassen blieb. Einen weiteren Überblick über unsere Aktivitäten im Zusammenhang mit der Covid-19-Pandemie erhalten Sie im nächsten Kapitel (S. 8 ff.).

Cloud

Zunehmende Dynamik Schon im letzten Tätigkeitsbericht hat der Gang in die Cloud einen wichtigen Platz eingenommen.[1] In den beiden Berichtsjahren 2020 und 2021 hat uns das Thema weiterhin sehr prominent beschäftigt. Erstens wurde im Rahmen von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten (deren Präsidium ich von 2016–2020 innehatte und deren Büroausschuss ich auch weiterhin angehöre), die Schweizerische Informatikkonferenz (SIK)[2] in ihren Verhandlungen für einen Rahmenvertrag mit Microsoft unterstützt. Auch im Rahmen von privatim wurde zweitens das «Cloud-Merkblatt» überarbeitet, und drittens hat das Thema dann auch kantonsintern an verschiedenen Orten an Gewicht, an Dynamik und Dringlichkeit gewonnen.

Verantwortung Die Öffentlichkeit hat Ende März 2022 zur Kenntnis nehmen können, dass der Regierungsrat des Kantons Zürich einen Entscheid zu M365 gefällt hat. Es entstand der Eindruck – und der wurde von Berater:innen auch noch geschürt – dass nun dem Gang der öffentlichen Organe in die Cloud nichts mehr entgegenstehe. Dem ist nicht so. Vor allem ist mit der Beurteilung des Risikos eines Zugriffs ausländischer Behörden («Lawful Access») nur ein sehr kleiner Teil der Vorbereitung getan. Es geht darum, dass dieser Richtungsentscheid, der einen zusätzlichen, schwer rückgängig zu machenden, mehr oder weniger grossen Verlust der direkten Kontrolle über Infrastruktur und Daten mit sich bringt, auf einer umfassenden Beurteilung basiert (dazu mehr hinten S. 21 ff.). Da können Exekutiven noch so viele Gutachten von Anwält:innen einholen (neusterdings sogar von solchen, die gegenüber privatim als Vertreter von Microsoft aufgetreten sind) – die Gesamtverantwortung bleibt bei ihnen.

Rolle der Regierung Was dabei nach unserer Überzeugung die Rolle und Verantwortung des Regierungsrates oder von der Bedeutung her sogar des Grossen Rates (oder bei der Universität: des Universitätsrates, bei den Universitätsspitälern: des Verwaltungsrates) ist, das lesen Sie ab S. 32.

Der Bericht

Drei Teile Der vorliegende Bericht gliedert sich in drei Teile:

— Im ersten Teil (S. 8 ff.) behandeln wir mehrere Trends, die uns in den vergangenen zwei Jahren beschäftigt haben – und aktuell immer noch beschäftigen.

— Im zweiten Teil (S. 43 ff.) geben wir – etwas knapper – einen Überblick, womit wir uns in dieser Zeit in der Beratungs- und Kontrolltätigkeit auch noch beschäftigt haben. Dieser Teil endet mit der Statistik (S. 50 f.).

— Im dritten und letzten Teil (S. 53 ff.) illustrieren wir ein paar spezifische Fragestellungen in Form von Fällen – in der Hoffnung, dass die eine oder der andere Leser:in daraus etwas für die eigene Tätigkeit ziehen möge.

Wir wünschen Ihnen eine erspriessliche Lektüre!

Fast zum Schluss eine sehr persönliche Einschätzung

Hut ab! In den beiden Corona-Jahren gab es viele Amtsstellen und Mitarbeiter:innen, die sich «ein Bein ausgerissen» haben, um weiterhin die versprochenen behördlichen Dienstleistungen zu erbringen – wie auch viele in der Wirtschaft hart darauf hingearbeitet haben, die notwendigen Dienstleistungen (im Gesundheitswesen, in der Versorgung mit lebenswichtigen Gütern usw.) aufrechtzuerhalten. Hut ab vor all diesen Menschen und herzlichen Dank! Etwas befremdet hat mich dann, was Bürger:innen leider bei einzelnen anderen Amtsstellen erlebt haben: Rückzug statt alles daran zu setzen, mit Schutzkonzepten, Plastikscheiben, organisatorischen Massnahmen usw. den Dienstleistungsbetrieb zugunsten der Menschen und der Wirtschaft in unserem Kanton und unserer Wirtschaft aufrechtzuerhalten. Schade!

Ganz zum Schluss

Danke! Unsere Aufgabe zum Schutz der Privatheit der Einwohner:innen, über welche die öffentlichen Organe Daten bearbeiten, und im Interesse ihres Informationszugangsrechts nach dem Öffentlichkeitsprinzip könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb

— der Bevölkerung und den staatlichen Institutionen für das entgegengebrachte Vertrauen;

— allen, die sich mit Fragen zum Datenschutz und zum Öffentlichkeitsprinzip vertrauensvoll an uns wenden;

— den Mitarbeiter:innen der Verwaltung, der öffentlich-rechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;

— den Kolleg:innen der «Kleeblatt-Dienststellen» für die unkomplizierte Zusammenarbeit;

— den Präsidien und Mitgliedern des Grossen Rates, des Büros, der Datenschutz-Delegation des Büros und der Kommissionen für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung;

— den Volontär:innen Alina Schneider, Aurin Schweizer, Deborah De Col und Matthias Plattner für ihre kritische Neugier und ihre aktive Mitarbeit in ihrem jeweils sechsmonatigen Volontariat und

— last but not least meinem Team, Eva Maria Bader, Pascal Lachenmeier, Sukhwant Singh, Thomas Sterchi, Ines Weihrauch und Barbara Widmer, das in den zwei Berichtsjahren mit unverändert grossem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und vorangebracht hat.

Beat Rudin, Datenschutzbeauftragter

1 TB 2017/2018/2019 des DSB/BS, S. 11 ff.
2 Die in den Texten erwähnten Rechtsquellen und Materialien und die verwendeten Abkürzungen sind in einem Verzeichnis am Ende des Berichts detailliert aufgeführt (S. 57 f.).

Trends

Trend 1 Datenschutz in Corona-Zeiten

Trend 2 Präventiver Datenschutz

Trend 3 Projektmanagement und die Rolle der/des Datenschutzbeauftragten

Trend 4 In die Cloud? Viel mehr als ein blosser Releasewechsel!

Trend 5 In die Cloud? Eine grosse Aufgabe für den Regierungsrat

Trend 6 Entwicklungen bei der Videoüberwachung

Trend 1 Datenschutz in Corona-Zeiten

Die Pandemie hat die Gesellschaft, die Wirtschaft und die Verwaltung im Berichtszeitraum 2020 und 2021 im Griff gehabt. Das hat auch den Datenschutzbeauftragten sehr stark beschäftigt. Einerseits natürlich, weil auch das Team des Datenschutzbeauftragten von Lockdown und Home-office-Pflicht betroffen war. Andererseits hat aber der Umgang der öffentlichen Organe im Zusammenhang mit Covid-19 auch vielfältige datenschutzrechtliche Fragen aufgeworfen.

Aufrechterhaltung der Dienstleistungen während des Lockdown

Homeoffice Der Datenschutzbeauftragte hatte bereits zu Beginn der Corona-Pandemie insofern eine gute Ausgangslage, als mit einer Ausnahme alle Mitarbeiter:innen schon Homeoffice-tauglich ausgerüstet waren. Mit Unterstützung der IT des Präsidialdepartements konnte der Übergang ins Homeoffice deshalb fast reibungslos vollzogen werden. Besten Dank!

Nachteile Natürlich war auch das Team des Datenschutzbeauftragten konfrontiert mit den üblichen Erschwernissen, welche die Pandemie mit sich brachte. Dank dem Engagement aller Mitarbeiter:innen konnten aber die internen Prozesse so gestaltet werden, dass nach kurzer Zeit auch die Zusammenarbeit trotz räumlicher Trennung gut geklappt hat. Trotzdem haben sich – vor allem zunehmend mit der Dauer der jeweiligen Homeoffice-Phasen – gewisse Defizite bemerkbar gemacht. Alle Videokonferenz-Tools vermögen den persönlichen Austausch nicht zu ersetzen. Der «kleine Informationsaustausch» an der Kaffeemaschine und das Mitbekommen von Informationen aus einem Gespräch zwischen Kolleg:innen fehlt einfach.

Kein Geschäftsrückgang Zu Beginn des ersten Lockdown gingen wir davon aus, dass die Geschäftszahlen rückgängig sein würden. Das hat sich jedoch nicht bewahrheitet – im Gegenteil. Zwar kamen aus einzelnen Amtsstellen kaum mehr Anfragen, weil – je nach der technischen Ausstattung – Mitarbeiter:innen im Homeoffice keinen oder nur begrenzten Zugriff auf Personendaten in den Datenablagen hatten. Auf der anderen Seite entstanden aber gerade auch aufgrund der Homeoffice-Empfehlung bzw. -Pflicht spezifische Fragestellungen, etwa wenn Mitarbeiter:innen, die Personendaten mit einem sehr hohen Schutzbedarf zu bearbeiten hatten, (gegen Ende der Pandemie) auch von zuhause aus arbeiten wollten, obwohl nach den Aussagen der Departements-IT mit der vorhandenen Ausstattung nur eine tiefere Schutzstufe gewährleistet werden konnte.[1]

Verzögerung bei den Audits Der Start verschiedener Datenschutz-Prüfungen lief nach dem ersten Lockdown gut an. Allerdings verzögerte der zweite Lockdown die Fortsetzung und den Abschluss, indem Vor-Ort-Interviews und Begehungen nicht oder nur sehr eingeschränkt möglich waren. Aus diesem Grund konnte leider nur einer der begonnenen Audits in den Berichtsjahren abgeschlossen werden. Die begonnenen Audits werden im Jahr 2022 vollendet werden.

Corona-spezifische Fragestellungen

Auswahl Die Corona-Pandemie hat, wie zu erwarten war, auch viele Corona-spezifische Fragestellungen aufgeworfen. Sie können hier nicht alle aufgeführt werden. Es wird nur auf ein paar wenige eingegangen.

Erhebung der Zugehörigkeit zu Risikogruppen Durfte ein öffentliches Organ – zu Beginn der Pandemie – von allen Personen, die (im Hinblick auf eine allfällige Einsprache) Einsicht in aufliegende Akten nehmen wollen, verlangen, dass sie angeben, ob sie positiv auf Covid-19 getestet worden sind oder mit einer positiv getesteten Person Kontakt hatten, ob sie sich krank fühlen oder ob sie zu einer (genauer umschriebenen) Risikogruppe gehören? Was tut das öffentliche Organ mit diesen Daten? Besitzt es dafür eine gesetzliche Grundlage? (Dazu mehr hinten im Fall 1, S. 54)

Nennung von positiv getesteten Mitarbeiter:innen Durfte – in der ersten Phase der Pandemie – die Leitung eines öffentlichen Organs die Tatsache, dass bestimmte Mitarbeiter:innen positiv auf Covid-19 getestet worden sind, innerhalb der Dienststelle bekannt geben? Die juristische Antwort: Es kommt darauf an. Die Tatsache, dass jemand an einer bestimmten Krankheit erkrankt ist, ist ein Gesundheitsdatum, mithin also ein besonderes Personendatum, das nur mit einer formell-gesetzlichen Grundlage bekannt gegeben werden darf.[2] Andererseits ist eine solche Information mindestens in kleineren Teams und gerade in Pandemiezeiten ohnehin bald bekannt. Bei niedrigeren Ansteckungszahlen – also bevor die Omikron-Variante dominierend wurde – konnte die Information unter Umständen auch wichtig sein für die Empfehlung, sich testen zu lassen, oder die Anordnung von Quarantäne-Massnahmen. In letzterem Fall kann allenfalls eine mittelbare Rechtsgrundlage[3] hergeleitet werden aus der Pflicht, den Dienstleistungsbetrieb für die Öffentlichkeit aufrecht zu erhalten. «Einfach so», also ohne dass die Information für bestimmte Vorkehren zur Aufrechterhaltung des Betriebes zwingend notwendig ist, ist eine generelle Bekanntgabe unzulässig. Zulässig kann die Bekanntgabe aber sein, wenn die Bekanntgabe zwingend notwendig ist, damit bestimmte Massnahmen getroffen werden können. Selbstverständlich ist dann dafür zu sorgen, dass nur genau diejenigen Daten bekannt gegeben werden, die zur Aufgabenerfüllung nötig sind.

Der DSB hat sich – gemeinsam mit der Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft – an der Beurteilungen von Online-Tools durch die Datenschutzbeauftragte des Kantons Zürich beteiligt.

Bekanntgabe des Impfstatus' von Mitarbeiter:innen Ab Beginn des Jahres 2021 kamen dann vermehrt Fragen danach, ob die Arbeitgeberin den Impfstatus von Mitarbeiter:innen erheben und allenfalls bekannt geben darf. Hier gilt grundsätzlich dasselbe wie bei Daten über positive Tests. Festzustellen war aber, dass die Auseinandersetzungen zu dieser Frage zunehmend emotional geführt wurden.

Überprüfung von Maskenattesten Noch heftiger wurden – gegen Ende der Pandemie – die Diskussionen bei der Frage, ob die Arbeitgeberin oder die Schulen Maskenattests, also ärztliche Dispensationen von der Pflicht, eine Maske zu tragen, verlangen, in eine Liste eintragen und überprüfen dürfen. Die Listen sollten in der Regel erstellt werden, damit nicht täglich (oder beim Fachunterricht in Schulen stundenweise durch die jeweiligen Lehrpersonen) die jeweils für eine bestimmte Dauer ausgestellten Atteste kontrolliert werden müssen. Erst recht zu Konfrontationen geführt hat das Verlangen, die Ärzt:innen, welche die Atteste ausgestellt haben, von der Schweigepflicht zu entbinden.

Videokonferenz-Lösungen

Dringender Bedarf Der Datenschutzbeauftragte hat zu Beginn der Homeoffice- und Distance-Schooling-Pflicht rasch festgestellt, dass ein dringender Bedarf nach Unterstützung bei der Beurteilung der Datenschutzkonformität von möglichen Lösungen (Anwendungen, Tools usw.) besteht. Es war anfangs eine äusserst unübersichtliche Situation, weil sich beispielsweise einzelne initiative und datenschutzbewusste Lehrpersonen an den DSB gewandt haben mit der Frage, ob dieses oder jenes Online-Tool datenschutzkonform einsetzbar sei.

Interkantonale Zusammenarbeit Solche Fragestellungen gab es natürlich nicht nur im Kanton Basel-Stadt. Insbesondere die Datenschutzbeauftragte des Kantons Zürich arbeitete auch schon an solchen Beurteilungen von Online-Tools. Der DSB hat sich deshalb – gemeinsam mit der Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft – an deren Beurteilungen beteiligt. Das Ziel der interkantonalen Zusammenarbeit war eine *Bündelung der Ressourcen*, um eine möglichst ähnliche Beurteilung von Online-Tools, Messenger-Diensten und anderen Angeboten zu erreichen. Die Resultate wurden auf der Website der Datenschutzbeauftragten des Kantons Zürich veröffentlicht.

Beurteilungsmassstab Für die Corona-Zeit galten nicht etwa weniger hohe Datenschutzanforderungen. Die ergeben sich ja letztlich aus dem «Datenschutz-Grundrecht», dem Grundrecht auf informationelle Selbstbestimmung,[4] und sind deshalb nicht beliebig verhandelbar. Ein gewisser *Spielraum* bestand aber *bei der Risikobeurteilung und -abwägung*. Die Nutzung von Onlinediensten stellt in den meisten Fällen eine Auftragsdatenbearbeitung dar. Insbesondere wenn dann noch Cloud-Dienste genutzt werden sollen – und um solche handelte es sich bei den Videokonferenz-Lösungen, die zur Diskussion standen, häufig –, muss eine *Gesamt-Risikoabwägung* stattfinden, um beurteilen zu können, ob die Restrisiken hinnehmbar sind (mehr dazu hinten S. 21 ff.). Diese Gesamt-Risikoabwägung kann *in Pandemie-Zeiten* anders ausfallen als in «normalen» Zeiten. >

Gesamt-Risikoabwägung in Pandemie-Zeiten Illustrieren lässt sich das am *Beispiel* einer Suchtberatung, die ein *Videokonferenz-Tool* einsetzen will: Wenn ein Klient früher wöchentlich bei seiner Therapeutin zu einer Sitzung vorgesprochen hat, kann das beispielsweise in Zeiten des «Social Distancing» und der Homeoffice-Pflicht nicht mehr wie gewohnt stattfinden. Wenn auch ein Ausweichen auf eine telefonische Betreuung nicht erfolgversprechend ist, weil bei diesem Klienten der Sichtkontakt unverzichtbar ist, dann ist ein Ausfallenlassen der Therapie («kommen Sie wieder, wenn die Pandemie vorbei ist!») allenfalls ein schwereres Risiko als das, welches durch die Verwendung eines Videokonferenz-Tools entsteht, bei welchem die Tool-Anbieterin den Namen des Klienten erfahren könnte. Die Suchtberatungsstelle kann in einem solchen Fall zum Schluss kommen, dass das Aussetzen der Beratung den grösseren Schaden anrichten könnte als die Verwendung eines Videokonferenz-Tools, bei dem noch nicht alle Datenschutzeinstellungen optimal sind. Auf jeden Fall darf aber ein Videokonferenz-Tool nur verwendet werden, wenn die betroffenen Personen über die Risiken aufgeklärt worden sind und in Kenntnis dieser Risiken mit der Nutzung einverstanden sind.

Und nachher? Wichtig ist auf jeden Fall, dass *nachher*, wenn also wieder ein «normaler Betrieb» möglich ist, und/oder wenn Online-Tools auch im Regelbetrieb genutzt werden sollen, diese Ausnahme-Begründung nicht mehr gilt. Dann ist erneut eine umfassende Risikoabwägung vorzunehmen, bei welcher die Risiken des Regelbetriebs in Rechnung gestellt werden. Das auftraggebende öffentliche Organ muss die Anbieterin und ihr Produkt sorgfältig auswählen, muss sie sorgfältig instruieren – vertraglich und/oder über Einstellungen – und muss die Anbieterin schliesslich auch sorgfältig überwachen. Das ist nötig, aber zugegebenermassen oft alles andere als trivial. Oft versprechen Hochglanzprospekte mehr, als dann einfach umzusetzen ist. Zum Beispiel muss genau hingeschaut werden, wenn «Verschlüsselung» versprochen wird: Nicht jede Verschlüsselung verhindert den Zugang der Anbieterin zu den bearbeiteten Daten.

Herausforderungen

Krise Bei der Corona-Pandemie handelte es sich um eine Krise. Staatliches Handeln in Corona-Zeiten ist Krisenbewältigung. *Krisenbewältigung* muss mit geringen Gewissheiten auskommen. Das Wissen um Zusammenhänge und Kausalitäten ist meistens noch dünn, doch die Zeit reicht nicht abzuwarten, bis man «alles» weiss. Während Corona haben uns drei Aspekte besonders herausgefordert:

Krisenbewältigung muss mit geringen Gewissheiten auskommen. Das Wissen um Zusammenhänge und Kausalitäten ist meistens noch dünn, doch die Zeit reicht nicht abzuwarten, bis man «alles» weiss.

Geschwindigkeit, Zeit Bei der Rechtsetzung und Projektabwicklung waren die Geschwindigkeit und die Zeit erschwerende Faktoren. Beratungen, Vernehmlassungen und Vorabkonsultationen brauchen in der Regel mehr als zwei Tage, ebenso Prüfungen oder Kontrollen. Wenn aber der Kanton zu Vorschlägen des Bundes innert zweier Tage Stellung nehmen muss, dann sind die «Regelabläufe» nicht möglich. Wenn dann die Entscheide des Bundesrates schon nach kurzer Zeit, manchmal nach zwei Wochen, revidiert werden, stellt es auch schon ein Problem dar zu wissen, was jetzt gilt.

Unsichere Datenlage Bei der Prüfung der *Verhältnismässigkeit staatlicher Massnahmen* wird beurteilt, ob die Massnahmen *geeignet, erforderlich und den betroffenen Personen zumutbar* (verhältnismässig im engeren Sinne) sind. Was aber, wenn – zum Beispiel bei Beginn der Pandemie – unsicher ist, wie das Virus übertragen wird, mit welchen Massnahmen (durch wen, wann und wie – zum Beispiel auch mit der Erhebung und Verfolgung von Ansteckungen) sich die Ausbreitung des Virus bremsen oder stoppen lässt? Das Virus bestimmt den Zeitplan! Mit allen Massnahmen zuwarten, bis klar ist, wie die Massnahmen wirken, ist bei einer Pandemie keine Option.

Dynamik Der Vollzug der vom Bund angeordneten Massnahmen erfolgte in den meisten Fällen durch die Kantone. Es vergeht eine Zeit, bis die Massnahmen wirken («time to market»). Bei schneller Änderung der Rechtslage können sich die Wirkungen von Massnahmen überlagern. Hinzu kommt, dass die Kantone nicht identisch vollziehen.

Erkenntnisse

Rechtsetzung, gesetzliche Grundlage Unsere «normalen» Instrumente taugen begrenzt für den Krisenfall. «Gewissheiten» müssen hinterfragt werden: Ein positiver Covid-19-Test enthält Gesundheitsdaten, also besondere Personendaten, die nur aufgrund einer formell-gesetzlichen Grundlage bearbeitet werden dürfen. Ein negativer Test auch? Und der Impfstatus? Reicht die Zeit für die Schaffung einer formell-gesetzlichen Grundlage? Erlaubt das (Informations- und) Datenschutzgesetz das Bearbeiten von besonderen Personendaten auch aufgrund einer mittelbaren gesetzlichen Grundlage, also auch wenn nur die Aufgabe in einem Gesetz festgehalten ist, zu deren Erfüllung das Bearbeiten von besonderen Personendaten zwingend notwendig ist? Oder gilt das nur im Einzelfall? Das kann im Bund und in anderen Kantonen anders geregelt sein als in Basel-Stadt und Basel-Landschaft.

Verhältnismässigkeit Für die Prüfung der Geeignetheit fehlen belastbare Informationen. Die Dynamik erfordert eine Beurteilung vor einer zuverlässigen Wirkungsanalyse. Die Prüfung der Erforderlichkeit einer Massnahme ist schwierig vorzunehmen, wenn aufs Mal ein Mix von Massnahmen ergriffen wird (oder werden muss). Kurz: Wir müssten viel mehr wissen, als wir wirklich wissen.

Die Prüfung der Erforderlichkeit einer Massnahme ist schwierig vorzunehmen, wenn aufs Mal ein Mix von Massnahmen ergriffen wird (oder werden muss).

Föderalistische Gemengelage In Bezug auf die Rechtsetzungs- bzw. Vollzugskompetenzen herrscht eine föderalistische Gemengelage. Zum Teil wirken Bund, Kantone und Private in unterschiedlichen Konstellationen zusammen. Die Kantone setzen unterschiedlich um: Ist das Impfzentrum ein kantonales öffentliches Organ und untersteht damit dem kantonalen Informations- und Datenschutzgesetz? Oder ist es eine private Institution mit einer Praxisbewilligung und untersteht damit dem Bundesdatenschutzgesetz? Was geschieht bei «Kompetenzüberschreitungen», wenn beispielsweise das Bundesamt für Gesundheit (BAG) für kantonale Datenbearbeitungen (z. B. zu bestimmten Registrierungen) Empfehlungen abgibt, ohne die datenschutzrechtlichen Aufgaben gemacht zu haben? Wie stimmen sich in solchen Fällen die kantonalen Datenschutzbeauftragten ab?

«Normal» Das alles ist für eine Krise nichts Ungewöhnliches. Zwar können die involvierten Stellen mehr oder weniger gut vorbereitet sein. Aber es ist ein Merkmal von Krisen, dass Unerwartetes passiert oder etwas in unerwartetem Mass passiert.

Und jetzt?

Rückblickend hinterfragt Rückblickend kann – hier einzig aus datenschutzrechtlicher Sicht – Verschiedenes hinterfragt werden:

— Im Frühjahr 2020 hiess es: «Die Verwendung der SwissCovid App muss freiwillig sein». Nein. Wenn die Verwendung aus epidemiologischen Gründen *erforderlich* ist, hätte der Bund mit der entsprechenden Rechtsgrundlage die Verwendung der (nach «Privacy by design» und «Privacy by default» geschaffenen) App vorschreiben können.

— Im Sommer 2021 hiess es: «Die Arbeitgeberin darf nicht danach fragen, ob Arbeitnehmer:innen geimpft sind». Doch. Wenn die Arbeitgeberin Massnahmen zum Schutz von Klient:innen, Patient:innen und/oder Mitarbeiter:innen treffen muss/kann, kann es durchaus gerechtfertigt und erforderlich sein, den Impfstatus zu kennen. Wenn zum Beispiel Ungeimpfte nach einem Kontakt mit einer positiv getesteten Person nicht in Quarantäne müssen, wenn sie FFP2-Masken getragen haben, dann kann die Anordnung, welche Maske getragen werden muss, vom Impfstatus abhängig gemacht werden – womit dieser dann für die Kolleg:innen erkennbar wird, wenn nicht auch Geimpfte zu ihrem besseren Schutz freiwillig FFP2-Masken tragen.

— Im Sommer 2021 hiess es ebenfalls: «Teilnehmer:innen nur mit Covid-Zertifikat zu Veranstaltungen zuzulassen, diskriminiert die Nichtgeimpften». Das kann auch von der anderen Seite gesehen werden: Der Verzicht auf die Zertifikatspflicht auferlegt den Geimpften Einschränkungen, die nicht erforderlich wären.

— Es wurde beim Contact Tracing argumentiert, eine zentrale Datenhaltung (also der Zusammenzug der bei Restaurationsbetrieben erhobenen Gästedaten bei einer kantonalen Stelle) sei verfassungswidrig. Nein, mit einer entsprechenden kantonalen Rechtsgrundlage ist das – wie auch das Bundesgericht für den Kanton Bern entschieden hat[5] – zulässig; die Vertraulichkeit, die Verfügbarkeit, die Sicherheit (Zugriffsschutz, Verschlüsselung, Löschung) kann zentral sehr gut (oder vielleicht sogar besser) gewährleistet und kontrolliert werden. >

Lehren für die Zukunft

Erfahrungen Was können wir aus den Erfahrungen der letzten beiden Jahren lernen?

Zwingend Je dringender von staatlicher Seite gehandelt werden muss, umso wichtiger ist es, dass die *Verantwortlichkeit* geklärt ist. Bei Gemengelagen, wo Bund, Kantone und Private in unklaren Konstellationen zusammenarbeiten, besteht die Gefahr, dass niemand die Gesamtverantwortung trägt, dass also wichtige Themen (Rechtfertigung, Sicherheitsmassnahmen) zwischen den Teilverantwortlichkeiten durchfallen.

Einflussnahme des DSB In Diskussionen im Team und vor allem mit anderen Datenschutzbeauftragten taucht immer die Frage auf, wie am effektivsten Einfluss genommen werden kann. Wenn ein Kanton eine epidemiologische Massnahme treffen will, bei der aber – keine Überraschung im Kontext einer Pandemie – auch besondere Personendaten bearbeitet werden, dann setzt das IDG eine formell-gesetzliche Grundlage voraus.[6] Muss diese Grundlage auf dem Weg der ordentlichen Gesetzgebung geschaffen werden, dann kommt die Massnahme wohl zu spät. Vielleicht kann sich der Kanton aber auf eine möglicherweise etwas vage bundesgesetzliche Grundlage im Epidemiengesetz stützen[7] und mit einer kantonalen Verordnung zeitgerecht eine Grundlage für die Massnahme schaffen – aber eben keine formell-gesetzliche. Soll sich der DSB dann auf die Frage der Rechtsgrundlage versteifen («ohne eine Regelung in einem Gesetz im formellen Sinn geht gar nichts!») und sich mit dieser strengen Haltung aus der Diskussion sprengen – oder auf das Manko aufmerksam machen, aber gleichzeitig aktiv mitwirken, dass inhaltlich wenigstens alles richtig gemacht wird? Am oben erwähnten Beispiel einer zentralen Aufbewahrung von Contact Tracing-Daten:

— dass die *Verantwortung klar zugeordnet* wird,

— dass der *Zweck möglichst präzis umschrieben* wird,

— dass die Verwendung für andere Zwecke (z.B. für die Strafverfolgung) *ausdrücklich als unzulässig erklärt* wird,

— dass die *Aufbewahrungsfrist bestimmt und die Vernichtung* nach Ablauf der Frist angeordnet wird,

— dass die *notwendigen Schutzmassnahmen* für die Datenübermittlung, die Datenaufbewahrung und die Zugriffe auf die Daten getroffen werden, und

— dass die Einhaltung der Schutzmassnahmen regelmässig *überprüft* wird.

Unsere Haltung Wir sind klar der Meinung, dass wir uns nicht aus der Diskussion sprengen dürfen, sondern *mehr Wirkung* erreichen, indem wir zwar auf die Defizite (zum Beispiel bei der Rechtsgrundlage) hinweisen, aber uns vor allem aktiv an der Diskussion um eine (abgesehen von der Normstufe der Rechtsgrundlage) möglichst datenschutzkonforme Lösung beteiligen. Das darf aber keinesfalls so verstanden werden, dass wir generell die vom IDG verlangte Gesetzesgrundlage als verzichtbar ansehen.

Vertrauen ins Milizsystem Zum Schluss darf auch noch – als persönliche Meinung – festgehalten werden: Auch während den zwei Corona-Jahren war die Schweiz *keine Diktatur*. Ich hatte und habe grosses Vertrauen in die Resilienz unseres Milizsystems.

Post-Corona

Rückkehr Während der Pandemie waren nicht Regeln aufgehoben, aber Abwägungen konnten – wie vorne an einem Beispiel illustriert (S. 10) – anders ausfallen. Jetzt, nach der Pandemie, geht es um die Rückkehr zum «Regelbetrieb». Das wird für alle eine Herausforderung. «Man hat sich halt so daran gewöhnt», hören wir ab und zu. Jetzt muss aber wieder darauf geachtet werden, dass Videokonferenz-Tools ohne zusätzliche Schutzmassnahmen nicht zur Übermittlung von Personendaten oder gar von besonderen Personendaten geeignet sind.

1 Hier hat der DSB die Sicherheitsverantwortlichen gestützt: Sicherheitsmassnahmen sind auch in Pandemiezeiten einzuhalten. Im konkreten Fall wurde später von den verantwortlichen öffentlichen Organen der Schutzbedarf aufgrund einer Neubeurteilung – und in Übereinstimmung mit der Beurteilung durch den DSB – von «sehr hoch» auf «erhöht» reduziert.
2 § 21 Abs. 2 IDG.
3 Im Sinne von § 21 Abs. 2 lit. b IDG.
4 Art. 10 und 13 Abs. 2 BV; § 11 Abs. 1 lit. j KV/BS.
5 Urteil 2C_369/2021 der II. öffentlich-rechtlichen Abteilung des Bundesgerichts vom 22. September 2021.
6 § 21 Abs. 2 IDG.
7 Anders als im Bund und in anderen Kantonen erlaubt das baselstädtische IDG eine Datenbearbeitung gestützt auf eine mittelbare gesetzliche Grundlage (§ 21 Abs. 1 und 2, jeweils lit. b IDG) nicht nur ausnahmsweise oder im Einzelfall; vgl. dazu PK-IDG/BS-Rudin, § 21 N 6 ff. und N 37.

Trend 2 Präventiver Datenschutz

Zukunftsorientierter Datenschutz ist präventiver Datenschutz. Die heute schon gesetzlich vorgesehene Vorabkontrolle leidet aber unter verschiedenen Schwächen. Die laufende IDG-Revision wird den präventiven Datenschutz durch eine Pflicht der öffentlichen Organe zur Datenschutz-Folgenabschätzung bei datenschutzrelevanten Vorhaben und durch die Prinzipien «Privacy by design» und Privacy by default» verstärken.

Zukunftsorientierter Datenschutz

Verstärkt Einer der Ansätze eines zukunftsorientierten Datenschutzes ist der *präventive Datenschutz*: nicht hinterher feststellen, dass die Grundrechte von betroffenen Personen verletzt wurden, sondern vorher dazu beitragen, dass ein Bearbeiten von Personendaten datenschutzkonform erfolgt. Diesen Ansatz kennt bereits das geltende Informations- und Datenschutzgesetz; er soll aber mit der laufenden Revision[1] deutlich verstärkt werden.

Elemente Zum präventiven Datenschutz gehören verschiedene Elemente:

— der Grundsatz des Datenschutzes durch Technikgestaltung («Privacy by design»)[2];

— der Grundsatz der datenschutzfreundlichen Voreinstellungen («Privacy by default»)[3];

— die Datenschutz-Folgenabschätzung (DSFA)[4] und

— die Vorabkonsultation[5] (bisher: Vorabkontrolle[6])

Zwei Technikgestaltungsprinzipien

«Privacy by design» Der Grundsatz *«Privacy by design»* – so steht es im Ratschlag zur IDG-Revision[7] – verlangt, dass bei Datenbearbeitungen von Anfang an Massnahmen getroffen werden, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen. Das bedeutet, dass eine Aufgabenerfüllung, wenn dies möglich ist, im Sinne der Datenvermeidung als Ausfluss des Verhältnismässigkeitsprinzips ohne, ohne sensitive, mit weniger oder mit weniger sensitiven Personendaten erfolgt, dass technische Möglichkeiten wie die Anonymisierung oder Pseudonymisierung genutzt werden und dass weitere datenschutzfreundliche Technologien («Privacy enhancing technologies»/PET) verwendet werden. Umzusetzen ist dies etwa dadurch, dass Personendaten nur erhoben werden, wenn eine Rechtfertigung dafür besteht, dass nur die für die Aufgabenerfüllung tatsächlich erforderlichen Personendaten überhaupt erhoben werden, dass Randdaten, die bei der Nutzung von IT-Systemen anfallen, nicht gespeichert, möglichst rasch anonymisiert oder mindestens pseudonymisiert werden oder dass die Zweckänderung der Datenbearbeitung verhindert wird. Beispielsweise muss der Download von Informationen von einer staatlichen Website anonym möglich sein; bei Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen muss es möglich sein, die Angabe des Standortes manuell vorzunehmen (und nicht einfach durch eine Ortung durch das Handy). Wenn solche *grundrechtsschonenden Möglichkeiten* nicht bestehen, werden die Grundrechte der betroffenen Personen unnötigerweise verletzt – und wenn diese Möglichkeiten nicht von Anfang an in den Systemen und Anwendungen eingebaut sind, ist es oft nicht mehr möglich oder sehr viel aufwändiger, dies nachträglich zu tun.

«Privacy by default» Das Prinzip *«Privacy by default»* verlangt – so der Ratschlag zur IDG-Revision[8] –, dass bei Datenbearbeitungen die Voreinstellungen datenschutzfreundlich gewählt werden. Die betroffene Person soll sich nicht durch Einstellungen kämpfen müssen, um ihr Grundrecht auf informationelle Selbstbestimmung zu schützen. Die Voreinstellungen sollen ihre Selbstbestimmung schützen und nur die Erfassung der absolut notwendigen Daten zulassen. Die betroffene Person soll selber bestimmen, wenn sie eine weiter gehende Einschränkung ihres Grundrechts zulassen will (Opt-in anstelle von Opt-out). Am Beispiel der Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen: In den Voreinstellungen darf der Standortdienst nicht aktiviert sein. Die Benutzer:innen müssen diesen selber aktivieren, wenn sie ihn nutzen wollen.

Umsetzung Diese Gestaltungsprinzipien sind vor allem bei neuen Vorhaben zu beachten. Sie sind mit entsprechenden technischen und organisatorischen Massnahmen umzusetzen. >

Datenschutz-Folgenabschätzung und Vorabkonsultation

Ziel Diese beiden Schritte zielen im Rahmen eines Projektes darauf ab, rechtzeitig die Risiken für die Grundrechte der betroffenen Personen zu erkennen und durch geeignete Massnahmen zu vermeiden oder mindestens so weit zu verringern, dass das Risiko nicht mehr als hoch einzustufen ist und den betroffenen Personen zuzumuten ist. Bleibt trotz Massnahmen das Risiko für die Betroffenen hoch, dann ist auf das Vorhaben zu verzichten.

Vorabkonsultation

Nicht neu Warum wird nun zuerst die Vorabkonsultation dargestellt und nicht die Datenschutz-Folgenabschätzung (DSFA)? Die Vorabkonsultation war schon im geltenden Gesetz (§ 13 IDG, Vorabkontrolle) vorgesehen; hier können wir also an Bestehendes und Bekanntes anknüpfen. Ausserdem ist die DSFA im Grunde genommen nichts anderes als die Vorbereitung für die Vorabkonsultation. Deshalb macht es Sinn, zuerst zu verstehen, was vorbereitet werden soll.

Auch Rechtsetzungsvorhaben Neu umfasst die Vorabkonsultation nicht nur die Vorabprüfung von Datenbearbeitungs-Projekten, sondern auch von Rechtsetzungsvorhaben. Sie waren bisher indirekt erfasst, indem es zu den gesetzlichen Aufgaben der/des Datenschutzbeauftragten (DSB) gehört hat, zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind, Stellung zu nehmen (§ 44 lit. f IDG). Neu wird klar, dass die öffentliche Organe die Rechtsetzungsvorhaben aktiv zur Vorabkonsultation einreichen müssen – und zwar richtig verstanden nicht erst im Rahmen der Vernehmlassung. Bei der datenschutzrechtlichen Stellungnahme geht es ja nicht um politische Bewertungen, sondern um Empfehlungen und Hinweise, wie Datenbearbeitungen grundrechtskonform geregelt werden können. So müssen Verantwortlichkeiten und Aufgaben klar geregelt werden, damit die Betroffenen abschätzen können, was sie erwartet, und die Verwaltungsmitarbeiter:innen nicht wegen unklarer Regelungen riskieren, die Rechte der Betroffenen zu verletzen und dafür allenfalls zur Rechenschaft gezogen zu werden. Diese Hinweise kommen im Rahmen des Vernehmlassungsverfahrens, also fast am Schluss des Rechtsetzungsvorbereitungsprozesses, in der Regel zu spät. Sie müssen oft bereits bei der Konzeption eines Erlasses berücksichtigt werden. Auf diese Rechtsetzungsvorhaben soll aber hier nicht weiter eingegangen werden.

Kernfrage Bei der Vorabkonsultation wird ein Projekt vorab auf seine Datenschutzkonformität geprüft. Die Kernfrage lautet: Kann ein Vorhaben datenschutzkonform umgesetzt werden?

Vorzulegende Dokumentation Nach § 4 IDV muss die vom öffentlichen Organ der/dem DSB vorzulegende Dokumentation alle für die Beurteilung relevanten Unterlagen enthalten, insbesondere:

— eine Beschreibung des Vorhabens,
— eine Darstellung der Rechtslage und
— eine Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen.

Präventiver Datenschutz: nicht hinterher feststellen, dass die Grundrechte von betroffenen Personen verletzt wurden, sondern vorher dazu beitragen, dass ein Datenbearbeiten datenschutzkonform erfolgt.

Beschreibung des Vorhabens Zuerst muss ein Vorhaben so beschrieben werden, dass Nichtinvolvierte verstehen können, was getan werden soll. Aus der Beschreibung muss hervorgehen, für welche Aufgabe(n) welche (Personen-)Daten in welcher Art und durch wen bearbeitet werden. Kurz«beschreibungen» wie «Geschäftsverwaltungssystem» erfüllen diese Anforderungen nicht. Relevant sind Unterlagen, die zum technischen Verständnis beitragen, und Aussagen dazu, ob ein bestehendes System abgelöst werden soll und/oder welche Schnittstellen zu anderen Systemen geschaffen werden sollen.

Darstellung der Rechtslage Ausserdem ist aufzuzeigen, dass für das konkret geplante Bearbeiten von Personendaten die notwendigen Rechtsgrundlagen bestehen. Die können in zwei Formen vorliegen:

— als *unmittelbare gesetzliche Grundlage*: In diesem Fall regelt das Gesetz oder die Verordnung unmittelbar das Datenbearbeiten[9], oder
— als *mittelbare gesetzliche Grundlage*: Hier legt das Gesetz oder die Verordnung eine Aufgabe fest, die nur erfüllt werden kann, wenn Personendaten bearbeitet werden[10], die Bestimmung regelt also nur mittelbar das Bearbeiten.
— Falls (auch) *besondere Personendaten* im Sinne von § 3 Abs. 4 IDG bearbeitet werden sollen, muss diese (unmittelbare oder mittelbare) Grundlage in einem Gesetz *im formellen Sinn* stehen[11].

Rechtsgrundlage(n) Die gesetzliche Grundlage für das Datenbearbeiten ist nicht § 9 IDG – diese Bestimmung verlangt ja erst eine gesetzliche Grundlage; sie ist im entsprechenden Fachgesetz – also beispielsweise für die Kantonspolizei im Polizeigesetz oder der Strafprozessordnung, für die Sozialhilfe im Sozialhilfegesetz, für die Volksschule im Schulgesetz usw., zu finden. Es reicht aber nicht, einfach ein Gesetz zu nennen – es braucht die präzisere Angabe, in welchen *Paragrafen* das Datenbearbeiten oder die Aufgaben, die erfüllt werden soll, geregelt sind. Falls die notwendigen Rechtsgrundlagen noch nicht existieren, sind sie rechtzeitig zu schaffen.

Übersicht über die Massnahmen Ein Bearbeiten von Personendaten darf die Grund- und Persönlichkeitsrechte der von der Datenbearbeitung betroffenen Personen nicht verletzen. Zu diesen Rechten gehört insbesondere das Grundrecht auf informationelle Selbstbestimmung.[12] Dieser dritte Teil der einzureichenden Dokumentation muss aufzeigen, mit welchen *technischen, organisatorischen und rechtlichen Massnahmen* die Risiken für die Betroffenen ausgeschlossen oder so weit reduziert werden, dass das Risiko nicht mehr als hoch zu bewerten und somit den betroffenen Personen zuzumuten ist. Der Weg dorthin führt über mehrere Analysen (siehe unten unter dem Absatz-Stichwort Analyseprozesse). Die Erkenntnisse aus diesen Analysen sind für das umzusetzende Projekt schliesslich im Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) festzuhalten.

Resultat der Vorabkonsultation Am Ende einer Vorabkonsultation sollte die Frage beantwortet sein, ob und wie ein Vorhaben datenschutzkonform umgesetzt werden kann. Das «Wie» kleidet die/der DSB in Empfehlungen im Sinne von § 46 IDG. Die Verantwortung für die Umsetzung oder Ablehnung der Empfehlungen liegt beim öffentlichen Organ, an welches die Empfehlungen gerichtet sind. Eine Weisung in Form einer verbindlichen Verfügung (§ 47 IDG) kommt hier (noch) nicht zum Zuge: Eine solche kann von der/dem DSB erst erlassen werden, wenn tatsächlich Personendaten unrechtmässig oder unverhältnismässig bearbeitet werden[13], nicht schon, wenn das Bearbeiten erst geplant ist.

Datenschutz-Folgenabschätzung (DSFA)

Erste Voraussetzungen Die DSFA ist die *Vorbereitung der Vorabkonsultation* durch das verantwortliche öffentliche Organ. Voraussetzungen dafür sind – wie soeben für die Vorabkonsultation beschrieben – auch hier erstens eine *Beschreibung des Vorhabens* und zweitens eine *Rechtsgrundlagenanalyse*. Wenn nicht klar ist, was überhaupt gemacht werden soll und ob dafür die notwendigen Rechtsgrundlagen bestehen, kann auch keine DSFA vorgenommen werden.

Mehrere Schritte Sobald diese Voraussetzungen gegeben sind, erfolgt die DSFA in verschiedenen Schritten:

— *Erster Schritt*: *Fragebogen*: In einem ersten Schritt soll mittels eines Fragebogens eruiert werden, ob überhaupt eine DSFA zu erstellen ist. Bei jedem Projekt ist dieser auszufüllen, um festzustellen, ob *überhaupt Datenschutz-Risikofaktoren* bestehen. Die/der DSB wird dazu einen einfachen Fragebogen zur Verfügung stellen. Falls keine Datenschutz-Risikofaktoren bestehen, weil z.B. gar keine Personendaten bearbeitet werden, ist dieser Befund von den Verantwortlichen zu unterschreiben und zur Projektdokumentation zu nehmen, damit später nachgewiesen werden kann, dass die Projektleitung diese Prüfung vorgenommen hat.

— *Zweiter Schritt: Schutzbedarfs- und ggf. Risikoanalyse*: Wenn Risikofaktoren bestehen, dann sind in einem zweiten Schritt die entsprechenden Risiken vertieft anzuschauen. Dabei geht es nicht um die Projektrisiken – also z.B. das Risiko, dass eine Anbieterin Konkurs geht, dass sie nicht rechtzeitig liefern kann oder dass die geschätzten Kosten überschritten werden –, sondern um *Datenschutzrisiken*, also Risiken für die Rechte der betroffenen Personen (z.B. Bekanntwerden von Daten, die nur für das verantwortliche öffentliche Organ bestimmt sind, mit dem Risiko der Diskriminierung, Rufschädigung u. ä.). Diese Risiken sind zu eruieren und in Bezug auf Schadensausmass und Eintretenswahrscheinlichkeit zu bewerten. Als nächstes sind Massnahmen ins Auge zu fassen, um diese Risiken auszuschliessen oder auf ein tragbares Mass zu verringern. Im Ergebnis ist das Restrisiko, das nach dem Umsetzen aller Massnahmen noch besteht, festzuhalten. Dieses Restrisiko, das nicht mehr durch Massnahmen verringert werden kann, ist durch das verantwortliche öffentliche Organ (d.h. durch dessen Leitung) zu übernehmen.

Analyseprozesse Im Rahmen des zweiten Schrittes sind verschiedene Analyseprozesse zu durchlaufen. Mit der *Schutzbedarfsanalyse* wird der Schutzbedarf bestimmt: Welchen Schutz brauchen die Daten bzw. Datenbearbeitungsprozesse – und zwar, wie in § 8 Abs. 2 IDG vorgegeben – pro Schutzziel: Vertraulichkeit, Integrität (inkl. Zurechenbarkeit und Nachvollziehbarkeit) und Verfügbarkeit. Nach dem >

Konzept des Grundschutzes wird der Grundschutzbedarf durch die standardmässig zu treffenden Grundschutzmassnahmen erfüllt. Sobald in Bezug auf ein Schutzziel nicht nur Grundschutzbedarf, sondern ein erhöhter Schutzbedarf besteht, ist diesbezüglich eine *Risikoanalyse* durchzuführen, um die spezifischen zusätzlichen Massnahmen zu definieren, mit denen der erhöhte Schutzbedarf (pro Schutzziel) abgedeckt werden soll. Wichtig ist dabei, dass die geplanten Massnahmen den eruierten Risiken zugeordnet werden, weil nur dann die Auswirkungen der Massnahmen auf die Risiken beurteilt werden können.

ISDS-Konzept mit den technischen und organisatorischen Massnahmen Die Erkenntnisse aus diesen Analysen sind, wie bereits erwähnt, für das umzusetzende Projekt schliesslich im *Informationssicherheits- und Datenschutz-Konzept* (ISDS-Konzept) festzuhalten. Es hat (aus Datenschutzsicht) mindestens folgenden Inhalt:

— eine Umschreibung der geplanten *technischen und organisatorischen Umsetzung*;

— eine Beschreibung, wie die Prinzipien von *«privacy by default» und «privacy by design» umgesetzt* sind;

— ein *Zugriffsberechtigungskonzept* mit Rollen: Welche Nutzer:innen (Rollen) haben Zugriff auf welche Daten? Wer löst Mutationen aus? Wer sorgt dafür, dass die Berechtigungen aktuell sind (insb. dass die nicht mehr zu Recht bestehenden Berechtigungen entfernt werden)?

— ein *Löschkonzept*: Wann sind die Daten durch wen zu löschen? Oder durch wen ist innert welcher Fristen zu prüfen, ob die Personendaten zur Aufgabenerfüllung noch weiter erforderlich sind oder ob sie archiviert oder vernichtet werden müssen?

Rechtliche Massnahmen bei Auftragsdatenbearbeitungen Enthält ein Vorhaben auch eine Auftragsdatenbearbeitung, sollen also bestimmte Datenbearbeitungen im Auftrag des öffentlichen Organs durch Dritte vorgenommen werden, dann werden auch rechtliche Massnahmen notwendig werden. Insbesondere braucht es eine *schriftliche Vereinbarung* des auftraggebenden öffentlichen Organs mit der Auftragsdatenbearbeiterin. Dabei hilft der vom DSB veröffentlichte Leitfaden Auftragsdatenbearbeitung.[14]

Schriftliche Vereinbarung Der Regierungsrat hat 2011 beim Erlass der IDV festgelegt, dass der Auftrag nur dann schriftlich erteilt werden muss, wenn Organisationseinheiten oder Private, die dem IDG nicht unterstehen, beauftragt werden.[15] Der DSB hat schon damals empfohlen, immer eine schriftliche Vereinbarung zu treffen. Zum Schutz des auftraggebenden öffentlichen Organs, das ja verantwortlich bleibt, auch wenn es Personendaten durch ein anderes öffentliches Organ bearbeiten lässt, empfehlen wir immer noch dringend, auch die Auftragserteilung an dem IDG unterstehende öffentliche Organe schriftlich vorzunehmen, insbesondere wenn besondere Personendaten bearbeitet werden sollen, wenn die Bearbeitung eine grosse Anzahl von Personen betrifft oder wenn es aus anderen Gründen[16] angezeigt ist.[17] Nur so kann sichergestellt werden, dass nicht (Sicherheits-)Lücken entstehen, weil jede Stelle gedacht hat, die andere «macht das».

Dokumente für die Vorabkonsultation Im Rahmen der Datenschutz-Folgenabschätzung sind also genau die Dokumente zu erstellen, die ohnehin nach § 4 IDV im Rahmen der Vorabkonsultation der/dem DSB vorzulegen sind:

— die Beschreibung des Vorhabens,

— die Darstellung der Rechtslage und

— die Übersicht der Schutzmassnahmen – in frühen Prozessphasen in Form der Risikoanalyse, im Resultat in Form des ISDS-Konzeptes, in welchem die Ergebnisse aus den vorhergehenden Analysen festgehalten werden.

Defizite bei der Umsetzung

Defizite im Projektmanagement Mit dem revidierten IDG soll – wie erwähnt – der präventive Datenschutz gestärkt werden. Leider sind aber schon bei der Umsetzung der Vorabkonsultation (oder wie sie im geltenden IDG noch heisst: der Vorabkontrolle) Defizite festzustellen. Darauf und auf die Rolle der/des DSB soll im Text zum Projektmanagement (S. 17 ff.) näher eingegangen werden.

1 Ratschlag 21.1239.01, Geschäft: https://www.grosserrat.bs.ch/ratsbetrieb/geschaefte/200111340.
2 § 14 Abs. 1 E-IDG.
3 § 14 Abs. 2 E-IDG.
4 § 12a E-IDG.
5 § 13 E-IDG.
6 § 13 IDG; vgl. dazu PK-IDG/BS- Rudin, § 13 N 1 ff.
7 Ratschlag 21.1239.01, S. 27.
8 Ratschlag 21.1239.01, S. 28.
9 § 9 Abs. 1 und 2, jeweils lit. a IDG.
10 § 9 Abs. 1 und 2, jeweils lit. b IDG.
11 § 9 Abs. 2 (im Vergleich zu Abs. 1) IDG.
12 Art. 10 und 13 Abs. 1 BV; § 11 Abs. 1 lit. j KV.
13 PK-IDG/BS-Schilling, § 47 N 2 ff. und 8.
14 https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html.
15 § 1 IDV.
16 Zum Beispiel bei mehreren beteiligten Stellen aus verschiedenen Departementen.
17 PK-IDG/BS-Rudin, § 7 N 38.

Trend 3 Projektmanagement und die Rolle der/des Datenschutzbeauftragten

Digitalisierung braucht Vertrauen. Der präventive Datenschutz soll dazu beitragen, u.a. mit der Vorabkonsultation. Dies funktioniert bei gewissen öffentlichen Organen recht zuverlässig, bei anderen allerdings leider nicht. Die Defizite werden in Zukunft durch die Datenschutz-Folgenabschätzung möglicherweise beseitigt, aber es braucht mehr: ein einheitlich strukturiertes und durchgesetztes Projektmanagement und Standards. Dabei sind die Verantwortlichkeiten und Rollen zu beachten: Die/der DSB ist nicht der Rechtsdienst oder die IT-Sicherheitsabteilung der Departemente oder Dienststellen, sondern hat eine Aufsichtsaufgabe. Und zwar eine Datenschutz-Aufsichtsaufgabe – auch beim Kantonalen Bedrohungsmanagement.

Digitalisierung braucht Vertrauen

Erhalt des Vertrauens der Bürger:innen Digitalisierungsprojekte nehmen zu. In sehr vielen Fällen sind dabei Personendaten im Spiel. Die Digitalisierung braucht das Vertrauen der Bürger:innen – unter anderem darein[1], dass auch in der digitalen Verwaltung ihre Grundrechte geachtet werden. Wenn solche Projekte unsorgfältig durchgeführt und die Grundrechte der betroffenen Personen verletzt werden, dann geht dieses Vertrauen verloren und ist – wenn überhaupt – nur schwer wieder zu gewinnen. Darum muss bei solchen Projekten zum Schutz der informationellen Selbstbestimmung[2] der Bürger:innen der Datenschutz rechtzeitig mitgedacht werden.

Präventiver Datenschutz

DSFA und Vorabkonsultation Der präventive Datenschutz, wie im vorangehenden Kapitel (vorne S. 13 ff.) beschrieben, soll dafür sorgen, dass bei datenschutzrelevanten Vorhaben der Datenschutz rechtzeitig mitgeplant wird. Neben den Technikgestaltungsprinzipien «Privacy by design» und «Privacy by default» dienen insbesondere die Datenschutz-Folgenabschätzung (DSFA) und die Pflicht zur Vorabkonsultation der/des DSB dem Zweck, rechtzeitig – nämlich bevor eine Datenbearbeitung die Grundrechte verletzt – das Risiko einer Grundrechtsverletzung möglichst auszuschliessen.

Pflicht und Umsetzung Wie vorne (S. 14 f.) beschrieben, muss das verantwortliche öffentliche Organ bei Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, vorab die/den DSB konsultieren.[3] Wir stellen fest, dass die Vorlage zur Vorabkontrolle (oder künftig eben: die Vorabkonsultation der/des DSB) bei gewissen öffentlichen Organen recht zuverlässig erfolgt, bei anderen allerdings leider nicht.

Festgestellte Defizite

Gründe für die Nicht-Umsetzung Warum vorabkonsultationspflichtige Vorhaben nicht wie vorgeschrieben zur Vorabkonsultation kommen, kann nicht abschliessend festgestellt werden – weil sie zum Teil gar nicht kommen, kann ja auch nicht nachgefragt werden, weshalb dem so sei. Hingegen zeigen unsere Erfahrungen mit denjenigen Vorhaben, die zu spät oder mit unvollständigen Unterlagen vorgelegt werden, dass die Nicht-Umsetzung verschiedene Gründe haben kann:

— Die öffentlichen Organe übersehen, dass ein Vorhaben vorabkonsultationspflichtig ist.

— Die öffentlichen Organe legen ein Vorhaben dem DSB zu spät zur Vorabkonsultation vor.

— Die Unterlagen zu den zur Vorabkonsultation vorgelegten Vorhaben werden unvollständig oder nicht in der erforderlichen Qualität eingereicht.

— Die aktuell verwendeten Dokumente (Schutzbedarfs- und Risikoanalyse) decken nicht alle datenschutzrechtlichen Prüfbereiche ab.

Übersehene Pflicht Wir haben keine Anhaltspunkte zur Annahme, dass die verantwortlichen öffentlichen Organe absichtlich versuchen, ihre Projekte an den Datenschutz- (und Informationssicherheits-) Stellen vorbei zu schmuggeln (*«project hiding»*). Darum sollte mit der Pflicht, bei allen Vorhaben eine DSFA durchzuführen, die Gefahr, dass ein öffentliches Organ übersieht, dass ein Vorhaben vorabkonsultationspflichtig ist, verringert werden können. Mit dem vorne (S. 15) erwähnten ersten DSFA-Schritt («Bestehen keine Datenschutz-Risikofaktoren?») kann >

schnell und ohne grossen Aufwand geklärt werden, ob ein konkretes Projekt eine vertiefte DSFA und allenfalls auch eine Vorabkonsultation der/des DSB braucht. Bestehen keine Risikofaktoren, ist dieser Befund – wie erwähnt – von den Verantwortlichen zu unterschreiben und zur Projektdokumentation zu nehmen, damit später nachgewiesen werden kann, dass die Projektleitung diese Prüfung vorgenommen hat. Bestehen hingegen Risikofaktoren, dann folgt im zweiten Schritt die vertiefte Auseinandersetzung mit den Risiken.

Verspätete Einreichung Eine fundierte Prüfung der zur Vorabkonsultation vorgelegten Dokumentation braucht ihre Zeit – je besser die Vorabkonsultation vorbereitet ist, umso rascher geht es. Wird ein Vorhaben erst kurz vor dem geplanten *Go-life* vorgelegt, dann ist eine regelkonforme Durchführung der Vorabkonsultation nicht möglich. Wenn ein öffentliches Organ sich über die Vorabkonsultation erkundigt, dann aber die erforderlichen Dokumente erst über anderthalb Jahre später und erst wenige Wochen vor dem geplanten *Go-life* vorlegt (und sich aus diesen Dokumenten in verschiedener Hinsicht nicht hinreichend nachvollziehen lässt, mit welchen Massnahmen das hohe Risiko für die betroffenen Personen ausgeschlossen oder verringert werden sollen), dann ist eine seriöse Aussage zur Frage, ob das Projekt datenschutzkonform umgesetzt werden kann, nicht gewährleistet. Die Aussage, die zuständigen Stellen hätten keine Zeit, die notwendige Dokumentation zu erstellen, zeigt, wo mindestens zum Teil die Probleme liegen.

Projekte werden offensichtlich nicht nach der vorgesehenen Projektmanagementmethode PM.BS abgewickelt.

Qualität und Vollständigkeit der Unterlagen Das dritte Defizit hat nach unserer Feststellung – gestützt auf die Erfahrungen bei Vorabkonsultationen – verschiedene Ursachen. Es beginnt damit, dass Projekte offensichtlich nicht nach der vorgesehenen Projektmanagementmethode PM.BS abgewickelt werden. In anderen Kantonen werden alle Projekte strikt nach einer vorgegebenen Projektmanagementmethode[4] abgewickelt, was dazu führt, dass standardmässig die Prozesse *(z.B. Rechtsgrundlagen-, Schutzbedarfs- und ggf. Risikoanalyse)* und die daraus resultierenden *Dokumentationen (wie zum Beispiel ein Informationssicherheits- und Datenschutz-Konzept)* klar vorgegeben sind. Eine weitere Ursache sehen wir darin, dass offensichtlich immer wieder nicht die «richtigen» Stellen einbezogen werden. Wenn Projektleiter:innen sagen, dass sie keine Rechtsgrundlagenanalysen oder Informationssicherheits- und Datenschutz-Konzepte (ISDS-Konzepte) erstellen können, dann mag das zutreffen – dann müssen einfach rechtzeitig die Rechtsabteilungen der Dienststellen oder Rechtsdienste der Departemente bzw. die Informationssicherheitsbeauftragten der Departemente (ISBD) beigezogen werden. Allenfalls sind, wenn diese Dienste ressourcenmässig nicht in der Lage sind, diese Unterstützung zu leisten, entweder die notwendigen Ressourcen zuzuordnen oder extern einzukaufen.

Dokumente Die aktuell im Zusammenhang mit der Informationssicherheit verwendeten Dokumente (insbesondere die Schutzbedarfs- und Risikoanalyse) decken die datenschutzrechtlichen Prüfbereiche nicht ab. Es werden fast ausschliesslich die Risiken für das Schutzziel der Verfügbarkeit erfasst und entsprechende Schutzmassnahmen vorgeschlagen. Die datenschutzrechtlich relevanteren Schutzziele der Vertraulichkeit und Integrität stehen weniger im Fokus.

Wirkung erhöhen

Zusammenarbeit Es ist unser Ziel, die Wirkung der Instrumente des präventiven Datenschutzes für die Zukunft zu erhöhen. Um dieses Ziel zu erreichen, tauschen wir uns seit geraumer Zeit mit der Geschäftsleitung von IT BS aus. IT BS muss ja durch die Integration der früheren Fachabteilung Informatiksteuerung und -organisation (ISO) auch deren Funktionen (mindestens vorübergehend) übernehmen. Zum Beispiel kann die zentrale Steuerung über aufeinander abgestimmte Dokumentenvorlagen sicher verbessert werden, und es können Standards in Form von Best practices eingefordert werden.

Hoffnung Wir hoffen, mit dieser engen Zusammenarbeit, in die auch die IT-Leiter:innen der Departemente und Gerichte einzubeziehen sein werden, Schritt für Schritt Verbesserungen zu erreichen. Es wäre sicher hilfreich, wenn die Abwicklung von IT-Projekten im Kanton einheitlicher strukturiert würde (und dabei DSFA und Vorabkonsultation implementiert werden) – und diese Vorgaben dann auch durchgesetzt würden. Unerlässlich wird der *Einbezug des entsprechenden fachlichen Knowhow* sein, zum Beispiel der zuständigen Rechtsdienste. Können die

erforderlichen Kompetenzen (Knowhow und Kapazitäten) nicht departements- oder dienststellenintern bereitgestellt werden, dann könnte auch geprüft werden, ob entsprechende (z.B. Projektmanagements-) Kompetenzen nicht zentral zur Verfügung gestellt werden und von den Projektverantwortlichen beigezogen werden müssen – wie dies zum Teil in Privatunternehmen auch gehandhabt wird.

Rolle der/des Datenschutzbeauftragten Die/der DSB hat von Gesetzes wegen eine Aufsichtsaufgabe; sie besteht aus Beratung und Kontrolle. Aber auch diese Beratungsaufgabe macht sie/ihn *nicht* zum *Rechtsdienst der verantwortlichen öffentlichen Organe.* Wenn beispielsweise im Sinne von § 7 Abs. 2 lit. b IDG Verträge mit Auftragsdatenbearbeiter:innen geschlossen werden müssen, dann können die DSB-Jurist:innen den Vertragsentwurf prüfen, aber sie schreiben ihn nicht. Genau dasselbe gilt für die Informatiker im DSB-Team: Sie sind nicht die *IT-Sicherheitsabteilung* der *verantwortlichen öffentlichen Organe* und legen nicht fest, wie die Informationssicherheit gewährleistet wird, sondern prüfen, was die Dienststellen oder Departemente an Massnahmen vorlegen. Diese sind und bleiben verantwortlich und müssen auch den Empfehlungen des DSB nicht zwingend folgen. Sie müssen sie aber in ihren Überlegungen berücksichtigen, tun gut daran, eine Nichtbeachtung gut begründen zu können, und tragen schliesslich die Verantwortung dafür, wenn sie sie ablehnen oder nicht umsetzen.

Kantonales Bedrohungsmanagement

Rolle der/des Datenschutzbeauftragten Die Rolle der/des DSB ist aktuell auch in anderem Zusammenhang zu klären: beim Kantonalen Bedrohungsmanagement (KBM).

Änderung des Polizeigesetzes Am 19. Mai 2021 hat der Grosse Rat die Änderungen des Polizeigesetzes (PolG)[5] im Zusammenhang mit dem Kantonalen Bedrohungsmanagement (KBM) beschlossen. Einem Bedrohungsmanagement ist eigen, dass nicht alle Datenbearbeitungen vorweg präzise geregelt werden können, weil es ja eben um die Reaktion auf ausserordentliche Situationen geht. In solchen Fällen ist es umso wichtiger, dass das konkrete Datenbearbeiten nachträglich unter die Lupe genommen wird. Genau so macht es der Kanton Basel-Stadt im Bereich des Staatsschutzes. Dort prüft nachträglich das Staatsschutzkontrollorgan mindestens stichprobenweise, ob die gesetzlichen Regeln eingehalten worden sind. Auf diesem Weg können allfällige Unschärfen der gesetzlichen Regelungen erkannt, in Ruhe analysiert und die Datenbearbeitungen für die Zukunft verbessert werden.

Vorschlag für eine Dienstaufsicht Im Vorfeld der Behandlung durch den Grossen Rat hat der DSB angeregt, im KBM ebenfalls eine solche nachträgliche Überprüfung einzuführen. Damit könnten einerseits Befürchtungen, die entsprechenden öffentlichen Organe würden überborden, anhand von Fakten nachträglich überprüft werden. Andererseits reduziert sich die Gefahr für die Mitarbeiter:innen, hinterher plötzlich wegen Rechtsverletzungen belangt zu werden.

Die/der Datenschutzbeauftragte hat eine Aufsichtsaufgabe und ist nicht der Rechtsdienst und nicht die IT-Sicherheitsabteilung der verantwortlichen öffentlichen Organe.

Kein spezielles Dienstaufsichtsorgan Weder hat der Regierungsrat diesen Ansatz in den Ratschlag und seinen Gesetzesrevisionsentwurf übernommen noch hatte ein entsprechender Antrag in der Parlamentsdebatte Erfolg. Hingegen hat der Grosse Rat eine zusätzliche Bestimmung ins Polizeigesetz eingefügt: «[1] Die oder der Datenschutzbeauftragte legt als unabhängige Aufsichtsstelle gemäss § 37 Abs. 1 IDG der Wahlbehörde jährlich einen speziellen Bedrohungsmanagement-Bericht im Sinne von § 50 IDG vor. Der Bericht äussert sich insbesondere über die durchgeführten Kontrollen gemäss § 45 IDG aufgrund der Aufgaben der oder des Datenschutzbeauftragten gemäss § 44 IDG.»[6]

Ende gut – alles gut? Leider nicht, denn Datenschutzaufsicht ist nicht Dienstaufsicht.

Datenschutzaufsicht ist nicht Dienstaufsicht

Beispiel Staatsschutzkontrollorgan Das, was das Staatsschutzkontrollorgan tut, ist ein Teil der *Dienstaufsicht*: «Die übergeordnete Verwaltungsbehörde hat die Befolgung der Gesetze und Verordnungen und die Einhaltung der Dienstbefehle und Weisungen zu überwachen. Sie kann u.U. die Entscheidungen der unteren Instanzen aufheben und selber entscheiden oder die Sache zur Neubeurteilung zurückweisen»[7]. >

Im Staatsschutzbereich wählt der Regierungsrat «zur Wahrnehmung der Dienstaufsicht durch die Vorsteherin oder den Vorsteher des Justiz- und Sicherheitsdepartements (…) ein aus drei Mitgliedern bestehendes Kontrollorgan»[8]. Hier prüfen somit besonders dafür ausgewählte Fachleute, ob die Aufgabenerfüllung des beaufsichtigten öffentlichen Organs rechtmässig und verhältnismässig ist.

Datenschutzaufsicht Etwas anderes ist die Datenschutzaufsicht. Die/der DSB überprüft (immerhin, aber auch nur), ob die ihrer/seiner Aufsicht unterstellten öffentlichen Organe datenschutzkonform handeln, also ob das Bearbeiten von Personendaten durch die beaufsichtigte Stelle im Sinne des Datenschutzes rechtmässig und verhältnismässig ist. Es ist keine umfassende Aufsicht, sondern eben nur eine *Datenschutzaufsicht.*

Die Frage, ob das KBM seine gesetzliche Aufgabe erfüllt, kann nicht aus rein datenschutzrechtlicher Warte beurteilt werden. Das hätte eben eine Verstärkung der Dienstaufsicht durch ein Fachorgan bedingt.

Unterschied An einem Beispiel illustriert, besteht der folgende Unterschied zwischen Datenschutzaufsicht und Dienstaufsicht. Die/der DSB prüft, ob eine bestimmte Erhebung oder Bekanntgabe von Personendaten durch die gesetzlichen Grundlagen gerechtfertigt und zur Zweckerreichung (d.h. der Aufgabenerfüllung des beaufsichtigten öffentlichen Organs) geeignet und erforderlich ist. Wenn hier also beispielsweise das KBM Personendaten *nicht* an eine Empfängerin (z.B. die Sozialhilfe) bekannt gibt, dann mag das datenschutzkonform sein: Es werden eben keine Personendaten weitergegeben und damit auch keine Datenschutzbestimmungen verletzt. Vielleicht wäre es aber zur Erfüllung der gesetzlichen Aufgabe des KBM gerade notwendig gewesen, die Personendaten an eine bestimmte Empfängerin weiterzuleiten. Dies zu beurteilen, ist Gegenstand der Fach- oder Dienstaufsicht, nicht aber der Datenschutzaufsicht im engeren Sinne.

Beschränkte Wirksamkeit In diesem Sinne wird mit § 61i PolG nur eine beschränkte Wirkung erreicht: Zwar kann die/der DSB im Rahmen ihrer/seiner Aufsichtstätigkeit beurteilen, ob die Datenbearbeitung durch das KBM datenschutzkonform erfolgt. Die Frage, ob das KBM seine gesetzliche Aufgabe erfüllt, kann aber nicht aus rein datenschutzrechtlicher Warte beurteilt werden. Das hätte eben eine – aber politisch offenbar nicht gewollte – Verstärkung der Dienstaufsicht durch ein Fachorgan bedingt.

1 Um zu verhindern, dass Sie hier einen Schreibfehler vermuten: «darein» ist korrekt. Der Duden merkt dazu an: «Adv. 1. Lokaladv. *zum Ausdruck der Bewegungsrichtung eines Gegenstands / Geschehens in eine räumliche (oder räumlich vorgestellte) Bezugsgröße hinein*: ‹in diesen Gegenstand, diesen Raum hinein›».
2 Art. 10 und 13 Abs. 2 BV; § 11 Abs. 1 lit. j KV/BS.
3 § 13 E-IDG (nach dem Ratschlag 21.1239.01) bzw. § 13 IDG (noch unter dem Namen Vorabkontrolle).
4 Oft HERMES, auf der auch PM.BS aufbaut.
5 Gesetz vom 13. November 1996 betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG), SG 510.100.
6 § 61i PolG.
7 Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 8., überarbeitete Auflage, Zürich/St. Gallen 2020, Rz. 1576.
8 § 3 Abs. 1 der Verordnung vom 21. September 2010 über den Vollzug des Bundesgesetzes zur Wahrung der inneren Sicherheit, SG 123.200.

Trend 4

In die Cloud? Viel mehr als ein blosser Releasewechsel!

Vor zwei Jahren haben wir an dieser Stelle auf die cloud-spezifischen Risiken hingewiesen. Inzwischen hat sich einiges getan: privatim hat die Schweizerische Informatikkonferenz SIK in Verhandlungen mit Microsoft unterstützt. Durch Corona ist der Drang der Verwaltung in Richtung Cloud nicht kleiner geworden, die Verlockung dank günstigen Angeboten grösser – die Abhängigkeit von (Fast-)Monopolist:innen aber auch. Der Richtungsentscheid muss umfassend geprüft und begleitet werden, sonst droht ein schwer rückgängig zu machender, mehr oder weniger grosser Verlust der direkten Kontrolle über Infrastruktur und Daten.

Trends

Fortschreitende Digitalisierung Die Digitalisierung schreitet unaufhaltsam voran. Langsam manchmal, manchmal eruptiv. Digitalisierung ist nicht a priori gut und nicht a priori schlecht. Es ist aber dafür zu sorgen, dass die Digitalisierung Menschen und Unternehmen in unserem Kanton nützt und auf keinen Fall zu ihren Lasten geht. Das ist der Staat ihnen schuldig.

Festzustellende Trends Wir stellen gewisse Trends fest:

— Immer mehr Anbieter:innen zügeln ihre Angebote in die Cloud. Microsoft versucht zu erreichen, dass ihre Kund:innen nicht on premises-Angebote, sondern möglichst Cloud-Angebote nutzen. SAP kündigt an, dass seine Dienste in absehbarer Zeit nur noch als Cloud-Dienste angeboten werden.

— Immer mehr Verwaltungsstellen wollen den hier wohnenden, arbeitenden oder den Kanton besuchenden Menschen Dienstleistungen in digitaler Form anbieten: Apps, über die man Informationen bekommen, etwas melden oder Bestellungen senden kann. Viele der im Internet angebotenen App-Lösungen haben Cloud-Komponenten – mehr oder weniger transparent ersichtlich.

— Verwaltungsstellen möchten vermehrt messen können, wie die angesprochenen Menschen oder Unternehmen ihre Angebote nutzen, und liebäugeln deshalb mit Tools, welche das Nutzer:innen-Verhalten analysieren.

— Immer mehr Nutzer:innen – auch Verwaltungsmitarbeiter:innen – erwarten, dass sie ihre Daten von möglichst allen Geräten aus zur Verfügung haben und bearbeiten können.

Datenschutzrechtliche Qualifikation

Auftragsdatenbearbeitung Der Beizug von Dritten, die Cloud-Dienstleistungen anbieten, stellt in der Regel[1] eine Auftragsdatenbearbeitung dar. Ein öffentliches Organ kann das Bearbeiten von Informationen an Dritte übertragen, wenn keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht[2]. Es bleibt für die Datenbearbeitung *verantwortlich*, auch wenn es diese auf Dritte übertragen hat[3]. Allein schon aus diesem Grund muss das öffentliche Organ sicherstellen, dass die Informationen durch die Auftragsdatenbearbeiter:innen nur so bearbeitet werden, wie es selber das auch tun dürfte[4]. Für solche Auslagerungen von Datenbearbeitungen hat der Datenschutzbeauftragte ein Merkblatt veröffentlicht[5]. Wichtig ist, wie es schon der Bundesrat in seiner Botschaft zum Erlass des (ersten) Bundesdatenschutzgesetzes[6] betont hat: Die Auslagerung von Datenbearbeitungen darf die betroffenen Personen nicht schlechter stellen, als wenn das verantwortliche öffentliche Organ die Personendaten selber bearbeitet.

Die Auslagerung von Datenbearbeitungen darf die betroffenen Personen nicht schlechter stellen, als wenn das verantwortliche öffentliche Organ die Personendaten selber bearbeitet.

Zusätzlich Cloud-Dienste Wenn jetzt auch noch Cloud-Dienstleistungen in Anspruch genommen werden, akzentuieren sich (auch, aber beileibe nicht nur aus Datenschutzsicht) bestimmte Risiken – Stichwort: Kontrollverlust. Diese Risiken gilt es im konkreten Fall zu vermeiden oder zu minimieren und, wenn sie nicht eliminiert werden können, gegenüber dem Nutzen abzuwägen. privatim hat dazu ein Merkblatt veröffentlicht[7]. Danach ist zuerst zu prüfen, ob eine Auslagerung überhaupt zulässig ist (§ 7 Abs. 1 IDG). Ist dies der Fall und soll bei der Auftragsdatenbearbeitung Cloud-Infrastruktur genutzt werden, sind anschliessend in einer *umfassenden Risikoabwägung* >

sämtliche, insbesondere jedoch die cloud-spezifischen Risiken zu prüfen. Das öffentliche Organ hat bei der Inanspruchnahme von Cloud-Dienstleistungen die spezifischen Risiken – nicht nur für die staatliche Aufgabenerfüllung, sondern auch für die Grundrechte der betroffenen Personen (z.B. Einwohner:innen oder Mitarbeiter:innen) – durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren.

Vorabkonsultation Nach den Voraussetzungen von § 13 IDG hat das öffentliche Organ Vorhaben dem DSB zur Vorabkonsultation[8] vorzulegen (vorne S. 14 f.). Das wird bei Cloud-Lösungen oft der Fall sein.

Gesetzliche Schweigepflichten

Vorgelagerte Fragestellung Im Rahmen der Vorabkonsultation führt der DSB eine *datenschutzrechtliche* Prüfung durch. *Vorgelagert* zu dieser Prüfung liegt die strafrechtliche Frage, ob die Auslagerung einer Datenbearbeitung (und insbesondere die Nutzung von Cloud-Diensten) eine Offenbarung eines besonderen Amts- oder Berufsgeheimnisses darstellt, ob dies gegebenenfalls einer Auslagerung der vom Geheimnis geschützten Informationen (i.S.v. § 7 Abs. 1 lit. a IDG) entgegensteht oder welche Massnahmen zum Schutz des Geheimnisses bzw. zur Rechtfertigung seiner Offenbarung zu treffen sind.

Nicht DSB, sondern vorgesetzten und/oder Aufsichtsorgane Es ist nicht Sache des DSB, sondern der vorgesetzten Behörden und/oder Aufsichtsbehörden, zu entscheiden, ob ein Berufs- oder besonderes Amtsgeheimnis einer Auftragsdatenbearbeitung entgegensteht. Es obliegt dem verantwortlichen öffentlichen Organ, diese Fragen mit der zuständigen Fachbehörde bzw. den vorgesetzten Behörden und/oder Aufsichtsbehörden zu klären.

Offenbaren Diese Behörden müssen die Tatbestandsmässigkeit einer bestimmten Auslagerung prüfen, also beurteilen, ob die konkrete Auslagerung ein unzulässiges Offenbaren und damit eine Verletzung eines Amtsgeheimnisses (Art. 320 StGB) oder Berufsgeheimnisses (Art. 321 StGB) darstellt. Schutzmassnahmen (wie etwa eine [wirksame!] Anonymisierung oder Pseudonymisierung oder eine Verschlüsselung) können dazu führen, dass die konkrete Auslagerung kein Offenbaren mehr darstellt.

Rechtfertigung durch Entbindung von der Geheimhaltungspflicht Wenn aber die konkrete Auftragsdatenbearbeitung ein Offenbaren darstellt, dann kann durch eine Rechtfertigung, wie im Strafgesetzbuch vorgesehen, die Strafbarkeit aufgehoben werden:

— bei Amtsgeheimnissen durch eine schriftliche Einwilligung der vorgesetzten Behörde[9] (Art. 320 Ziff. 2 StGB),

— bei Berufsgeheimnissen auf Grund einer Einwilligung der berechtigten Personen oder einer auf Gesuch des «Täters» erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde (Art. 321 Ziff. 2 StGB).

Es ist nicht Sache des DSB, sondern der vorgesetzten Behörden und/oder Aufsichtsbehörden, zu entscheiden, ob ein Berufs- oder besonderes Amtsgeheimnis einer Auftragsdatenbearbeitung entgegensteht.

Pauschalisierte Entbindung? Entbindungen sind klassischerweise Entscheidungen im Einzelfall. Es wäre zu prüfen, ob für Auftragsdatenbearbeitungen und die Inanspruchnahme von Cloud-Diensten eine Art «pauschalisierte Entbindung» durch die vorgesetzte bzw. Aufsichtsbehörde zulässig sein soll.

Berücksichtigung des Entscheides Der DSB seinerseits wird das Resultat dieser Prüfung beachten. Wenn also die zuständigen vorgesetzten bzw. Aufsichtsstellen entscheiden, dass eine Auslagerung der Datenbearbeitung in die Cloud kein unzulässiges Offenbaren darstellt oder dieses Offenbaren durch eine Entbindung gerechtfertigt werden kann, dann ist dieser Entscheid auch für den DSB bindend. Falls damit das Berufs- oder besondere Amtsgeheimnis nach Beurteilung der zuständigen Behörden einer konkreten Auslagerung nicht a priori entgegensteht, wird der DSB darauf hinwirken, dass die Daten, die einem Berufs- oder besondere Amtsgeheimnis unterstehen, durch angemessene Massnahmen so geschützt werden wie die besonderen Personendaten. Die Massnahmen, mit denen die Risiken beseitigt oder auf ein tragbares Mass verringert werden sollen, sind letztlich dieselben für besondere Personendaten und solche, die einem besonderen Amts- oder Berufsgeheimnis unterstehen.

Umfassende Risikoabwägung

Kein Freipass Auch wenn «keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht»[10], heisst das aber keineswegs, dass nun einfach Cloud-Dienste oder Online-Services genutzt werden dürfen. Es ist also kein Freipass für den «Gang in die

Cloud». Vielmehr muss eine umfassende Risikoabwägung stattfinden. Dabei sind die Risiken aufzuzeigen und zu bewerten, die dagegen wirkenden Schutzmassnahmen zu beschreiben, das verbleibende Risiko aufzuzeigen und gegenüber dem Nutzen abzuwägen. Zu berücksichtigen ist, dass die Datenschutzrisiken nie direkt das verantwortliche öffentliche Organ treffen, sondern die Personen, über die es Daten bearbeitet.

Risikoausschluss, -reduktion oder Verzicht Anzustreben ist, dass mit technischen, organisatorischen und rechtlichen Schutzmassnahmen die Risiken ausgeschlossen oder doch mindestens auf ein tragbares Mass reduziert werden können. Falls das nicht möglich ist, ist auf ein solches Projekt zu verzichten.

Vor dem «Gang in die Cloud» muss eine umfassende Risikoabwägung stattfinden. Dabei sind die Risiken aufzuzeigen und zu bewerten, die dagegen wirkenden Schutzmassnahmen zu beschreiben, das verbleibende Risiko aufzuzeigen und gegenüber dem Nutzen abzuwägen.

privatim-Aktivitäten

Unterstützung der SIK privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, ist – unter Mitwirkung des baselstädtischen DSB (bis November 2020 als Präsident, seither als Mitglied des Büroausschusses) – auch in diesem Bereich tätig geworden. Einerseits hat privatim die Schweizerische Informatikkonferenz (SIK) zum Thema Datenschutz in Verhandlungen mit Microsoft zu einem Rahmenvertrag, der für alle öffentlichen Organe der Schweiz – also auch die baselstädtischen – gilt, unterstützt und andererseits auch das Merkblatt zu Cloud-spezifischen Risiken und Massnahmen aktualisiert[11].

Kritische Aspekte Im Rahmen der Prüfung, ob die datenschutzrechtlichen Anforderungen bei einer Cloud-Lösung eingehalten sind, stehen die folgenden kritischen Aspekte im Vordergrund:

— anwendbares Recht und Gerichtsstand für Klagen;
— Person der Vertragspartnerin;
— Unterbeauftragte der Cloud-Anbieter:innen;
— Gleichbehandlung aller Personendaten;
— Schutz der Vertraulichkeit/Geheimnisschutz;
— Orte der Datenbearbeitung (und Möglichkeit des Zugriffs ausländischer Behörden);
— Zweckbindung (insb. Bearbeitung von Daten zu Zwecken der Auftragsdatenbearbeiterin);
— Audit-Recht;
— einseitige Vertragsänderung.

Diese Aspekte gelten *für Cloud-Lösungen generell*. Weil sowohl kantonsintern als auch in der interkantonalen Zusammenarbeit im Rahmen von privatim konkrete Fragestellungen im Zusammenhang mit *Microsoft 365 (M365)* behandelt wurden, nehmen die folgenden Ausführungen schwergewichtig auf diese Online-Dienste und die entsprechenden vertraglichen Regelungen Bezug. Aber auch bei anderen in Frage stehenden Cloud-Diensten gelten dieselben Überlegungen. >

Kurz & bündig

Der Drang in die Cloud ist riesig, auch weil viele Anbieter:innen on-premises-Lösungen längerfristig wohl gar nicht mehr anbieten wollen. Die Einführung von Microsoft 365 (M365) wird auch in unserem Kanton ins Auge gefasst. Dieser Schritt muss aber sehr gut überlegt und vorbereitet werden. Denn es geht keineswegs bloss um einen Releasewechsel, sondern um einen Richtungsentscheid, der einen zusätzlichen, schwer rückgängig zu machenden, mehr oder weniger grossen Verlust der direkten Kontrolle über Infrastruktur und Daten mit sich bringt.

Die in diesem Beitrag dargestellten kritischen Aspekte betreffen grundsätzlich alle Cloud-Dienste. Im konkreten Zusammenhang mit M365 konnten in den vergangenen zwei Jahren vertraglich mit Microsoft etliche Punkte geklärt werden – andere, wesentliche bleiben weiterhin offen. Sie sind in einer umfassenden Risikobeurteilung zu berücksichtigen: Für welche Kategorien von staatlichen Datenbearbeitungen kann die Inanspruchnahme von welchen Online-Services mit welchen Schutzmassnahmen ins Auge gefasst werden – für welche Kategorien muss darauf verzichtet werden?

Die kritischen Aspekte im Einzelnen

Anwendbares Recht und Gerichtsstand für Klagen Die Durchsetzung der vertraglichen Pflichten der Cloud-Anbieter:innen muss nach einer dem auftraggebenden öffentlichen Organ vertrauten Rechtsordnung vor für das Organ einfach zugänglichen Gerichten möglich sein. Die SIK hat 2020 mit Microsoft, mit der sie seit langem einen Rahmenvertrag hat, Verhandlungen geführt über das anwendbare Recht und den Gerichtsstand bei Datenschutzklagen. Dabei geht es nicht um die Anwendbarkeit des Datenschutzgesetzes, sondern des Vertragsrechts. Wenn ein baselstädtisches öffentliches Organ eine Auftragsdatenbearbeiterin bezieht, muss es sie durch Vertrag darauf verpflichten, das einzuhalten, was es selber aus dem IDG gegenüber den betroffenen Personen zu garantieren hat,[12] also beispielsweise, dass die Personendaten nicht unberechtigten Dritten zur Kenntnis gelangen. Wichtig ist in diesem Zusammenhang, dass auf diesen Vertrag dann Schweizer Recht (und nicht inhaltlich allenfalls abweichendes ausländisches Recht) anwendbar ist und dies vor einem Schweizer Gericht geltend gemacht werden kann.

Vertragspartnerin Es muss für das öffentliche Organ klar sein, wer seine Vertragspartnerin ist und als solche für alle datenschutzrechtlichen Verpflichtungen (auch ihrer Unterbeauftragten) einstehen muss, z.B. für M365: die Microsoft (Schweiz) GmbH, Microsoft Ireland Operations Ltd. (MIOL) oder die Microsoft Corp.?

Das verantwortliche öffentliche Organ muss über ein «Rückbauszenario» verfügen – auch, weil nach Vertragsablauf die Anbieterin vielleicht neue Bedingungen offeriert, welche für das öffentliche Organ nicht akzeptabel sind.

Unterbeauftragte der Cloud-Anbieter:innen Weil das öffentliche Organ für das Datenbearbeiten durch Dritte (Auftragsdatenbearbeiter:innen, *processors*) verantwortlich bleibt, auch wenn diese Unter(unter) auftragsdatenbearbeiter:innen beizieht, muss das öffentliche Organ entscheiden können, ob es die Verantwortung auch für diese Vierte oder Fünfte usw. übernehmen will. Es muss also erstens jederzeit *nachvollziehbar* sei, wer alles wie genau an der Auftragsdatenbearbeitung mitwirkt (bzw. noch vorher: künftig mitwirken soll), mit allen Informationen, die nötig sind zur Beurteilung des veränderten Risikos. Und zweitens muss das verantwortliche öffentliche Organ einen Beizug *ablehnen* können. Das kann, mindestens bei grösseren Cloud-Anbieter:innen, praktischerweise nicht ein Vetorecht gegen jeden Beizug jeder Unterauftragsdatenbearbeiterin sein; unerlässlich ist aber mindestens das Recht, innert einer praktikablen Frist vorzeitig aus dem Vertrag aussteigen zu können.[13] Damit dieses Recht nicht nur eine Alibi-Möglichkeit ist, muss das verantwortliche öffentliche Organ selbst über ein *«Rückbauszenario»* verfügen – nicht nur wegen dieser Ausstiegsmöglichkeit, sondern auch, weil nach Vertragsablauf die Anbieterin vielleicht neue Bedingungen offeriert, welche für das öffentliche Organ nicht akzeptabel sind.

Gleichbehandlung aller Personendaten Teilweise wurden Daten in den vertraglichen Regelungen unterschiedlich behandelt, je nachdem, ob es sich um «Kundendaten» (Daten, die das öffentliche Organ durch die Onlinedienste bearbeiten lässt), um weitere von der Anbieterin selbst erhobene oder um von den Onlinediensten generierte Daten handelt. Datenschutzrechtlich ist allein entscheidend, ob es sich um Personendaten handelt, also ob die Daten einen (direkten oder indirekten) Bezug zu einer (mindestens bestimmbaren) Person aufweisen (z.B. Einwohner:innen oder Mitarbeiter:innen). Für alle Personendaten, ob «Kundendaten», weitere erhobene oder von den Diensten generierte, gelten nach unserem Recht die datenschutzgesetzlichen Vorschriften – und das auftraggebende öffentliche Organ muss sicherstellen, dass diese auch von der Auftragsdatenbearbeiterin eingehalten werden.

Schutz der Vertraulichkeit/Geheimnisschutz (1) Das IDG verlangt, dass das öffentliche Organ Informationen (u.a.) vor dem Zugriff Unberechtigter schützt.[14] Die von Cloud-Anbieter:innen bearbeiteten *Personendaten* sind gegen unbefugte Zugriffe durch Dritte zu schützen. Unabhängig davon, ob es sich um «einfache» oder um besondere Personendaten handelt, sind alle Daten *zumindest* bei der Übertragung *(data in transit)* nach dem aktuellen Stand der Technik zu *verschlüsseln* und bei der Speicherung *(data at rest)* angemessen zu schützen (z.B. durch Verschlüsselung).

Schutz der Vertraulichkeit/Geheimnisschutz (2) Bei *besonderen Personendaten* (inkl. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) ist dem Umstand, dass bei Cloud-Dienstleistungen regelmässig Risiken für die Vertraulichkeit bestehen, zusätzlich Rechnung zu tragen. Deshalb sind erhöhte Anforderungen an den Schutz der Vertraulichkeit der Daten zu stellen und in der Risikoabwägung zu berücksichtigen:

— Die *Verschlüsselung* soll *durch das öffentliche Organ* erfolgen. Die Schlüssel dürfen nur für das öffentliche Organ verfügbar sein. Sie sind vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen.

— Nur wenn sich daraus *keine untragbaren Risiken für die Grundrechte der betroffenen Personen* ergeben (was vom öffentlichen Organ nachvollziehbar darzulegen ist), kann eine *Verschlüsselung bei den Cloud-Anbieter:innen* geprüft werden. Hierbei muss die Ebene, auf welcher die Verschlüsselung erfolgt (Applikation, Datenbank oder Festplatte), berücksichtigt werden. Die Schlüssel können allenfalls bei den Cloud-Anbieter:innen aufbewahrt werden,[15] wenn diese sich vertraglich verpflichten, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind zu protokollieren. Ausserdem müssen die Cloud-Anbieter:innen die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden können.

Ort der Datenbearbeitung: Geolokalisierung Je nach dem, wo Daten bearbeitet werden, können andere Gesetze gelten. Zum Beispiel können andere Staaten aufgrund ihres (in der Regel zwingenden) Rechts auf Daten in ihrem Land zugreifen. Aus diesem Grund sehen die schweizerischen und europäischen Datenschutzregeln[16] vor, dass Personendaten nur in Länder bekanntgegeben werden dürfen, in denen ein *angemessenes Datenschutzniveau* herrscht. Unser Grundrechtsschutz darf nämlich nicht einfach dadurch umgangen werden, dass Datenbearbeitungen ins Ausland ausgelagert werden. Die Anbieter:innen müssen deshalb offenlegen, in welchen Staaten sie ihre Cloud-Infrastruktur für die Bearbeitung von Personendaten betreiben und gegebenenfalls in welchen weiteren Staaten eine Bearbeitung (z.B. durch Unterauftragsdatenbearbeiter:innen) stattfindet, damit das verantwortliche öffentliche Organ die Zulässigkeit von Datenübermittlungen ins Ausland beurteilen und die Risiken in Bezug auf die Bearbeitungsorte bei der Risikoabwägung mitberücksichtigen kann. Dabei gilt:

— *Datenbearbeitungsstandorte in der Schweiz* sind zu bevorzugen (Sicherheit der Infrastruktur, z.B. in Bezug auf die Schutzziele Verfügbarkeit und Integrität, Zurechenbarkeit und Nachvollziehbarkeit, sowie Zugänglichkeit für Kontrollen).

Unser Grundrechtsschutz darf nicht einfach dadurch umgangen werden, dass Datenbearbeitungen ins Ausland ausgelagert werden.

— *Datenbearbeitungen an ausländischen Standorten*[17] sind nur in Staaten zulässig, die über ein gleichwertiges Datenschutzniveau verfügen[18] oder in denen ein angemessener Datenschutz vertraglich – namentlich durch anerkannte Standardvertragsklauseln – erreicht werden kann. Letzteres ist dann nicht zu erreichen, wenn im betreffenden Staat behördliche Zugriffe möglich sind, die den verfassungsmässigen Grundrechtsgarantien (Legalitätsprinzip, Verhältnismässigkeit, Rechte der betroffenen Personen, Zugang zu unabhängigen Gerichten) nicht genügen. Diesfalls sind zusätzliche Massnahmen (insbesondere wirksame Verschlüsselung) zu treffen, damit die Übermittlung von Personendaten ins Ausland zulässig ist. Der Datenexport in (oder Datenzugriff aus) Staaten ohne Einhaltung der Verfassungsgarantien ist *a priori* unzulässig, auch wenn kein Behördenzugriff erfolgt, aber ein solcher nicht ausgeschlossen werden kann[19].

Ort der Datenbearbeitung: Spezialfall USA Viele der grossen Cloud-Anbieter:innen kommen aus den Vereinigten Staaten. Das *Privacy Shield*-Regime[20] hatte für den Datenaustausch im kommerziellen Bereich gewisse Garantien gebracht, indem sich zertifizierte amerikanische Unternehmen zur Einhaltung der Schweizer Datenschutzgrundsätze verpflichteten. Doch hat das (für die Schweiz nicht verbindliche) Urteil *«Schrems II»* des Europäischen Gerichtshofs (EuGH)[21] den Angemessenheitsbeschluss der EU-Kommission zum *EU-US Privacy Shield* aufgehoben: Die USA zählen also nicht mehr zu den Staaten mit einem angemessenen Datenschutzniveau. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat sich dem für das *Swiss-US Privacy Shield*-Abkommen angeschlossen: Er hält in seiner Stellungnahme[22] und in der gestützt auf Art. 7 VDSG geführten Staatenliste[23] fest: «Datenbearbeiter, die >

in Bezug auf Personendaten, welche aus der Schweiz stammen, dem Regime Privacy Shield zwischen den USA und der Schweiz beitreten und auf der Liste des U.S. Department of Commerce verzeichnet sind, gewähren Personen in der Schweiz besondere Schutzrechte. *Letztere genügen den Anforderungen an einen angemessenen Datenschutz i.S. des DSG jedoch nicht.*»

Möglichkeit des Zugriffs ausländischer Behörden auf Daten an «sicheren» Speicherorten Selbst an «sicheren» Speicherorten besteht aber die Möglichkeit des Zugriffs ausländischer Behörden auf Daten. Dem US-amerikanischen CLOUD Act[24] unterstehende Anbieter:innen[25] müssen US-Behörden auch dann Zugriff auf gespeicherte Daten gewährleisten, wenn die Speicherung nicht in den USA, sondern z.B. in einem EU-Mitgliedstaat oder in der Schweiz erfolgt.

Zweckbindung: Datenbearbeitung für «legitime Geschäftstätigkeiten» von Microsoft Unter dem (alten) SIK-Rahmenvertrag behielt sich Microsoft das Recht vor, auf «Kundendaten» (Daten, die das öffentliche Organ durch die Onlinedienste bearbeiten lässt) und andere Personendaten des öffentlichen Organs für «legitime Geschäftstätigkeiten von Microsoft» zuzugreifen. Damit ist Microsoft nicht mehr Auftragsdatenbearbeiterin (*processor*), sondern wird zur Verantwortlichen (*controller*), der die Daten nicht mehr nur treuhänderisch anvertraut, sondern (wie einem Dritten) bekanntgegeben werden. Damit stellt sich die Frage, ob das öffentliche Organ über eine Rechtsgrundlage für eine solche Datenbekanntgabe verfügt bzw. ob die damit stattfindende Zweckänderung gerechtfertigt ist. Nur dann wäre eine solche Bekanntgabe zulässig.

Audit-Recht Das öffentliche Organ und die (Datenschutz-)Aufsicht müssen die Möglichkeit haben, im Bedarfsfall ein eigenes Audit durchzuführen. Das DPA sieht Prüfungen durch Microsoft selbst vor, welche sich jedoch auf die Informationssicherheit und nicht auf Datenschutzfragen (z.B. Einhaltung der Zweckbindung) beziehen.

Einseitige Vertragsänderung Es kann dem auftraggebenden öffentlichen Organ nicht zugemutet werden, dass Microsoft abgeschlossene Verträge einseitig abändern kann. Wesentliche Vertragsänderungen, wozu auch Datenschutzthemen gehören können, dürfen nur im gegenseitigen Einverständnis erfolgen.

Bezüglich M365 (teilweise) geklärte Punkte

Nur akzeptabel: anwendbares Recht und Gerichtsstand Dank der Unterstützung von privatim konnte erreicht werden, dass in einer Zusatzvereinbarung[26] für Klagen wegen Verletzung der Bestimmungen des Datenschutz-Amendments («DPA-Klagen») – nicht aber für andere Vertragsinhalte! – Schweizer Recht[27] gilt und die schweizerische Gerichtsbarkeit[28] zuständig ist – wenn auch *nicht bedingungslos*:

— Vor der Einreichung einer DPA-Klage (je nach Fall monetär oder nicht-monetär) müssen die zuständigen Datenschutzbehörden eine Abschätzung durchführen und der berechtigten Einrichtung (d.h. dem öffentlichen Organ, das den Vertrag mit Microsoft abgeschlossen hat) schriftlich bestätigen, dass die Rechte und Freiheiten der betroffenen Personen gefährdet würden (also bestätigen, dass es sich um eine *Datenschutzfrage* handelt und nicht [bloss] um einen Streit, ob die sonstigen Vertragspflichten eingehalten sind).

Es konnte erreicht werden, dass für Klagen wegen Verletzung der Bestimmungen des Datenschutz-Amendments («DPA-Klagen») Schweizer Recht gilt und die schweizerische Gerichtsbarkeit zuständig ist.

— Monetäre Klagen (d.h. Klagen, die auf Leistung einer Geldsumme gehen) können nur in der Schweiz eingereicht werden, wenn sie CHF 150 000 übersteigen. Unterhalb dieser Schwelle gilt irisches Recht und ist die Klage in Irland einzureichen.

Nur akzeptabel: «Streitwertgrenze» Der DSB geht davon aus, dass primär *Klagen zur Durchsetzung von Datenschutzpflichten* vor Schweizer Gerichten und nach Schweizer Recht beurteilt werden müssen, nicht Klagen auf eine Geldleistung. Ein öffentliches Organ soll – im Interesse des Schutzes der betroffenen Personen – in der Schweiz durchsetzen können, dass Microsoft die Datenschutzversprechen einhält; Klagen auf Geldleistung stehen hier nicht im Vordergrund. Aus diesem Grund erscheint der bedingte Gerichtsstand in der Schweiz – eben mit einer vertraglichen

«Streitwertgrenze» bei monetären Klagen – zwar nicht als gut, sondern *nur* (aber immerhin) und vorübergehend als *akzeptabel*. Es ist weiterhin dringend zu *fordern*, dass, wie im Rahmenvertrag von Microsoft mit Educa, der Fachagentur (von Bund und Kantonen) für den digitalen Bildungsraum Schweiz, *Schweizer Recht und Schweizer Gerichtsstand ohne weitere Bedingungen* gelten.

Vertragspartnerin Diese Frage ist für M365 inzwischen geklärt: Es ist MIOL (Microsoft Ireland Operations Ltd.), die dann als Auftragsdatenbearbeiterin die erforderlichen Standardvertragsklauseln (Standard Contractual Clauses, SCC) mit der Microsoft Corp. als Unterauftragsdatenbearbeiterin abschliesst.[29]

Gleichbehandlung aller Personendaten Das DPA vom September 2021 legt fest, dass nun alle Personendaten gleich behandelt werden.[30]

Zweckbindung Die Ziff. 3 der Zusatzvereinbarung[31] bringt hierzu einen Teil der Lösung: Danach ist der Zugriff auf den Inhalt von «*Kundendaten*» (Daten, die das öffentliche Organ durch die Onlinedienste bearbeiten lässt) für solche Geschäftstätigkeiten ausgeschlossen,[32] nicht aber auf die Daten über die Benutzer:innen (siehe hinten S. 28 f.).

Audit-Recht Ziff. 8 der Zusatzvereinbarung[33] erlaubt nun, dass die zuständigen Aufsichtsbehörden Prüfungen (durch anerkannte Revisionsgesellschaften) auf Kosten der Kund:innen (hier: des Kantons Basel-Stadt) durchführen lassen können, wenn das anwendbare Recht die Kund:innen verpflichtet, direkte Prüfungen durch die Aufsichtsbehörden zu gewährleisten. Damit kann § 45 IDG (Kontrollbefugnisse der/des DSB) erfüllt werden. Der Kanton, dessen auftraggebende öffentliche Organe die Verantwortung auch für das Datenbearbeiten durch die Auftragsdatenbearbeiter:innen tragen, muss unbedingt kontrollieren, ob dieses Recht auch ihm zusteht, oder sich dieses im Anschlussvertrag mit Microsoft einräumen lassen. >

Einschub: Das M365-Vertragswerk

Aktuell (seit 1. Mai 2022) gelten für die Vertragsbeziehungen zwischen Microsoft und öffentlichen Stellen in der Schweiz die folgenden Verträge und Vertragszusätze:

— *MBSA*: Microsoft Business- und Service-Vertrag (MBSA), Version MBSA2010Agr(WW) (GER)(Oct2010): Grundvertrag mit Definitionen, Regeln über die Nutzungsrechte, Vertraulichkeit, Garantien, Haftungsbeschränkung, Laufzeit und Kündigung usw.

— *SIK-Rahmenvertrag* (CTM 1-SIKFRAME2022) vom 17. Juni 2022 (rückwirkend gültig ab 1. Mai 2022): v.a. Regelungen zur Teilnahmeberechtigung, Rabattierung; zum Datenschutz: Fortführung der bisherigen Zusatzvereinbarung zum Datenschutz vom Herbst 2020 (SIKDPA2020), Verweis auf zusätzliche Vereinbarungen und Klärungen und auf Zusatzvereinbarung M329 (siehe unter dem nächsten Spiegelstrich) mit Klärungen im Zusammenhang mit den anwendbaren Standardvertragsklauseln.

— *Zusatzvereinbarung zum Datenschutz* (DPA2022) (CTM 1-SIKDPA2022): (= Fortführung des DPA2020) inkl. Anlage A, Zusatzvereinbarung für die Schweiz in Bezug auf den Datenschutz für Microsoft-Produkte und -Dienste (Addendum) (CTM-M329).

Der Kanton muss mit Microsoft einen *Anschlussvertrag* schliessen und kann sich darin weitere Zusicherungen geben lassen (z.B. im Zusammenhang mit dem anwendbaren Recht und Gerichtsstand, mit der Zweckbindung, mit dem Subcontracting, mit dem Schutz der Vertraulichkeit/dem Geheimnisschutz oder mit den Orten der Datenbearbeitung).

Einseitige Vertragsänderung Im aktuellen Vertragswerk[34] sind Klärungen vorgenommen worden, so dass die Microsoft erlaubten Vertragsänderungen als hinreichend eingeschränkt beurteilt werden können.

Weiterhin bezüglich M365 nicht hinreichend geklärte Punkte

Unterbeauftragte der Cloud-Anbieter:innen Microsoft stellt in seinem *Trust Center*[35] Informationen über die Unterauftragsdatenbearbeiter:innen zur Verfügung. Unseres Erachtens sind diese Informationen aber für eine sorgfältige Risikobeurteilung durch das auftraggebende öffentliche Organ *nicht ausreichend*; es trägt ja gegenüber den betroffenen Personen die Verantwortung auch für das, was Unter(unter)auftragsdatenbearbeiter:innen mit den Personendaten tun. Hier besteht *Nachbesserungsbedarf* bei der Transparenz. Ein besonderes Problem stellen Unter-(unter)auftragsdatenbearbeiter:innen in Ländern mit nicht als angemessen anerkanntem Datenschutzniveau dar. Dieses könnte aber – wie sogleich im nächsten Absatz unter dem Stichwort «Geolokalisierung» erwähnt – durch die «*EU Data Boundary for the MS Cloud*» entschärft werden, wenn sichergestellt ist, dass keine Datenbearbeitungen ausserhalb der EU stattfinden.

Die Anforderung, dass Personendaten nicht in Ländern ohne angemessenes Datenschutzniveau bearbeitet werden dürfen, kann durch die Umsetzung der «EU Data Boundary for the MS Cloud» erfüllt werden.

Geolokalisierung Für die Anforderung, dass Personendaten *nicht in Ländern ohne angemessenes Datenschutzniveau* (wie beispielsweise in den USA) bearbeitet werden dürfen, kann es zwei Lösungsmöglichkeiten geben:

— Entweder setzt Microsoft – wie angekündigt[36] bis Ende 2022 – die «*EU Data Boundary for the MS Cloud*» («EU-Datengrenze für Microsofts Cloud-Lösungen») so um, dass (für die vom öffentlichen Organ gewählten Dienste) *alle Datenbearbeitungen* ausschliesslich in Mitgliedstaaten der EU[37] erfolgen,[38] und/oder

— das US-amerikanische Datenschutzniveau wird als angemessen anerkannt, weil die USA entsprechendes Recht setzen[39] oder weil zwischen (der EU bzw.) der Schweiz und den USA ein neues Abkommen abgeschlossen wird, das Anforderungen definiert, die zur Anerkennung der Angemessenheit führen («Privacy Shield II»).[40]

Ohne eine solche Lösung wird eine umfassende Nutzung von MS-Onlinediensten schwierig werden (zum zusätzlichen Vorbehalt wegen des CLOUD Act siehe sogleich im nächsten Absatz). Es ist weitgehend anerkannt, dass vertragliche Regelungen (wie der Standardvertragsklauseln SCC) gegenüber (in der Regel zwingendem) öffentlichem Recht, das staatlichen Stellen einen Zugriff auf Daten erlaubt, keine Wirkung entfalten können.

Möglichkeit des Zugriffs ausländischer Behörden an «sicheren» Speicherorten (1) Die Übermittlung von Personendaten innerhalb der Schweiz oder der EU an Anbieter:innen, die unter dem US-amerikanischen CLOUD Act stehen, ist unseres Erachtens nicht schon unzulässig; hier wäre erst die tatsächliche Bekanntgabe an die US-Behörden unzulässig, weil sie sich weder auf eine Vereinbarung mit den USA stützt noch den gesetzlichen Vorschriften über die Rechtshilfe folgt. Das diesbezügliche Risiko ist nach unserer Auffassung einer *Risikobetrachtung* zugänglich.

Möglichkeit des Zugriffs ausländischer Behörden an «sicheren» Speicherorten (2) Das sehen aber nicht alle Datenschutzbeauftragten so:[41] Es wird auch die Ansicht vertreten, dass die potenzielle Herausgabepflicht eine Auftragsdatenbearbeitung durch dem CLOUD Act unterstehende Anbieter:innen grundsätzlich verbietet, womit mindestens alle amerikanischen Anbieter:innen ausser Betracht fallen. Auch ein Datenbearbeitungsort in der Schweiz oder in der EU schützt diesfalls nicht vor der Herausgabepflicht.

Möglichkeit des Zugriffs ausländischer Behörden an «sicheren» Speicherorten (3) Eine Risikobetrachtung aus datenschutzrechtlicher Sicht müsste sicher nach der «*Gefährlichkeit*» der in Frage stehenden Daten und Datenbearbeitungen für die Rechte der betroffenen Personen differenzieren. Das Risiko, soweit es nicht zum Ausschluss der Inanspruchnahme von Cloud-Lösungen führt, müsste zudem durch *vertragliche Massnahmen* reduziert werden, v.a. durch die Verpflichtung der Cloud-Anbieter:innen, alle Rechtsbehelfe zu ergreifen, um die Herausgabe der Daten zu verhindern, und das öffentliche Organ umgehend

über behördliche Herausgabebegehren zu informieren (soweit dies den Cloud-Anbieter:innen überhaupt erlaubt ist). Microsoft hat im aktuellen Vertragswerk die für sie möglichen Versprechen abgegeben.[42] Dieses bringt nun noch die Klarstellung, dass auch die schweizerischen (inkl. kantonalen) Datenschutzgesetze gleich wie die Datenschutz-Grundverordnung der EU (DSGVO) behandelt werden,[43] so dass auch deren Verletzung zur Anfechtung eines Herausgabebeschlusses und/oder eine Entschädigung der betroffenen Personen führen kann. Das Thema bleibt aber als Risiko in der Beurteilung zu berücksichtigen.

Zweckbindung Das aktuelle Vertragswerk[44] schliesst den Zugriff auf den Inhalt von «Kundendaten» für die erwähnten Geschäftstätigkeiten (vorne Ziff. 5.4) aus. Für die *Daten über die Benutzer:innen* der Online-Services bleibt die Situation aber *unbefriedigend*: Es ist klar, dass ein öffentliches Organ Microsoft nicht instruieren darf, solche Personendaten z.B. zur Berechnung von Mitarbeiterprovisionen oder Lieferantenprämien zu verwenden (im aktuellen Vertragswerk[45] wird deshalb zu Recht klargestellt, dass das DPA keine solche Weisung darstellt, die Microsoft die fraglichen Datenbearbeitungen als *processor* erlauben würde). Aber auch wenn Microsoft der Ansicht wäre, hier als *controller* zu handeln dürfen Personendaten, welche Microsoft im Rahmen der Vertragserfüllung anvertraut werden (dazu zählen auch die Daten über die Benutzer:innen), nicht für Zwecke verwendet werden, die dem auftraggebenden öffentlichen Organ nicht erlaubt wären. Microsoft erklärt, nicht alles zu tun, was nach den vertraglichen Bestimmungen als erlaubt erscheint: Es existiert ein *White Paper*[46], wonach Datenbearbeitungen für Geschäftstätigkeiten[47] von Microsoft in der Regel nur mit pseudonymisierten Daten erfolgen. Microsoft erklärt dieses Papier aber als vertraulich und nicht verbindlich. Inzwischen hat Microsoft privatim erlaubt, dieses *White Paper* an die privatim-Mitglieder zu verteilen und die öffentlichen Organe darauf hinzuweisen, dass jenes bei privatim oder Microsoft angefragt werden kann; es soll jedoch nicht frei öffentlich zugänglich gemacht, sondern nur in relevanten Einzelfällen an öffentliche Organe abgegeben werden. Wann darf ein auftraggebendes öffentliches Organ darauf vertrauen, dass Microsoft Daten nur so bearbeitet, wie es dies in dem *White Paper* darlegt? Damit solches *Vertrauen berechtigt* ist, muss das auftraggebende öffentliche Organ darauf bestehen, von Microsoft *verbindliche Zusagen* zu erhalten.

Verschlüsselung als Lösung?

Verschlüsselung Die Aspekte anwendbares Recht, Gerichtsstand, Vertraulichkeit/Geheimnisschutz, Orte der Datenbearbeitung, Möglichkeit des Zugriffs ausländischer Behörden und die Zweckbindung wären quasi von selbst für alle Daten erledigt, welche vom öffentlichen Organ so End-zu-End-verschlüsselt sind, dass die Auftragsdatenbearbeiter:innen sie gar nicht lesen können. Oft glauben öffentliche Organe, mit einer Verschlüsselung alle (oder doch die meisten) Risiken für die Vertraulichkeit – eines der vom IDG genannten Schutzziele (§ 8 Abs. 2 IDG) – beseitigen zu können. Voraussetzung dafür wäre aber eben eine wirksame *End-zu-End-Verschlüsselung*. Das ist in vielen Fällen aber gar nicht möglich. Zwar ist die Verschlüsselung durch die Cloud-Anbieter:innen auf dem Transportweg (*data in transit*) heute *state of the art* (wenn nicht, dann sollte die Verwaltung ohnehin die Finger von solchen Lösungen lassen). *Software-as-a-Service* (SaaS) kann mit vom öffentlichen Organ selbst verschlüsselten Daten nicht genutzt werden: Hier *muss* das System ja gerade Zugriff auf die zu bearbeitenden Daten haben. Hier kann eine Verschlüsselung durch das öffentliche Organ als technische Lösung – nach heutigem Stand der Technik[48] – nicht helfen. Abhilfe schaffen hier höchstens organisatorische oder rechtliche Massnahmen, indem die Anbieterin (vertraglich) verspricht, dafür zu sorgen, dass ihre Mitarbeiter:innen nicht auf die (unverschlüsselten oder nicht pseudonymisierten) Daten bzw. auf die Schlüssel greifen. Ob dieses Versprechen ausreicht, ist wiederum in der umfassenden Risikobeurteilung mit Blick auf den Schutzbedarf der Daten – einerseits aus Datenschutzsicht, andererseits aber auch aus Sicht der Aufgabenerfüllung – zu beurteilen.

Damit ein auftraggebendes öffentliches Organ berechtigt darauf vertrauen kann, dass Microsoft Daten nur so bearbeitet, wie es dies in dem White Paper darlegt, muss es darauf bestehen, von Microsoft verbindliche Zusagen zu erhalten.

Kritische Fragen bei SaaS-Lösungen Wird eine SaaS-Lösung vorgeschlagen, dann sind die folgenden Fragen zu beantworten:

— Ist eine *Software-as-a-Service*-Lösung (SaaS-Lösung) notwendig oder können die Aufgaben (wenigstens teilweise) auch mit *on-premises*-Lösungen erfüllt werden?

— Für welche der Dienste, die als SaaS-Dienste bezogen werden müssten, gibt es Alternativen und mit welcher Begründung können diese nicht genutzt werden? >

— Wenn es SaaS-Dienste braucht: Welche Massnahmen sind geplant, um die Risiken (insbesondere das potenzielle Schadensausmass) bei SaaS-Diensten zu reduzieren?

Bevorstehende Schritte

Die Hauptarbeit kommt erst Ist es mit den vertraglichen Regelungen und entsprechenden Zusagen der Cloud-Anbieter:innen – zum Beispiel von Microsoft für die Einführung von M365 – getan? Nein, denn die Hauptarbeit steht noch bevor: einerseits die *umfassende Prüfung* durch das *für die jeweilige Datenbearbeitung* verantwortliche öffentliche Organ (hinten S. 32), andererseits aber vorgängig das «Abstecken» eines verbindlichen Rahmens durch einen *Grundsatzentscheid und die Risikoübernahme durch den Regierungsrat* (hinten S. 32 f.), eventuell samt Einbezug des Grossen Rates (hinten S. 33).

Umfassende Prüfung Das öffentliche Organ muss umfassend prüfen:

— mit welchen Datenbearbeitungen es «in die Cloud gehen» darf,

— welche Online-Services es dafür nutzen darf und

— mit welchen Massnahmen die Risiken ausgeschlossen oder auf ein tragbares Mass reduziert werden.

Dabei sind alle vorne erwähnten Aspekte zu beachten. Insbesondere, wenn Anforderungen technisch nicht umsetzbar sind und/oder Anbieter:innen nicht alle geforderten Zusicherungen machen (z.B. im Zusammenhang mit dem anwendbaren Recht und Gerichtsstand, mit der Zweckbindung, mit dem Subcontracting, mit dem Schutz der Vertraulichkeit/dem Geheimnisschutz oder mit den Orten der Datenbearbeitung), dann muss das öffentliche Organ die entsprechenden Abwägungen vornehmen – zum Beispiel prüfen, ob für die betroffenen Personen keine untragbaren Risiken entstehen, wenn die Verschlüsselung nicht durch das öffentliche Organ, sondern bei Cloud-Anbieter:innen erfolgen soll – und je nach Ergebnis auf die Nutzung der Cloud-Dienste bzw. der SaaS-Dienste verzichten.

Umsetzung Selbstredend brauchen diese Schritte entsprechende Ressourcen:

— sicher bei IT BS, sowohl bei der Vorbereitung als auch beim Betrieb, aber auch

— bei den Departementen und Dienststellen (oder entsprechenden Organisationseinheiten z.B. in den Gemeinden), welche insbesondere bei der Vorbereitung auf Seiten der verantwortlichen öffentlichen Organe sehr stark in der Risikobeurteilung beansprucht werden, und

— bei der/dem Datenschutzbeauftragten, welche/welcher die Aufsicht sowohl bei der Vorbereitung (Beratung, Vorabkonsultation) als auch beim Betrieb (Überwachung) sicherstellen muss.

1 Datenschutzrechtlich relevant ist eine Auftragsdatenbearbeitung, wenn Personendaten im Spiel sind. Dies ist heute praktisch immer der Fall, weil selbst dann, wenn die Inhaltsdaten reine Sachdaten sind, aber Daten über bestimmbare Mitarbeiter:innen der öffentlichen Organe von der Auslagerung (mit-) betroffen sind.
2 § 7 Abs. 1 lit. a IDG.
3 § 7 Abs. 2 IDG.
4 § 7 Abs. 1 lit. b IDG.
5 Link auf der Website des DSB: https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html.
6 Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (BBl 1988 II 413, S. 463), zum damaligen Art. 11 E-DSG.
7 Vgl. dazu das privatim-Merkblatt Cloud-spezifische Risiken und Massnahmen auf der Website des DSB: https://www.dsb.bs.ch/handreichungen/privatim-merkblatt-cloud.html (letzte Version: 03.02.2022).
8 Die Stellungnahme bedient sich bereits der Terminologie der Teilrevision des Informations- und Datenschutzgesetzes, die zurzeit vom Grossen Rat beraten wird: Vorabkonsultation statt Vorabkontrolle.
9 Als «vorgesetzte *Behörde*» verstehen wir nicht die vorgesetzte Person innerhalb derselben Behörde (also nicht die Abteilungsleiterin als Vorgesetzte des Teamleiters), sondern die nächsthöhere *Behörde* (also der Bereich, in dem sich die Dienststelle befindet, oder das Departement, in dem sich der Bereich, die Abteilung oder Stabsstelle befindet).
10 § 7 Abs. 1 lit. a IDG.
11 Vgl. dazu das privatim-Merkblatt Cloud-spezifische Risiken und Massnahmen (Fn. 7).
12 § 7 Abs. 1 lit. b IDG.
13 So z.B. von Microsoft angeboten im DPA (12.2020), S. 11 unten/12 oben.
14 § 8 Abs. 1 und Abs. 2 lit. a IDG.
15 Vgl. dazu die neuen Bestimmungen in Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 6, Ziff. 10 (Kunden-Lockbox).
16 Zum Beispiel § 23 IDG, Art. 6 DSG, Art. 16–18 revDSG, Art. 2 ZP zur ER-Konv 108, Art. 14 ER-Konv 108+, Art. 36 der Richtlinie (EU) 2016/680.
17 Als Datenbearbeitung im Ausland ist auch der Zugriff auf in der Schweiz gespeicherte Daten von einem Standort im Ausland aus (z.B. für Supportleistungen) anzusehen, da dabei die Daten mindestens temporär ins Ausland übermittelt werden.
18 Vgl. die Länderliste des EDÖB unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.
19 Ebenso der Europäische Datenschutz-Ausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Angenommen am 18. Juni 2021, https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementary measurestransferstools_de.pdf.
20 Für die Schweiz: zum US-Swiss Privacy Shield vgl. https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html; für die EU: zum US-EU Privacy Shield siehe https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:207:FULL&from=DE.
21 Urteil des Europäischen Gerichtshofs /Grosse Kammer) in der Rechtssache C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd und Maximilian Schrems, http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18.
22 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Stellungnahme (vom 8. September 2020) zur Übermittlung von Personendaten in die USA und weiterer Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, Ziff. 3.3 am Ende (Hervorhebung im Original fett).
23 «Länderliste» des EDÖB (aktuelle Fassung vom 15.11.2021, S. 12), unter https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/20211115_L%C3%A4nderliste_d.pdf.
24 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, https://www.congress.gov/bill/115th-congress/house-bill/4943.
25 Vgl. zur Frage, wer dem CLOUD Act untersteht, das Whitepaper des US-Justizdepartements von April 2019, insb. S. 8: https://www.justice.gov/opa/press-release/file/1153446/download.
26 Zusatzvereinbarung zu den Vertragsunterlagen, Konzernvertrag, Anwendbarer Nachtrag zum Datenschutz (DPA), Version August 2020.
27 Zusatzvereinbarung ID CTM (1-SIKDPA2022): S. 3 (Anwendbares Recht).
28 Zusatzvereinbarung ID CTM (1-SIKDPA2022): S. 2 (Streitbeilegung).
29 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 1 in Verbindung mit der Tatsache, dass der Vertrag, mit dem die berechtigten öffentlichen Organe Produkte und Dienste abonnieren, mit Microsoft Ireland Operations Ltd. abgeschlossen wird.
30 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 3 (Kundendaten und Professional Services-Daten).
31 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 3 (Kundendaten und Professional Services-Daten).
32 Ausnahme: zur Erfüllung von rechtlichen Verpflichtungen von Microsoft.
33 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 6, Ziff. 8 (Prüfungsrecht).
34 Zusatzvereinbarung ID CTM (1-SIKDPA2022): S. 1 (Beschränkungen der Aktualisierungen bzw. Neue Features, Ergänzungen oder zugehörige Software) und Anlage A, S. 5, Ziff. 7 (Änderungen und Verfügbarkeit der Onlinedienste).
35 https://www.microsoft.com/de-ch/trust-center/privacy.
36 https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/ bzw. https://news.microsoft. com/de-de/unsere-antwort-an-europa-microsoft-er-moeglicht-speicherung-und-verarbeitung-von-daten-ausschliesslich-in-der-eu/.
37 Inkl. Norwegen und die Schweiz.
38 Heute garantiert Microsoft das erst für die Datenspeicherung *(«data at rest»)*: Für diese Daten wird durch Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 9 (Kundendaten im Ruhezustand für Azure-Kerndienste) neu zugesagt, dass sie «*nur* innerhalb der angegebenen Geo» (Hervorhebung nicht im Original) gespeichert werden. Das bringt zusätzliche Verbindlichkeit und damit Sicherheit.
39 Der amerikanische Kongress arbeitet zurzeit an einem American Data Privacy and Protection Act (ADPPA). Ob dieses Gesetz in der letztlich verabschiedeten Form zu einem angemessenen Datenschutzniveau führt, wird sich noch zeigen müssen.
40 Skeptiker:innen könnten anmerken: mindestens bis zum nächsten entsprechenden EuGH-Urteil …
41 Noch unentschieden: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Stellungnahme zur Datenschutz[-]Risikobeurteilung der Suva zum Projekt Digital Workplace «M365», downloadbar auf der Seite https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1587794875.
42 Beilage M329 (Zusatzvereinbarung ID CTM [1-SIKDPA2022], S. 8), Klausel 1 (Aufforderung zur Bestellung: Pflicht zur Anfechtung einer Anordnung zur Offenlegung) und Klausel 2 (Entschädigung der betroffenen Person für den Schaden, welcher der betroffenen Person durch die Offenlegung auf Anordnung einer nicht-schweizerischen Behörde entsteht).
43 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 2 (Einhaltung von gesetzlichen Regelungen); Beilage M329 (Zusatzvereinbarung ID CTM [1-SIKDPA2022], S. 7, Definition von «Datenschutzanforderungen» und S. 8, Anhang C, Präambel.
44 Vorne Fn. 31.
45 Anlage A der Zusatzvereinbarung ID CTM (1-SIKDPA2022), S. 4, Ziff. 5 (Dokumentierte Weisungen).
46 *Microsoft Data Protection & Security Terms for Online Services: Legitimate Business Operations*, uns zur Verfügung gestellt in der Version von Juni 2020.
47 Z.B. Abrechnung und Vergütung, Kapazitätsplanung und Produkteentwicklung, Betrugsbekämpfung und Abwehr von (Cyber-)Angriffen, Einhaltung rechtlicher Bestimmungen.
48 Vgl. dazu Michael Herfert/Benjamin Lange/Dominik Spychalski, Verschlüsselung in der Cloud, digma 2019, S. 128 ff.

Trend 5

In die Cloud? Eine grosse Aufgabe für den Regierungsrat

Auch wenn die vertraglichen Regelungen besser werden: Für den Entscheid, für welche Kategorien von Datenbearbeitungen Online-Dienste (z.B. M365) genutzt werden dürfen, braucht es eine umfassende Risikoabwägung. Angesichts der Tragweite des Entscheides muss der Regierungsrat den Grundentscheid für die kantonale Verwaltung treffen. Er muss auch die Verantwortung übernehmen, für die notwendigen Prozesse und Organisation, ein Monitoring und Reporting, kurz: für eine Cloud-Governance sorgen. Allenfalls ist der Einbezug des Grossen Rates ratsam.

Ein «besserer Vertrag» ist kein Freipass

Umfassende Risikoabwägung Im vorangehenden Kapitel (vorne S. 21 ff.) werden die kritischen Aspekte der Inanspruchnahme von Online-Services (insbesondere M365) inhaltlich dargestellt. Es wird gezeigt, wo inzwischen die vertraglichen Grundlagen verbessert worden sind und wo von Microsoft noch nachgebessert werden muss. Ein «besserer Vertrag» ist aber noch kein Freipass für den «Gang in die Cloud». Vielmehr muss dann in einer umfassenden Risikoabwägung entschieden werden, für welche Kategorien von Datenbearbeitungen welche Online-Dienste mit welchen Schutzmassnahmen genutzt werden dürfen. Die Verantwortung für das datenschutzkonforme Bearbeiten von Personendaten trägt grundsätzlich das öffentliche Organ, das die Daten zur Erfüllung seiner gesetzlichen Aufgabe bearbeitet.[1]

Risikoübernahme

Risikoträger:innen Wer muss den Entscheid, dass ein Cloud-Dienst genutzt wird, treffen (und verantworten)?

— Die *IT-Dienstleisterin* (Departements-IT oder IT BS)? Nein, sie hat primär die Anforderungen, die an sie gestellt werden, zu erfüllen und kann mithelfen, die (technischen) Risiken zu erkennen und einzuschätzen und die (technischen) Vorkehrungen und Schutzmassnahmen zum Ausschluss bzw. zur Minimierung der Risiken vorzuschlagen.

— Die *Dateneigner:innen* (in der Regel die Dienststellenleitung)? Ja, grundsätzlich ist das öffentliche Organ, das zur Erfüllung seiner gesetzlichen Aufgabe Personendaten bearbeitet, nach dem Informations- und Datenschutzgesetz für den Umgang mit Informationen verantwortlich, auch wenn es die Daten zur Erfüllung seiner gesetzlichen Aufgabe durch Dritte (die Auftragsdatenbearbeiterin) bearbeiten lässt. Allerdings können die Dateneigner:innen diesen Entscheid – ausser vielleicht bei kleinen, wenig sensitiven Vorhaben, bei denen keine besonderen Personendaten und keine Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen, bearbeitet werden – *nicht einfach nach eigenem Gutdünken* und aufgrund des eigenen Risikoappetits treffen. Die Departementsvorsteher:innen verantworten die Summe der Risiken aus ihrem Departement, weshalb sie rechtzeitig zu involvieren sind.

Beim Gang in die Cloud geht es um einen Richtungsentscheid, der einen zusätzlichen, schwer rückgängig zu machenden, mehr oder weniger grossen Verlust der direkten Kontrolle über Infrastruktur und Daten mit sich bringt.

— Für «grössere» Schritte in die Cloud – sicher jedoch, wenn es um die grundsätzliche Einführung von Online-Services bzw. SaaS-Services (wie z.B. M365) für die Verwaltung und die Dienststellen gar keine Alternative mehr haben – muss der Entscheid wegen der *Tragweite* des Vorhabens mindestens vom *Regierungsrat* gefällt werden. Es geht keineswegs bloss um einen Releasewechsel; es geht um einen Richtungsentscheid, der einen zusätzlichen, schwer rückgängig zu machenden, mehr oder weniger grossen Verlust der direkten Kontrolle über Infrastruktur und Daten mit sich bringt. Der Regierungsrat hat in vollständiger Kenntnis der Risikoabwägung, der Alternativen, der Ausgestaltung (welche Bereiche in die Cloud, welche on-premises) und des «Ausstiegs-» oder «Rückbauszenarios» darüber zu entscheiden, ob er die Risiken als tragbar erachtet. Er trägt letztlich die *Gesamtverantwortung* und hat für ein angemessenes Risikomanagement zu sorgen.

Die Rolle der/des DSB Die/der Datenschutzbeauftragte nimmt im Rahmen einer Vorabkonsultation Stellung zu den Vorhaben, die ihr/ihm vorgelegt werden (dazu auch vorne S. 14 und 17 ff.). Sie/er prüft das Vorhaben in datenschutzrechtlicher Hinsicht,[2] also auf seine Datenschutzkonformität hin. Ergibt die Beur-teilung Nachbesserungsbedarf, kann sie/er *Empfehlungen* nach § 46 IDG abgeben. Das ist Ausdruck ihrer/seiner Aufsichtsverantwortung. Das öffentliche Organ, an das die Empfehlung gerichtet ist, hat ihr/ihm gegenüber zu erklären, ob es der Empfehlung folgen will oder nicht (§ 46 Abs. 2 IDG). Die Verantwortung für diesen Entscheid liegt beim öffentlichen Organ – es kann die Empfehlung auch ablehnen und bleibt verantwortlich. Die/der DSB wiederum kann die Empfehlung oder Teile davon, falls das Interesse an ihrer Durchsetzung schwer wiegt, als Weisung in Form einer Verfügung erlassen (§ 47 Abs. 1 IDG).

Berücksichtigung der Empfehlungen Im Zusammenhang mit dem Entscheid über die Zulässigkeit der Nutzung von Online-Services ist der Regierungsrat nicht auf die «Zustimmung» der/des DSB angewiesen. Der Regierungsrat tut hingegen gut daran, dafür zu sorgen, dass die Empfehlungen der/des DSB in die Gesamtabwägung einbezogen und beim Entscheid angemessen berücksichtigt werden.

Mindestinhalt des regierungsrätlichen Grundsatzentscheides

Cloud-Governance Zum notwendigen Grundsatzentscheid des Regierungsrates gehört aber nicht nur der Entscheid, dass die Verwaltung Online-Services (z.B. M365) nutzen dürfe bzw. solle. Der Regierungsrat muss:

— grundsätzlich entscheiden, welche *Risiken* bei der Nutzung von Online-Services für welche Kategorien von Datenbearbeitungen tragbar erscheinen – und dafür die *Verantwortung* übernehmen;

— für die *Prozesse* sorgen, mit denen für jede Kategorie von Datenbearbeitungen geprüft wird, ob und, wenn ja, mit welchen (technischen, organisatorischen und rechtlichen) Schutzmassnahmen Online-Services genutzt werden dürfen;

— für die *Organisation* sorgen, mit der sichergestellt wird, dass die Prozesse regelkonform abgewickelt werden, inkl. Zuordnung der Kompetenzen, stufengerecht über die Nutzung von Online-Services für bestimmte Kategorien mit geringerem Risiko zu entscheiden;

— ein «*Ausstiegs*-» oder «*Rückbauszenario*» erstellen lassen und abnehmen;

— für ein wirksames Monitoring sorgen, das den permanenten Überblick über die Risiken garantiert;

— für ein regelmässiges *Reporting* über alle Verwaltungsstufen bis zu ihm sorgen;

— mindestens jährlich die *Risikolage beurteilen* und ggf. die notwendigen Massnahmen anordnen;

— kurz: für eine *Cloud-Governance* sorgen.

Der Regierungsrat muss grundsätzlich entscheiden, welche Risiken bei der Nutzung von Online-Services für welche Kategorien von Datenbearbeitungen tragbar erscheinen – und dafür die Verantwortung übernehmen.

Einbezug des Grossen Rates Falls der Regierungsrat den Entscheid über den «Gang in die Cloud» nicht allein tragen mag, kann (und von der Tragweite her – immerhin geht es wie vorne erwähnt um die Frage eines zusätzlichen Kontrollverlusts – sollte) er den Grossen Rat mit einbeziehen:

— mindestens durch *periodische Berichte* über die getroffenen Entscheide und Massnahmen oder,

— wie es im Kanton Freiburg geschehen ist, indem er dem Grossen Rat den *Erlass spezifischer gesetzlicher Bestimmungen* beantragt: Dort hat der Gesetzgeber im kantonalen Datenschutzgesetz[3] in vier Artikeln die Auslagerung genauer geregelt (Art. 12b: Grundsätze, Art. 12c: Verantwortung, Art. 12d: Sicherheitsmassnahmen, Art. 12e: Massnahmen für besonders schützenswerte Personendaten). Auch wenn die konkreten freiburgischen Bestimmungen vielleicht noch nicht der Weisheit letzter Schluss sind,[4] so übernimmt damit doch der Gesetzgeber für diesen Grundsatzentscheid stufengerecht die Verantwortung, und die in den gesetzlichen Bestimmungen festgelegten Auflagen stärken die Verwaltung als Bestellerin gegenüber Anbieter:innen.

Weiteres Vorgehen

Programm, nicht einmaliger Entscheid Der Grundsatzentscheid, Cloud-Dienste für staatliche Datenbearbeitungen zuzulassen, ist nicht ein in den nächsten Wochen oder Monaten rasch zu treffender Regierungsratsbeschluss. Ein Regierungsratsbeschluss kann – und so ist es inzwischen geplant – ein *Programm-Startschuss* sein und für die Bereitstellung der entsprechenden Mittel für die Vorbereitung sorgen (Budgetierung). Dabei geht es nicht schon darum, alle Fragen zu beantworten, sondern vielmehr, dafür zu sorgen, dass alle Fragen auf den Tisch kommen, für die dann in der nächsten Phase Antworten zu finden sind.

>

Phasengerecht umfassende Beurteilung und Risikoübernahme Im Rahmen dieses Programms muss der Regierungsrat in mehreren Phasen aktiv werden. Mit einer «einmaligen Freigabe» – im Sinne von «aus den Augen – aus dem Sinn» – ist es keinesfalls getan. So wird aber zurzeit der entsprechende Regierungsratsbeschluss im Kanton Zürich[5] wahrgenommen – oder eine solche Wahrnehmung wird durch Berater geschürt: «Grünes Licht für M365»[6]. Ausserdem wurde argumentativ schwergewichtig die Gefahr des *Lawful access* durch ausländische Behörden behandelt.[7] Die Datenbekanntgabe in oder die Möglichkeit der Datenzugriffe aus Staaten ohne angemessenen Datenschutz ist, wie vorne (S. 25 f. und 27 f.) ausführlich gezeigt wurde, *ein* Aspekt, aber weder der einzige noch der wichtigste.[8] Wichtig ist, dass der Regierungsrat als Träger der Gesamtverantwortung festlegt, *welches Risiko er übernimmt* bei der Nutzung von Cloud-Diensten durch die ihm unterstellte Verwaltung – und dass er dafür sorgt, dass die Verwaltung innerhalb dieses Risikos bleibt.

Sachliche und realistische Darstellung Erforderlich ist eine fundierte und *sachliche Darstellung* der Chancen und Risiken. Es wäre nicht dienlich, für die Beurteilung einfach Texte aus den Werbebroschüren der Anbieter:innen zu kopieren. Vielmehr müssen *transparent, sachlich und realistisch* die Chancen und Risiken dargestellt werden, die der «Gang in die Cloud» mit sich bringt:

— die zu erwartenden *positiven Auswirkungen* (z.B. auf die Prozesse und auf die Organisation staatlicher Aufgabenerfüllung, aber eben nicht bloss Marketing«versprechen», an denen erfahrungsgemäss ein paar Jahre später niemand gemessen werden möchte!) und

— die *damit einhergehenden Risiken* (nicht bloss Projekt- oder Programmrisiken, sondern negative Auswirkungen z.B. auf die Prozesse und Organisation staatlicher Aufgabenerfüllung, z.B. das Risiko des Kontrollverlusts über die Infrastruktur, die Software und die Daten, die Abhängigkeit von Anbieter:innen, insb. wenn diese Quasi-Monopolist:innen sind – und die Risiken für die Grundrechte der betroffenen Personen).

Transparenz Der Regierungsrat kann – wie vorne (S. 19) erwähnt – Interessen und Risiken aus einer Gesamtsicht selbstverständlich anders gewichten, als dies die/der Datenschutzbeauftragte tut. Er kann beispielsweise aus finanziellen Gründen auf von der/dem DSB empfohlene Schutzmassnahmen verzichten oder aus finanziellen Überlegungen ein Angebot trotz Datenschutzbedenken auswählen – dann soll er aber Transparenz schaffen und den Verzicht oder die Inkaufnahme des Risikos auch entsprechend begründen.

Es wäre nicht dienlich, für die Beurteilung einfach Texte aus den Werbebroschüren der Anbieter:innen zu kopieren. Vielmehr müssen transparent, sachlich und realistisch die Chancen und Risiken dargestellt werden, die der «Gang in die Cloud» mit sich bringt.

Umsetzung Nicht zu vergessen: Das Programm braucht zur Umsetzung auch Ressourcen – bei IT BS, aber auch bei den Departementen und Dienststellen und bei der/dem Datenschutzbeauftragten (vorne S. 30).

Zu guter Letzt: fehlende digitale Souveränität als Sicherheitsrisiko

Abhängigkeit Ob Cloud oder nicht, ob Microsoft oder andere Anbieter:innen: Das Problem, mit dem sich die Verwaltung (wie die Privatwirtschaft) herumzuschlagen hat, ist die Abhängigkeit: die immer grössere Abhängigkeit von der Informatik generell und – vor allem – die wachsende Abhängigkeit von wenigen Grossanbieter:innen. Dass diese meistens auch noch aus den USA (oder neuerdings auch aus China, das aber ebenfalls nicht auf der Liste der Staaten mit einem angemessenen Datenschutzniveau figuriert) kommen, macht es auch nicht einfacher. Europa hat es im letzten Vierteljahrhundert versäumt, für eine digitale Souveränität zu sorgen. Im Bereich der digitalen Infrastruktur[9] von solchen Anbieterinnen abhängig zu sein, wird uns noch lange vor grosse Herausforderungen stellen. Es ist dringend, dass wir – die Schweiz und Europa – die digitale Infrastruktur als kritische Infrastruktur anerkennen und die Abhängigkeit von Grossanbieter:innen zu verringern versuchen.

Die Abhängigkeit bekommen öffentliche Organe auch zu spüren, wenn (Fast-)Monopolist:innen bei Ablauf der Verträge die Vertragsbedingungen ändern oder Preise erhöhen – zum Teil deutlich erhöhen.

(Fast-)Monopolist:innen

Die Schaffung dieser digitalen Souveränität kann logischerweise nicht von einem Kanton gestemmt werden. Auf der anderen Seite wäre es auch nicht gescheit, diesbezüglich die Hände in den Schoss zu legen und die Abhängigkeit als naturgegeben anzuschauen. Zu spüren bekommen sie auch öffentliche Organe, wenn etwa (Fast-) Monopolist:innen bei Ablauf der Verträge die Vertragsbedingungen ändern oder Preise erhöhen – zum Teil deutlich erhöhen. Dann tut es weh. Kann der Kanton faktisch überhaupt und innert nützlicher Frist aus einem Vertrag mit Microsoft, SAP oder anderen Lieferant:innen aussteigen? Die öffentliche Hand tut gut daran, die wachsende Abhängigkeit immer in ihren Risikoanalysen zu berücksichtigen. Ausserdem ist es immerhin prüfenswert, allfällige Bestrebungen zum Aufbau von Infrastruktur in der Schweiz (z.B. eine «Gov-Cloud» für die Verwaltungen von Bund und Kantonen) oder in Europa zu unterstützen. Eine diesbezügliche Koordination mit der Digitalen Verwaltung Schweiz (DVS) oder dem Bundesamt für Informatik und Telekommunikation ist sicher anzustreben.

1 § 6 IDG und – im Zusammenhang mit der Auslagerung von Datenbearbeitungen an Dritte – § 7 IDG; vgl. dazu PK-IDG/BS-Rudin, § 6 N 2 ff. und § 7 N 1 ff., insb. N 32 ff.

2 Zur nicht von ihm zu beantwortenden strafrechtlichen Frage, ob eine Auftragsdatenbearbeitung bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen, ein unzulässiges Offenbaren darstellt, vgl. vorne Ziff. 3.3.

3 Gesetz (des Kantons Freiburg) vom 25. November 1994 über den Datenschutz (DSchG), SGF 17.1 (in der Fassung gültig ab 01.03.2021), https://bdlf.fr.ch/app/de/texts_of_law/17.1.

4 Die Bestimmungen würden, so eine Äusserung aus Freiburg anlässlich der Diskussion am privatim-Herbstplenum 2021 in Biel/Bienne, auch noch nicht alle Fragen angemessen beantworten.

5 Beschluss Nr. 542 des Regierungsrates des Kantons Zürich vom 30. März 2022 zum Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung.

6 David Vasella, daten:recht, 16. April 2022, https://datenrecht.ch/regierungsrat-zuerich-gruenes-licht-fuer-m365-risikobeurteilungsmodell-rosenthal-kanonisiert-risikogrenze-bei-10-ueber-5-jahre/.

7 Im erwähnten Kommentar wurde auch ausgeführt, der Regierungsrat des Kantons Zürich habe das Risikobeurteilungsmodell Rosenthal «kanonisiert» (nach Duden: «aufgenommen in das Verzeichnis der Heiligen (Kanon) durch den Papst»), also heiliggesprochen – und das im reformierten Kanton Zürich! Ausserdem brauchte es dafür wohl eher eine fachliche Validierung der Wahrscheinlichkeitsberechnung als bloss einen Regierungsratsbeschluss.

8 Vgl. dazu die privatim-Stellungnahme «Kein Freipass für ‹Microsoft 365›» (wird demnächst auf https://www.privatim.ch/de/ veröffentlicht.

9 Vgl. zum Beispiel auch die verstärkt als Risiko erkannte Abhängigkeit der Untersee-Datenkabel: Oliver Rolofs, Der Krieg der Zukunft wird auch ein Krieg um die Untersee Datenkabel sein – Europa muss sich wappnen und schützen, NZZ 28.07.2021, https://www.nzz.ch/meinung/krieg-der-zukunft-ein-krieg-auch-um-die-untersee-datenkabel-ld.1630916.

Trend 6

Entwicklungen bei der Videoüberwachung

Mit dem Tätigkeitsbericht 2016 wurde dargestellt, wie es um die Transparenz bei staatlichen Videoüberwachungsanlagen steht. Fünf Jahre später hat sich die Situation etwas verbessert. Festzustellen ist jedoch, dass insbesondere bei Neubauten quasi selbstverständlich umfassende Videoüberwachungsanlagen eingeplant werden. Ausserdem werden vermehrt «Servicekameras» eingesetzt. Und schliesslich findet eine weitere Entwicklung statt: von der «Objekt-» zur «raumbezogenen Überwachung».

Die Regelung der Videoüberwachung

Die IDG-Regelung Die §§ 17 und 18 IDG regeln die Videoüberwachung. Erfasst sind:

— Videoüberwachungen an öffentlichen, allgemein oder nicht allgemein zugänglichen Orten,

— bei denen Personen identifiziert werden können.

Solange nur der im IDG vorgesehene Zweck – der Schutz von Personen oder Sachen vor strafbaren Handlungen beziehungsweise die Verfolgung solcher strafbarer Handlungen – verfolgt werden soll, stellt § 17 Abs. 1 IDG die erforderliche gesetzliche Grundlage dar. § 17 Abs. 2–5 IDG stellen weitere Regeln auf zur Verhältnismässigkeit, Hinweispflicht, Aufbewahrung. Die Konkretisierung hat jeweils in einem Reglement zu erfolgen (§ 18 IDG).

Videoüberwachungen zu anderen Zwecken Videoüberwachungen zu einem anderen als zu dem in § 17 Abs. 1 IDG erwähnten Zweck – wie erwähnt: der Schutz von Personen oder Sachen vor strafbaren Handlungen beziehungsweise die Verfolgung solcher strafbarer Handlungen – benötigen eine eigene gesetzliche Grundlage. Eine solche stellt beispielsweise § 58 des Polizeigesetzes (PolG) dar: Danach darf die Kantonspolizei zur Beweissicherung Teilnehmer:innen einer öffentlichen Veranstaltung aufnehmen, sofern die *konkrete Gefahr* besteht, dass Straftaten begangen werden. In diesem Moment braucht es die §§ 17 und 18 IDG nicht und gelten die entsprechenden Anforderungen (zum Beispiel die vorgängige Vorabkontrolle durch die oder den Datenschutzbeauftragten) logischerweise nicht – die allgemeinen Anforderungen des IDG aber sehr wohl, also etwa das Verhältnismässigkeitsprinzip (§ 9 Abs. 3 IDG), die Regelung der Erkennbarkeit (§ 15 IDG) und der Informationssicherheit (§ 8 IDG). Ausserdem verschärft das Polizeigesetz die allgemeine Regel von § 16 IDG: Aufnahmen nach Polizeigesetz müssen vernichtet werden, sobald feststeht, dass diese zur Strafverfolgung nicht mehr benötigt werden (§ 58 Abs. 2 PolG). Wenn also keine Straftaten begangen worden sind, müssen die Aufnahmen vernichtet werden. Nach unserer Meinung kann nicht argumentiert werden, dass die Strafantragsfrist von drei Monaten nach Art. 32 des Schweizerischen Strafgesetzbuches (StGB) dazu führt, dass die Kantonspolizei alle Aufnahmen so lange aufbewahren muss, weil ja jemand noch einen Strafantrag stellen könnte. Es ist nicht Aufgabe des Staates, Videoaufnahmen als mögliche Beweismittel bei Strafantragsdelikten herzustellen und über längere Zeit bereit zu halten: Strafantragsdelikte sind deshalb keine von Amtes wegen zu verfolgende Delikte, weil «der Staat nur ein sehr geringes Verfolgungsinteresse hat (Bagatellkriminalität, Art. 172ter StGB als Paradebeispiel)» bzw. «wenn der Private ein erhebliches Interesse auf Nicht-Verfolgung hat»[1]. Eine lange Aufbewahrungsfrist staatlicher Videoaufnahmen erscheint unverhältnismässig bei nicht von Amtes wegen zu verfolgenden Bagatelldelikten.

Videoüberwachungen zu einem anderen als zu dem im IDG erwähnten Zweck benötigen eine eigene gesetzliche Grundlage.

Reglement nach § 18 IDG

Konkretisierung für jedes Videoüberwachungssystem Der Betrieb einer Videoüberwachungsanlage ist nur dann gesetz- und verhältnismässig, wenn die entsprechenden Rechtsgrundlagen hinreichend bestimmt sind[2]. Deshalb muss für jedes Videoüberwachungssystem, das sich auf § 17 IDG stützt, vor seiner Inbetriebnahme ein Reglement erlassen werden, das insbesondere den Zweck des Systems, die Verantwortlichkeit und die Löschungsfrist festlegt (§ 18 Abs. 1 IDG).

Veröffentlichungspflicht Der Rechtsstaat erlaubt es den Gesetzesunterworfenen zu sehen, was die Verwaltung tut, auf welcher Grundlage und inwiefern sie ihre Grundrechte einschränken darf. Darum müssen Gesetze und Verordnungen auch in der Gesetzessammlung publiziert werden. Allein aus der generellen Regelung des IDG können die Betroffenen in keiner Weise erkennen, wo und wie ihr Grundrecht auf informationelle Selbstbestimmung durch staatlich betriebene Videoüberwachung eingeschränkt wird. Ein «geheimes» Reglement könnte natürlich die erforderliche Transparenz für die Betroffenen nicht sicherstellen. Deshalb hat der Verordnungsgeber klar festgelegt: Die Reglemente sind der Öffentlichkeit leicht zugänglich zu machen[3]. Einzig wenn durch die Bekanntgabe der Kamerastandorte die Zweckerreichung unmöglich würde, soll auf deren Veröffentlichung verzichtet werden können[4].

Neu auf Gesetzesstufe Die Veröffentlichungspflicht soll, weil es mit der Umsetzung etwas gehapert hat, samt leicht erweiterten Ausnahmen mit der IDG-Revision auf Gesetzesstufe gehoben werden.[5]

Prüfung Der Datenschutzbeauftragte hat im Jahr 2021 – wie schon 2016 – eine Übersicht über die von ihm vorab geprüften Videoüberwachungen und die im Internet veröffentlichten Reglemente erstellt. Das Resultat dieser Prüfung erscheint in der Tabelle auf den Seiten 39 f.

Erfasste und nicht erfasste Systeme In dieser Liste nicht erfasst sind private Videoüberwachungssysteme – sie unterstehen nicht dem IDG, sondern dem DSG. Nicht mitgezählt sind die von öffentlichen Organen betriebene Anlagen, die nicht in den Geltungsbereich des IDG fallen. Nicht enthalten sind demnach die Videoüberwachungssysteme der Basler Verkehrsbetriebe BVB[6], in den staatlichen Parkhäusern[7], der Basler Kantonalbank BKB[8], Kameras, die von der Kantonspolizei gestützt auf das Polizeigesetz[9] eingesetzt werden, Kameras, die zeitlich begrenzt zum Zweck einer nichtpersonenbezogenen Evaluation eingesetzt werden (z.B. bei einem Versuch zur Velozulassung auf einem Fussgängersteg) und schliesslich blosse «Türspione».

Entwicklungen

«Standardausstattung» Eine Herausforderung stellt die Tatsache dar, dass insbesondere bei Neubauten für Verwaltungsstellen (oder Neubauten, in denen sich Verwaltungsstellen einmieten) quasi selbstverständlich umfassende Videoüberwachungsanlagen eingeplant werden. Die Verwaltungsstellen, die schliesslich für den Betrieb der Videoüberwachung die Verantwortung tragen, sind bei der Planung der Überwachung häufig noch gar nicht miteinbezogen.

Eine Herausforderung stellt die Tatsache dar, dass bei Neubauten für Verwaltungsstellen (oder Neubauten, in denen sich Verwaltungsstellen einmieten) quasi selbstverständlich umfassende Videoüberwachungsanlagen eingeplant werden.

Servicekameras Immer mehr Kameras werden zu Aufgabenerfüllungszwecken eingesetzt, nicht zur Verhinderung oder Verfolgung von Straftaten. Das ist beispielsweise der Fall, wenn bei einer Anlieferung per Lastwagen ein Dosierungssystem nötig ist, also Lastwagen in einen Warteraum gewiesen werden müssen, damit sie nicht Zufahrtsstrasse verstopfen, und erst abgerufen werden, wenn eine «Entladebucht» frei wird, was von der Leitstelle dank einem Videobild festgestellt werden kann. Sie müssen nicht unbedingt Personendaten erfassen: Es kann reichen, dass erkannt wird, dass eine bestimmte Situation vorliegt, ohne dass die Personen oder über die Kontrollschilder die Fahrzeuge identifizierbar sind. Solche «Servicekameras» können nicht auf § 17 Abs. 1 IDG gestützt werden.[10] Trotzdem wollen öffentliche Organe sie regeln, teilweise im Videoüberwachungsreglement, das für andere Kameras erstellt werden muss. Der DSB empfiehlt in diesem Fall, erkennbar zwischen «§ 17-Kameras» und «Servicekameras» zu unterscheiden.

Von der «Objekt-» zur raumbezogenen Überwachung» Schliesslich lässt sich eine weitere Entwicklung beobachten: von der Überwachung eines Objekts (z.B. eines Eingangs, eines Schalters, eines Lagerraums usw.) zur eher raumbezogenen Überwachung. Ein Beispiel dafür ist die Reaktion auf Vorfälle an der Uferstrasse (sogleich unten). Der Grosse Rat hat in der Vergangenheit verschiedene raumbezogene Überwachungsprojekte abgelehnt. Nach dem Wortlaut von § 17 IDG ist dies aber nicht ausgeschlossen. >

Videoüberwachung Uferstrasse

Öffentliche Aufmerksamkeit Im Jahr 2021 hat die Videoüberwachung durch die Kantonspolizei an der Uferstrasse grosse Aufmerksamkeit auf sich gezogen. Nachdem es dort zu (aufgrund der Covid-19-Massnahmen illegalen) Partys und zu einer schweren Gewalttat gekommen war[11], hat der Regierungsrat ein Massnahmenpaket beschlossen.[12] Die Kantonspolizei richtete eine Videoüberwachung ein. Jurist:innen der Kantonspolizei machten auf die «dünne» Rechtsgrundlagen aufmerksam. Der Datenschutzbeauftragte hat diese Einschätzung unterstützt: § 58 PolG ist eine Art polizeiliche Generalklausel für die Videoüberwachung – mit (wie vorne erwähnt: S. 36) engen Grenzen: Sie erlaubt die Aufnahme von Teilnehmer:innen an «einer öffentlichen Veranstaltung, sofern die konkrete Gefahr besteht, dass Straftaten begangen werden». Ob die (spontanen) Partys eine «öffentliche Veranstaltung» sind, mag schon mal fraglich sein. Dass die «konkrete Gefahr besteht, dass Straftaten begangen werden», mag für bestimmte Momente zutreffen, aber nicht generell für alle Veranstaltungen an der Uferstrasse – auch nicht generell an Wochenenden und zu Abendzeiten und auch nicht einfach zwischen Mai und Oktober.

Unverständlich war, dass irgendjemand bei der Kantonspolizei das Gefühl hatte, es brauche es keine Hinweise auf die Videoüberwachung, solange das Reglement nicht veröffentlicht sei.

Empfehlung des DSB Aus diesem Grund hat der Datenschutzbeauftragte dringend empfohlen, eine Rechtsgrundlage in Form eines Reglements nach § 18 IDG zu schaffen, was von der Kantonspolizei auch zugesagt wurde. Jeweils innert spätestens zwei Tagen hat der DSB zu den unterbreiteten Reglementsentwürfen Stellung genommen. Rund sieben Wochen nach der Empfehlung wurde das Reglement schliesslich veröffentlicht.

Keine Intervention des DSB Weil die Kantonspolizei einerseits zugesagt hat, ein Reglement zu erlassen, die für eine Videoüberwachung nach §§ 17 f. IDG geltenden Rahmenbedingungen (zeitliche und räumliche Beschränkung) aber schon vor dem Erlass einzuhalten, und es andererseits durchaus möglich war, dass zu einem bestimmten Zeitpunkt eine Überwachung nach § 58 PolG zulässig wäre, hat der DSB auf eine Intervention verzichtet. Unverständlich war schliesslich nur, dass irgendjemand bei der Kantonspolizei das Gefühl hatte, solange das Reglement nicht veröffentlicht sei, brauche es auch keine Hinweise auf die Videoüberwachung. § 17 Abs. 3 IDG legt fest, der Einsatz von Videoüberwachung sei durch geeignete Massnahmen unter Angabe der verantwortlichen Stelle erkennbar zu machen – die Hinweispflicht hängt somit an der Überwachung, nicht am Reglement.

Befristung und Abbau Das Justiz- und Sicherheitsdepartement hat die Geltung des Reglements für die Uferstrasse bis Ende Oktober 2021 befristet, weshalb das Videoüberwachungssystem in der Zusammenstellung (S. 39 ff.) auch nicht aufgeführt ist. Die sieben Kameras wurden bereits wieder abgebaut.

1 BSK-Strafrecht I-Christoph Riedo, Vor Art. 30 Rz. 12.
2 BGE 136 I 87; vgl. dazu PK-IDG/BS-Husi, § 18 N 1.
3 § 6 Abs. 1 IDV; vgl. dazu auch PK-IDG/BS-Husi, § 18 N 46.
4 § 6 Abs. 2 IDV; vgl. dazu auch PK-IDG/BS-Husi, § 18 N 47.
5 Ratschlag 21.1239.01, S. 35 f.: § 18 Abs. 4bis und 4ter E-IDG.
6 Aufgrund des Personenbeförderungsgesetzes des Bundes (Art. 54 Abs. 1 und 3 PBG) ist dafür nicht mehr der kantonale DSB, sondern der EDÖB zuständig; vgl. dazu TB 2010, S. 10 f. und PK-IDG/BS, § 2 N 37 ff.
7 Sie werden zwar durch ein öffentliches Organ betrieben (Immobilien Basel-Stadt), hingegen handelt es sich dabei um die Verwaltung von Finanzvermögen, was sich ausserhalb des Geltungsbereichs von § 17 IDG abspielt.
8 Zwar ist die Kantonalbank eine Anstalt des kantonalen öffentlichen Rechts (§ 1 Kantonalbankgesetz), weshalb ihr Datenbearbeiten eigentlich in den Geltungsbereich des kantonalen IDG fällt (§ 2 Abs. 1 i.V.m. § 3 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin § 3 N 7); da aber die BKB am wirtschaftlichen Wettbewerb mit anderen (Universal-)Banken teilnimmt und dabei privatrechtlich handelt, fällt sie aus dem Geltungsbereich des IDG (§ 2 Abs. 2 lit. a IDG).
9 § 58 PolG; siehe vorne S. 36.
10 Teilweise können solche Kameras mittelbar gestützt auf eine Aufgabenerfüllungsnorm gerechtfertigt werden. Falls keine Personendaten erfasst werden, braucht es aus Datenschutzperspektive gar keine gesetzliche Grundlage.
11 So die Ausführungen im Jahresbericht (des Regierungsrates) 2021, S. 222.
12 Medienmitteilung des Regierungsrates vom 11. Mai 2021 – allerdings ohne Erwähnung der Videoüberwachung.

Videoüberwachungsanlagen öffentlicher Organe im Kanton Basel-Stadt: Links zu den Reglementen

Wo?	Wer?	Was?	*	Link zum Reglement oder zur Information	Bemerkungen
mehr als 200 Kameras					
Bässlergut	JSD, Amt für Justizvollzug	Überwachung des gesamten Gebäudekomplexes innen und aussen	*	https://www.bdm.bs.ch/Ueber-uns/Organisation/Amt-fuer-Justizvollzug/Gefaengnis-Baesslergut.html#page_section3_section7	Publikation des Reglements ohne Lagepläne
Kunstmuseum	PD, Kunstmuseum	Überwachung innen und aussen der fünf Gebäude	*	https://kunstmuseumbasel.ch/	Publikation des Reglements ohne Lagepläne
Waaghof	JSD und Staatsanwaltschaft	Überwachung des gesamten Gebäudekomplexes innen und aussen	*	https://www.bs.ch/publikationen.html	Publikation des Reglements ohne Lagepläne
101–200 Kameras					
IWB-Infrastruktur	IWB, Industrielle Werke Basel	Überwachung der Infrastruktur an verschiedenen Standorten		https://www.iwb.ch/Videoueberwachungsreglement.html	Publikation des Reglements ohne Lagepläne
51–100 Kameras					
Historisches Museum HMB, Haus zum Kirschgarten, Barfüsserkirche, Musikmuseum, Verwaltungsgebäude	PD, Historisches Museum HMB	Überwachung der Eingänge und Innenräume an den einzelnen Standorten	*	https://www.hmb.ch/ueber-uns/auftrag/	Publikation eines Informationsblatts zur Videoüberwachung
Polizeiwachen und Polizeiposten	JSD, Kantonspolizei	Überwachung von Polizeiwachen und -posten (ohne Waaghof und Spiegelhof)	*	http://www.polizei.bs.ch/was-tun/akteneinsichtsgesuch.html#page_section3_section2	Publikation des Reglements ohne Lagepläne
Sportanlagen und Bäder	ED	Überwachung der verschiedenen Sportanlagen und Bäder			Reglement in Revision
St. Jakobhalle	ED	Überwachung der St. Jakobhalle innen und aussen		https://www.stjakobshalle.ch/infos/#allgemeine-informationen	Publikation des Reglements mit Lageplänen
Universitätsspital	Universitätsspital Basel USB	Überwachung des gesamten Areals		https://www.unispital-basel.ch/ueber-uns/das-universitaetsspital/umgang-mit-personendaten/	Publikation des Reglements ohne Lagepläne
21–50 Kameras					
Betreibungsamt	Betreibungs- und Konkursamt Basel-Stadt	Überwachung der Schalter, der Kundenzonen und eines Sitzungszimmers		https://www.bka.bs.ch/ueber-uns/betreibungsamt.html	Publikation des Reglements ohne Lagepläne
Dreispitzareal	Christoph Merian-Stiftung CMS	Überwachung der Parkieranlagen sowie Polleranlagen	*	https://www.dreispitz.ch/de/bauen/baurecht.html	Publikation des Reglements mit Lageplänen
Gesundheitsdepartement Malzgasse	GD	Überwachung der Eingänge, des Treppenhauses und des Veloparkplatzes	*	https://www.gd.bs.ch/ueber-das-departement/bereiche-abteilungen.html	Publikation des Reglements ohne Lagepläne
Museum der Kulturen	PD, Museum der Kulturen	Überwachung der Ausstellungsräume, des Museumsshops und des Eingangs- und Aussenbereichs		https://www.mkb.ch/de/ihr-besuch/cIIp-0/hausordnung.html	Publikation eines Informationsblatts zur Videoüberwachung
REHAB Basel	REHAB Basel	Überwachung des Therapietiergartens, der Nebenzugänge, der Tiefgarage, des Serverraums und des Velokellers		https://www.rehab.ch/de/patientinnen-angehoerige/besucherinnen/videoueberwachung	Publikation des Reglements mit Lageplänen
St. Claraspital	St. Claraspital	Überwachung der Zugänge zum Spital		https://www.claraspital.ch/videoreglement/	Publikation des Reglements ohne Lagepläne
Universitäre Psychiatrische Kliniken	Universitäre Psychiatrische Kliniken Basel UPK	Überwachung der Eingangs- und Aussenbereiche		https://www.upk.ch/ueber-uns/umgang-mit-personendaten/videoreglement.html	Publikation des Reglements ohne Lagepläne
Universität	Universität Basel	Überwachung verschiedener Standorte	*	https://www.unibas.ch/de/Dokumente.html	Publikation des Reglements mit Lageplänen
Universitäts-Kinderspital beider Basel	Universitäts-Kinderspital beider Basel UKBB	Überwachung der Zugänge zum Spital, des Verbindungsgangs zum USB, der Notfallzone, des Schlaflabors, des Velokellers und zweier Isolationszimmer		https://www.ukbb.ch/de/ukbb/unternehmen.php	Publikation des Reglements ohne Lagepläne
Zeughaus	JSD	Überwachung des Areals und des Ein- und Ausgangsbereichs		https://www.bs.ch/publikationen/polizei/videoreglement-zeughaus.html	Publikation des Reglements ohne Lagepläne

Wo?	Wer?	Was?	*	Link zum Reglement oder zur Information	Bemerkungen
11–20 Kameras					
Berufsfeuerwehr Lützelhof	JSD, Rettung, Berufsfeuerwehr	Überwachung des Innenhofs, der Zugänge und der Ausfahrtsbereiche		https://www.rettung.bs.ch/feuerwehr?footeropen=publications	Publikation des Reglements mit Lageplänen
Sanität	JSD, Rettung, Sanität	Überwachung des Areals und der Innenräume der Rettungswagen	*	https://www.bs.ch/publikationen.html	Publikation des Reglements ohne Lageplän
Semistationäre Verkehrsstationen	JSD, Kantonspolizei	Überwachung der semistationären Verkehrsstationen	*	https://www.polizei.bs.ch/was-tun/akteneinsichtsgesuch.html#page_section3_section4	Publikation des Reglements ohne Lagepläne
Synagoge	Israelitische Gemeinde Basel IGB	Überwachung des Areals und der näheren Umgebung	*	https://www.igb.ch/datenschutz/	Publikation des Reglements mit Lageplänen
Velostation St. Johann	BVD, Allmendverwaltung	Überwachung der Velostation St. Johann			Reglement in Bearbeitung
5–10 Kameras					
Antikenmuseum Basel & Sammlung Ludwig	PD, Antikenmuseum Basel & Sammlung Ludwig	Überwachung des Eingangbereichs, des Kunstlicht- und des Ägyptensaals		http://www.antikenmuseumbasel.ch/de/footer/videoueberwachung.html	Publikation des Reglements ohne Lagepläne
Bau- und Verkehrsdepartement, Dufourstrasse 40 und 50, Münsterplatz 10–12	BVD	Überwachung der Gebäudeeingänge und des Stadtmodells		https://www.bvd.bs.ch/?footeropen=law	Publikation des Reglements ohne Lagepläne
Fachhochschule	Fachhochschule Nordwestschweiz FHNW	Überwachung der Campusgebäude an der Peter Merian-Strasse 86		https://www.fhnw.ch/de/impressum/datenschutz/datenschutzreglement-fhnw.pdf	Publikation des Reglements ohne Lagepläne
IT BS, Rechenzentren	FD, IT BS	Überwachung der kantonalen Rechenzentren bei den IWB und der EBM			Reglement in Revision
Musik-Akademie Basel	Musik-Akademie Basel und Hochschule für Musik FHNW	Überwachung einiger Gebäudeeingänge sowie sicherheitsrelevanter Innenbereiche		https://www.musik-akademie.ch/de/uber-uns/datenschutz.html	Publikation des Reglements ohne Lagepläne
Notschlafstelle der Männer	WSU, Sozialhilfe	Überwachung des Eingangsbereichs	*	https://www.sozialhilfe.bs.ch/not--und-soziales-wohnen/notschlafstellen.html	Publikation des Reglements mit Lageplänen
Steuerverwaltung	FD, Steuerverwaltung	Überwachung des Empfangs und der Schalter		https://www.steuerverwaltung.bs.ch/kontakt/leitbild.html	Publikation des Reglements mit Lageplänen
Strafgericht	Strafgericht	Überwachung des Eingangsbereichs und des Weibelgebäudes		http://www.strafgericht.bs.ch/verhandlungen/verhandlungsbesuch/reglement-videoueberwachung.html	Publikation des Reglements ohne Lagepläne
Wohnmodul-Anlage Asyl Dreispitz	WSU, Sozialhilfe	Überwachung der Zugänge zur Anlage	*	http://www.sozialhilfe.bs.ch/asyl/unterbringung.html	Publikation des Reglements mit Lageplänen
1–4 Kameras					
Aufnahmeheim Basel	Stiftung AHBasel	Überwachung des Aussenbereichs der offenen Abteilung	*	https://www.ahbasel.ch/downloads/	Reglement in Revision
Heilsarmee, Wohnen Basel	WSU, Amt für Sozialbeiträge	Überwachung des Eingangsbereichs der Wohnhäuser	*	http://www.wohnen.heilsarmee-basel.ch	Publikation des Reglements ohne Lagepläne
Heime auf Berg AG	Heime auf Berg AG	Überwachung des Zugangs zum Gebäude	*	https://aufberg.ch/downloads-dokumente	Publikation des Reglements ohne Lagepläne
Hostel Volta	Verein Mobile Basel	Überwachung des Eingangbereichs	*	https://www.mobilebasel.ch/hostel-volta/	Publikation des Reglements ohne Lagepläne
Institut für Rechtsmedizin IRM	GD	Überwachung des Eingangsbereichs		https://www.irm.bs.ch/ueber-uns.html	Publikation des Reglements ohne Lagepläne
IT BS, Betriebsräumlichkeiten	FD, IT BS	Überwachung der Warenanlieferung und der IT-Werkstatt			Reglement in Revision
Naturbad Riehen	Gemeinde Riehen	Überwachung des Haupteingangs und des Cafés		https://www.riehen.ch/wAssets/docs/GRB_Reglement-fuer-das-Videoueberwachungssystem-im-Naturbad-vo.pdf	Publikation des Reglements mit Lageplan
Naturhistorisches Museum	PD, Naturhistorisches Museum	Überwachung des Eingangstors (Innenhof)	*	https://www.nmbs.ch/home/info_angebote/ihr-besuch.html Link unter: Ihr Besuch I Lage Infos	Publikation des Reglements mit Lageplan
Schulhaus Sandgruben	ED	Überwachung des Velokellers			Reglement in Revision

Wo?	Wer?	Was?	*	Link zum Reglement oder zur Information	Bemerkungen
Sozialhilfe	WSU	Überwachung des Kassenbereichs	*	https://www.sozialhilfe.bs.ch/-sozialhilfe/unterstuetzung/nothilfe.html	Publikation des Reglements mit Lageplan
Claramatte	JSD	Überwachung der Kundenzone des Handelsregisteramts	*	https://www.jsd.bs.ch/jsd-medien/dokumentationen.html	Publikation des Reglements ohne Lagepläne
Werkhof Riehen	Gemeinde Riehen	Überwachung der Zugänge zur Tiefgarage und des Recyclinghofs		https://www.riehen.ch/verwaltung/dokumente/dokumente/gesetz/reglement_videoueberwachung_werkdienste.pdf	Publikation des Reglements mit Lageplan
Wertstoffsammelstelle Niederholzstrasse	Gemeinde Riehen	Überwachung des Containerbereichs		https://www.riehen.ch/verwaltung/dokumente/dokumente/abfall-entsorgung/reglement_videoueberwachung_werstoffsammelstelle_niederholzst.pdf	Publikation des Reglements mit Lageplan
0 Kameras (Ausser Betrieb)					
Spiegelhof	JSD	Überwachung der Kundenzone des Polizeipostens Spiegelhof			Während Umbau keine Video-überwachung
Vollzugszentrum Klosterfiechten	JSD, Amt für Justizvollzug	Überwachung des Empfangs-bereich und des Eingang zum Untersuchungszimmer			Während Umbau keine Video-überwachung

*** = Link auf der angegebenen Website**
(Stand: 30. Juni 2022)

Jahresrückblick

2020–2021:
Kurzer Blick auf die wichtigsten Geschäfte

Statistik

Jahresrückblick

2020–2021: Kurzer Blick auf die wichtigsten Geschäfte

Der Datenschutzbeauftragte berät und kontrolliert öffentliche Organe bei der Umsetzung des Informations- und Datenschutzgesetzes und berät die betroffenen Personen zu ihren Rechten gegenüber den Datenbearbeiter:innen. Was waren die wichtigsten Geschäfte in den vergangenen zwei Jahren? Wie steht es mit Pilotversuchen in der Basler Verwaltung? Und was sagt die Statistik über die Geschäftsfälle und personellen Ressourcen?

Aufgaben des Datenschutzbeauftragten

Beratung und Kontrolle Das Informations- und Datenschutzgesetz bezweckt, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern und die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.[1] Die oder der Datenschutzbeauftragte ist ebenfalls eingesetzt, um für die *Achtung der Grundrechte der betroffenen Personen* zu sorgen. Das IDG beauftragt die / den DSB schwergewichtig mit der Beratung und Kontrolle.[2] Beraten werden die öffentlichen Organe beim Umgang mit Informationen und die von einer Datenbearbeitung betroffenen Personen über ihre Rechte.

Beratungstätigkeit

Querschnittsthema Die Beratungstätigkeit bindet etwa drei Viertel der Ressourcen des Datenschutzbeauftragten. Thematisch wurde auch in den beiden letzten Jahren die gesamte Breite der Staatstätigkeit erfasst. Ausgewählte Bereiche sind vorne im Kapitel «Trends» (S. 7 ff.), einzelne Fragestellungen hinten im Kapitel «Fälle» (S. 53 ff.) dargestellt. Nur exemplarisch seien hier weitere Themen kurz erwähnt:

— *Stellungnahmen in Rechtsetzungsverfahren* sowohl auf kantonaler als auch (z.T. im Rahmen von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten) auf Bundesebene, so u.a. zum Bibliotheksverbund SLSP (Swiss Library Service Platform) und zu mehreren Schengen-Weiterentwicklungen u.a.m.

— Einen besonderen Stellenwert bei den Rechtsetzungsverfahren nimmt die Revision des *Informations- und Datenschutzgesetzes* (Anpassung an die europäischen Datenschutzreformen) ein. Nach langer Vorbereitung – der DSB hat den Ratschlags- und Gesetzesentwurf im Januar 2019 an die Staatskanzlei abgeliefert – hat der Regierungsrat das Geschäft am 29. September 2021 dem Grossen Rat überwiesen. Ab Januar 2022 begleitet der DSB das Geschäft in der grossrätlichen Justiz-, Sicherheits- und Sportkommission (JSSK).

— *Vorabkontrollen* (künftig: Vorabkonsultationen)[3] *zu Vorhaben*, die aufgrund der Art der Bearbeitung oder der Art der zu bearbeitenden Daten geeignet sind, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, so etwa zum Projekt des neuen Fallführungssystems Sozialhilfe (Ablösung von Tutoris), zum Projekt «Robotic Process Automation (RPA)» des Justiz- und Sicherheitsdepartements, zur Nutzung von Microsoft-Onlinediensten durch die Universitätsspitäler, zum Bibliotheksverbund SLSP (Swiss Library Service Platform), zu sehr vielen Anwendungen im Zusammenhang mit Distance-Schooling, zu Projekten im Zusammenhang mit der Verwaltung von Daten von Bewerber:innen und aus Assessments usw.

Die oder der Datenschutzbeauftragte ist eingesetzt, um für die Achtung der Grundrechte der betroffenen Personen zu sorgen.

Vorabkonsultationen bei der Einrichtung, Ausweitung oder Verlängerung von *Videoüberwachungen*, so u.a. bei der Israelitischen Gemeinde Basel (IGB), an der Uferstrasse (s. auch vorne S. 36 ff.) oder an semistationären Geschwindigkeitsmessstationen usw.

— Stellungnahmen im Zusammenhang mit dem Recht auf Zugang zu den eigenen Personendaten und mit dem allgemeinen Informationszugangsrecht (Öffentlichkeitsprinzip).

— Beratungen im Zusammenhang mit *Meldungen von Datenschutzverletzungen* (noch nicht gestützt auf die neu zu schaffende Meldepflicht bei Datenschutzverletzungen[4], sondern auf den Grundsatz von Treu und Glauben).

— Abklärungen im Zusammenhang mit konkreten Vorfällen, so etwa bei der Veröffentlichung einer Liste von Schüler:innen mit zu vielen und teilweise besonderen Personendaten oder wenn in «Autofill»-Listen Bankdaten oder Handynummern preisgegeben werden usw.

— Stellungnahmen zuhanden von Medienschaffenden, so etwa zur «Kamerapflicht» bei Hochschulprüfungen (Online-Prüfungen während der Covid-Pandemie), zu Videoüberwachungen usw.

Onlinezugriffs-Gesuche

Datenmarkt Im Rahmen der Beratungstätigkeit nimmt auch die Vorabkonsultation von Onlinezugriffs-Gesuchen einen breiten Raum ein. Was im Bund und in vielen Kantonen unter E-Government-Aspekten (Stichwort «Once only») erst diskutiert wird, besteht in Basel-Stadt seit langem: Im Datenmarkt werden den öffentlichen Organen Personen- und Sachdaten, die von mehr als einem öffentlichen Organ zur Erfüllung seiner gesetzlichen Aufgaben benötigt werden, tagesaktuell auf einer zentralen Plattform zur Verfügung gestellt.[5]

Diagnose Öffentliche Organe sind mit ihrer Unzufriedenheit nicht allein – der Datenschutzbeauftragte stimmt mit ihrer Diagnose völlig überein: Der Durchlauf vom Gesuch bis zur Aufschaltung der Zugriffsmöglichkeit dauert viel zu lange.[6] Das ist auch der Grund, dass der DSB seit geraumer Zeit daran ist, eine bessere Lösung für die Verfahren und Verantwortlichkeiten aufzugleisen, zum Beispiel mit der Einrichtung eines «Round Table» (siehe sogleich hinten im Absatz «Beschleunigungsvorschlag …»).

Beteiligte und ihre Verantwortung Beim Bezug von Personendaten via Datenmarkt «bedienen sich» die Datenempfänger:innen bei den Daten der Datenlieferant:innen (= Dateneigner:innen im Sinne von § 6 IDG). Datenschutzrechtlich handelt es sich um eine Bekanntgabe von Personendaten, wobei die nach § 6 IDG dafür verantwortlichen Dateneigner:innen ja systembedingt nicht im konkreten Einzelfall überprüfen können, ob die Datenbekanntgabe gesetz- und verhältnismässig ist, sondern dies vorweg generell tun müssen («Autorisierung» im Sinne von § 5 Abs. 2 der Datenmarktverordnung [DMV]). Dabei ergibt sich folgende *Aufgabenverteilung:*

— *Die Gesuchsteller:innen* müssen belegen, dass die Voraussetzungen für die beantragte Datenbekanntgabe (nach § 21 IDG) erfüllt sind, dass also das beantragte «Sich-bedienen-können» gesetzmässig und verhältnismässig ist. Sie müssen die Rechtsgrundlagen anführen und belegen, dass die Datenbekanntgabe für ihre Aufgabenerfüllung geeignet, erforderlich und verhältnismässig i.e.S. ist.

— Die *Dateneigner:innen* (als Verantwortliche im Sinne von § 6 IDG) müssen prüfen, ob die Voraussetzungen nach § 21 IDG erfüllt sind, ob die Datenbekanntgabe also gesetz- und verhältnismässig ist. Wenn diese Voraussetzungen erfüllt sind, dann dürfen sie die Autorisierung erteilen (§ 5 Abs. 2 DMV).

— Der *Datenschutzbeauftragte* prüft nach § 5 Abs. 3 DMV mit einer Vorabkonsultation vor der Umsetzung der Autorisierung, ob die Gesuchsteller:innen und die Dateneigner:innen ihre Aufgabe erfüllt haben.

Die Gesuchsteller:innen müssen belegen, dass das beantragte «Sich-bedienen-können» im Datenmarkt gesetzmässig und verhältnismässig ist. Die Dateneigner:innen dürfen, wenn diese Voraussetzungen erfüllt sind, die Autorisierung erteilen.

Bremsfaktoren Der letzte Schritt wäre eigentlich ein ganz kleiner – wenn die nötigen Informationen vorliegen. Das ist leider sehr oft nicht der Fall.[7] Oftmals waren in der Vergangenheit die Rechtsgrundlagen unvollständig (z.B. einfach ein Gesetz oder eine Verordnung angegeben statt die genaue[n] Bestimmung[en]) bzw. teilweise ganz falsch. Als Zweck, zu dessen Erreichung bestimmte Attribute erforderlich sind, wurde einfach «zur Aufgabenerfüllung» angegeben (oder dann wurde aus einem Dokument eine Viertelseite kopiert – quasi eine generelle «Auswahlsendung»). Der DSB hat selber in mühsamer Arbeit Gesetzesgrundlagen zusammengesucht und ergänzt – dabei war sicher nicht beschleunigend, wenn die die Gesuche ausfüllenden Personen zum Teil einfach geantwortet haben: «Wie soll ich das wissen?». Diese Arbeit hat in den letzten paar Jahren extrem zugenommen – wohl weil man sich daran gewöhnen kann, dass der DSB die nicht korrekt ausgefüllten Gesuche schon korrigiert. Weil diese Arbeit, die eben nicht die Aufgabe des DSB ist, von diesem nicht mehr geleistet >

werden kann, hat er sich überlegt, sich auf seine Aufsichtsfunktion zurückzuziehen und jedes Gesuch, das nicht vollständig und korrekt ausgefüllt ist, einfach an die Vorinstanzen zur Korrektur zurückzuweisen. Dann wären die «Verweilzeiten» beim DSB extrem verkürzt worden. Allerdings hätte dies nicht echt zu einer Lösung geführt. Nach der Feststellung des DSB haben die gesuchstellenden öffentlichen Organe oft Mitarbeiter:innen aus der IT «verknurrt», die Gesuche auszufüllen. Die Rechtsabteilungen der Dienststellen oder Rechtsdienste der Departemente und teilweise sogar die Verantwortlichen der Fachbehörden waren oft in keiner Weise involviert. Die Korrektur nicht genehmigungsfähiger Gesuche hat deshalb mehrfach zu einem für alle Seiten mühsamen Hin und Her geführt.

Beschleunigungsvorschlag: Vorbereitung am «Round Table» Zur Vereinfachung und Beschleunigung hat der Datenschutzbeauftragte darum einen regelmässigen *«Round Table»* vorgeschlagen: Bevor die Gesuche gestellt und dann zeitfressend hin- und hergeschoben werden, sollen Vertreter:innen der gesuchstellenden Organe und der Dateneigner:innen zusammensitzen und die Gesuchstellung vorbereiten – das Team des DSB ist dabei und versucht allenfalls zu vermitteln und auf fehlende Informationen hinzuweisen. Dann können Vorbehalte der Dateneigner:innen gleich berücksichtigt werden. Es kann darauf hingewiesen werden, dass gewünschte Attribute gar nicht das hergeben, was sich die gesuchstellenden Organe darunter vorstellen. Hier wurde auch verbessert, dass nicht einem Gesuch zwingend ein bestehendes «Bild» zugeteilt wird, so dass ein öffentliches Organ zum Beispiel vier Attribute benötigt, aber 20 zugeteilt erhält, für die 16 «überzähligen» aber logischerweise keine Begründung bzw. Rechtsgrundlage angeben kann. Wenn beim «Round Table» Attribute ohne Angaben zur Rechtgrundlage verlangt werden, dann können Rechtsgrundlagen nachgeliefert oder kann auf die Attribute verzichtet werden.

Erste Erfahrungen Dieses «Vorverfahren» hat sich nach der Beurteilung des DSB gut angelassen und als zeitsparend erwiesen. Leider werden aber noch zu oft nicht alle Stellen in den Dienststellen bzw. Departementen beigezogen, die kompetent ihren Beitrag leisten müssten. Es wird zwar beispielsweise in der Einladung zum «Round Table» darauf hingewiesen, dass es sinnvoll sei, den Rechtsdienst einzubeziehen. Das geschieht aber oft nicht, so dass die Rechtsgrundlagen auch nach dem «Round Table» noch nicht klar sind. Da gibt es eindeutig noch Optimierungsbedarf. Die Einsicht muss wachsen, dass ein begrenzter Ressourceneinsatz zu Beginn das «Verbraten» von viel mehr Ressourcen im Laufe des Prozesses verhindern kann.

Erwartungen Die Übernahme der Verantwortung bei Abrufverfahren gehört zu den Aufgaben der Dateneigner:innen – und das wird künftig eher noch wichtiger, wenn das «Once only»-Prinzip, das in den Digitalisierungsstrategien von Bund und Kantonen enthalten ist, vermehrt zum Tragen kommen soll. Der DSB ist überzeugt, dass mit der neuen Vorbereitung die Durchlaufzeiten und die einzusetzenden Ressourcen deutlich verringert werden können. Dafür müssen aber auch die richtigen Leute an den Tisch. Das erwartet er von den öffentlichen Organen. Dann kann er seinen Teil der Aufgabe auch zügig und schnell erledigen.

Kantonaler Datenmarkt

Defizite Der Datenschutzbeauftragte hat im Rahmen seiner Beratungstätigkeit den Eindruck gewonnen, dass in Bezug auf die Umsetzung der Datenmarktverordnung bestimmte, zum Teil beträchtliche Altlasten bestehen:

— Zugriffsmöglichkeiten aufgrund abgelaufener (in der Regel auf fünf Jahre befristeter) Autorisierung;

— Zugriffsmöglichkeiten aufgrund von Autorisierungen, die noch in einem sehr summarischen Verfahren durch die Datenschutzkommission, die per Mitte 2005 durch den Datenschutzbeauftragten abgelöst worden ist, bzw. durch eben diesen Datenschutzbeauftragten, nicht aber, wie es seit Inkrafttreten des Informations- und Datenschutzgesetzes am 1. Januar 2012 gefordert ist, durch die Dateneigner:innen erteilt worden sind, oder

— Zugriffsmöglichkeiten, zu denen eine Bewilligungserteilung offensichtlich gar nicht dokumentiert ist, so dass auch nicht kontrolliert werden kann, ob sie je erfolgt ist.

Begonnene «Aufräumarbeiten» Unter der neuen Leitung von IT BS und der neuen Betreuung des Datenmarktes sind, nicht zuletzt auch auf Initiative des DSB hin, erste Anstalten getroffen worden, um diese Defizite aufzuspüren und zu beschreiben. Die bisherigen Erkenntnisse aus diesen Schritten bestätigen den Eindruck des DSB.

Aufforderung an die KOI Nach § 3 Abs. 1 DMV trägt die Konferenz für Organisation und Informatik (KOI) als Vertreterin der dateneinliefernden Organe die Gesamtverantwortung für den kantonalen Datenmarkt. Der DSB hat Ende 2021 die KOI um Auskunft darüber gebeten, mit welchen Massnahmen die KOI ihre Gesamtverantwortung wahrnimmt in Bezug auf die Sicherstellung, dass im Datenmarkt nur durch die Dateneigner:innen gültig autorisierte Zugriffe erfolgen können, und bis zu welchem Zeitpunkt sie sicherstellen kann, dass keine unautorisierten Zugriffe erfolgen können.

Der DSB hat die KOI um Auskunft darüber gebeten, mit welchen Massnahmen sie ihre Gesamtverantwortung wahrnimmt in Bezug auf die Sicherstellung, dass im Datenmarkt nur durch die Dateneigner:innen gültig autorisierte Zugriffe erfolgen können.

Pilotversuche

Berichtspflicht § 9a IDG erlaubt es, unter engen Voraussetzungen und zeitlich befristet im Rahmen von Pilotversuchen besondere Personendaten zu bearbeiten, ohne dass die nach § 9 Abs. 2 IDG erforderliche formellgesetzliche Grundlage besteht.[8] Bei der Beratung des § 9a IDG in der Justiz-, Sicherheits- und Sportkommission des Grossen Rates wurde grossen Wert darauf gelegt, dass die Umsetzung der Bestimmung durch den DSB eng begleitet wird.[9] Er soll jährlich darüber berichten, welche Pilotversuche laufen und insbesondere auch kontrollieren, ob Pilotversuche nach Ablauf der fünfjährigen Versuchsphase, falls die notwendige formellgesetzliche Grundlage nicht geschaffen wurde, tatsächlich definitiv eingestellt worden sind.

Laufende Pilotversuche Zurzeit läuft kein auf § 9a IDG gestützter Pilotversuch.

Kontrolltätigkeit

Datenschutzprüfungen (Audits) Dank der Verstärkung der IT-Kompetenzen im DSB-Team konnte auch die Kontrolltätigkeit verstärkt werden. Von den zahlreichen laufenden Audits konnte – u.a. auch wegen der Covid-19-Einschränkungen – nur ein einziges förmlich abgeschlossen werden (als förmlicher Abschluss wird die Zustellung des finalen Schlussberichts nach der Schlussbesprechung erachtet).

Audit beim Care Management Bei der Abteilung Care Management (CM) von Human Resources Basel-Stadt (HR BS) wurde eine Prüfung durchgeführt mit dem Fokus auf die Rechtmässigkeit des Bearbeitens von Personendaten, die notwendigen Grundlagen (Systembeschreibung, Schutzbedarfs- und Risikoanalyse, ISDS-Konzept) und die Kontrolle der Umsetzung der darin vorgesehenen Massnahmen, den IT-Betrieb (Rollen, Prozesse, Auditlogs und Benutzermanagement), Aufbewahrung und Vernichtung der Daten sowie Sensibilisierung im Umgang mit Personendaten. Zwei Feststellungen (zu unvollständigen Unterlagen und zu fehlenden Vorgaben an die IT-Betreiber) waren von mittlerer bis hoher Priorität und zwei (zu zu konkretisierenden gesetzlichen Bestimmungen und zur Archivierung/Vernichtung) von mittlerer Priorität.

Laufende Audits In den zwei Berichtsjahren begonnen, aber noch nicht abgeschlossen wurden die folgenden Audits:

— Datenschutzprüfung ISMS.BS bei IT BS;
— Datenschutzprüfung beim Universitären Zentrum für Zahnmedizin Basel (UZB);
— Audit zum Smartmeter Grid und Datentrennung bei den Industriellen Werken Basel (IWB);
— SIS-Kontrolle beim Migrationsamt Basel-Stadt, Abteilung Einreisen.[10]

Das IDG erlaubt es, unter engen Voraussetzungen und zeitlich befristet im Rahmen von Pilotversuchen besondere Personendaten zu bearbeiten, ohne dass die erforderliche formellgesetzliche Grundlage besteht. Zurzeit läuft kein solcher Pilotversuch.

Weitere Prüfhandlungen Der DSB hat auch weitere Untersuchungen vorgenommen, die aber letztlich nicht förmlich als Datenschutzprüfung daherkamen. Die Feststellungen im Zusammenhang mit der Umsetzung der Datenmarktverordnung (vorne S. 45 f.) fallen etwa in diese Kategorien. >

Informationszugangsgesuche

Berichtspflicht Nach § 31 Abs. 2 IDV stellt die Staatskanzlei die Statistik über die bei der kantonalen Verwaltung schriftlich eingereichten Informationszugangsgesuche nach dem Öffentlichkeitsprinzip der oder dem Datenschutzbeauftragten zur Berichterstattung nach § 50 IDG zu. Daraus kann abgeleitet werden, dass im Tätigkeitsbericht über die Umsetzung des Öffentlichkeitsprinzips zu berichten ist.

Statistik Die Informationszugangsgesuchs-Zahlen für die Jahre 2020–2021 finden sich – über die gesamte Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (S. 50). Nach Departement aufgeschlüsselt hat sie der Regierungsrat jeweils in seinem Jahresbericht veröffentlicht.[11]

Der Anteil der ganz abgewiesenen Informationszugangsgesuche nach dem Öffentlichkeitsprinzip, der in der Vorperiode gesunken war, stieg wieder deutlich auf fast die Hälfte an.

Erledigung Die Zahl der eingegangenen Gesuche stieg gegenüber der Vorperiode (Vorjahr 2019: 24 / 2020: 35 / 2021: 31). Der Anteil der ganz oder teilweise gutgeheissenen Gesuche fiel in den beiden Berichtsjahren leicht gegenüber dem Vorjahr von zwei Dritteln auf rund die Hälfte (Vorjahr 2019: 67% / 2020: 57% / 2021: 52%). Der Anteil der ganz abgewiesenen Gesuche, der in der Vorperiode gesunken war, stieg nun wieder deutlich auf fast die Hälfte an (Vorjahr 2019: 17% / 2020: 31% / 2021: 45%). Die Zahl der am Jahresende noch nicht erledigten Gesuche fiel deutlich (Vorjahr 2019: 17% / 2020: 11% / 2021: 3%). Ob die tiefere Gutheissungs- und höhere Abweisungsquote an der schlechteren Qualität der Gesuche lag oder an der tieferen Bereitschaft der Verwaltung, allfällige Geheimhaltungsinteressen als weniger gewichtig zu bewerten, kann ohne Kenntnis der Ablehnungsgründe nicht beurteilt werden.

Statistik zu den Geschäften des Datenschutzbeauftragten

Verweis Die Zahlen für die Jahr 2020–2021 finden sich im Statistikteil dieses Tätigkeitsberichts (S. 50).

Zwei Jahre (mit Vorjahresvergleich) Die Zahl der neu eröffneten Geschäfte hat sich im Jahr 2020 um 5% (543; Vorjahr 2019: 517) und 2021 um 7% (583) erhöht. Bei den Beratungsgeschäften ist der Anteil komplexer Geschäfte im Langzeitvergleich äusserst stabil (Vorjahr 2019: 13%, 2020: 14%, 2021: 16%). Von den nicht-komplexen Beratungsgeschäften wurden in den letzten beiden Jahren ein ähnlich grosser Anteil innert 14 Tagen abgeschlossen (Vorjahr 2019: 40% / 2020: 48% / 2021: 44%). Ebenfalls konnten im den letzten beiden Jahr wieder mehr Schulungen von öffentlichen Organen durchgeführt werden (Vorjahr 2019: 5 / 2020: 6 / 2021: 9).

Involvierte Stellen Recht stabil sind die Zahlen bei den Stellen, die in die vom Datenschutzbeauftragten bearbeiteten Geschäften involviert waren.[12] In den meisten Fällen verändern sich die Zahlen wenig. Abgenommen hat gegenüber dem Vorjahr der Anteil der Fälle, in denen der Datenschutzbeauftragte selber aktiv geworden ist (Vorjahr 2019: 11% / 2020: 5% / 2021: 6%).

Personelle Ressourcen des Datenschutzbeauftragten

Team Das Team des Datenschutzbeauftragten setzt sich Ende 2021 aus sieben Personen[13] zusammen, die sich 550 Stellenprozente teilen (100% Leitung, 210% Jurist:innen, 160% Informatiker, 80% Assistenz). 50% einer Jurist:innenstelle waren zum Jahreswechsel zurzeit vakant. Ausserdem bietet der DSB zweimal im Jahr eine sechsmonatige juristische Volontariatsstelle an.

Die starke Zunahme von Digitalisierungsprojekten bringt – unabhängig von der IDG-Revision – eine zusätzliche Belastung des Datenschutzbeauftragten.

Ausblick: Digitalisierungsprojekte In den beiden Berichtsjahren war festzustellen, dass das Team mit der Geschäftslast ausserordentlich stark gefordert ist. Wie auch im Ratschlag 21.1239.01 (Anpassung des IDG an die europäischen Datenschutzreformen) festgehalten, hält sich beim DSB der Mehraufwand *aufgrund der IDG-Revision* in Grenzen.[14] Aber die *starke Zunahme von Digitalisierungsprojekten* bringt – unabhängig von der IDG-Revision – eine zusätzliche Belastung des Datenschutzbeauftragten. Dabei geht es

keineswegs nur darum, ein paar kleine Apps zu begutachten. Die Einführung von M365 bei mehreren grossen Organisationseinheiten bindet auch beim DSB sehr viele Ressourcen. Dann laufen solche umfangreichen Projekte nicht nur parallel, sondern häufig auch unter hohem Zeitdruck, was die Planung des Ressourceneinsatzes noch schwieriger macht. Wenn beispielsweise für eine Stellungnahme zu einem Projektauftrag von gegen 60 Seiten mit mehreren, ihrerseits umfangreichen Beilagen für ein sehr wichtiges, auf mehrere Jahre geplantes Projekt gerade mal fünf Tage bleiben, dann bleiben logischerweise mal alle anderen Geschäfte liegen. Die Entwicklung der Belastung gilt es im Auge zu behalten – haben auch andere öffentliche Organe und vor allem auch die betroffenen Personen einen Anspruch darauf, dass ihre Anliegen bearbeitet werden.

1 § 1 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 1 N 5 ff.
2 § 44 IDG; vgl. dazu PK-IDG/BS-Schilling, § 44 N 1 ff., insb. N 8 ff. und 18 ff.
3 Vgl. zur Vorabkonsultation auch vorne S. 14 f.
4 Ratschlag 21.1239.01, Ziff. 3.2.17 (S. 32 ff.), neuer § 16a.
5 § 2 DMV. Vgl. dazu die ausführlichere Darstellung in TB 2017–2019, S. 24 f.
6 Vgl. TB 2017–2019, S. 24 f.
7 Vgl. zu den Defiziten bei der Umsetzung der Vorabkonsultation auch vorne S. 17 f.
8 Vgl. dazu die Ausführungen in TB 2016 des DSB/BS, S. 41, sowie PK-IDG/BS-Husi, § 9a N 6 ff.
9 Bericht 13.0739.02, S. 5 f.
10 Bei der SIS-Kontrolle wurde zwar der Entwurf des Schlussberichts noch im Jahr 2021 dem geprüften öffentlichen Organ zugestellt. Der DSB erfasst eine Datenschutzprüfung aber erst mit der Zustellung des finalen Schlussberichtes als abgeschlossen.
11 Jahresbericht 2020 (des Regierungsrates), 3.2.3 Staatskanzlei, Öffentlichkeitsprinzip, S. 71; Jahresbericht 2021 (des Regierungsrates), 3.2.3 Staatskanzlei, Öffentlichkeitsprinzip, S. 70.
12 Grafik E im Statistikteil (S. 51).
13 Zu den einzelnen Personen siehe Impressum (Umschlagsseite 3).
14 Ratschlag 21.1239.01, Ziff. 4, S. 58.

Statistische Auswertungen 2020–2021 (mit Vorjahresvergleich)

A Geschäfte

	2021		2020		2019		2018	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	583		543		517		472	
prozentuale Veränderung gegenüber Vorjahr		7		5		10		5

B Indikatoren gemäss Budget

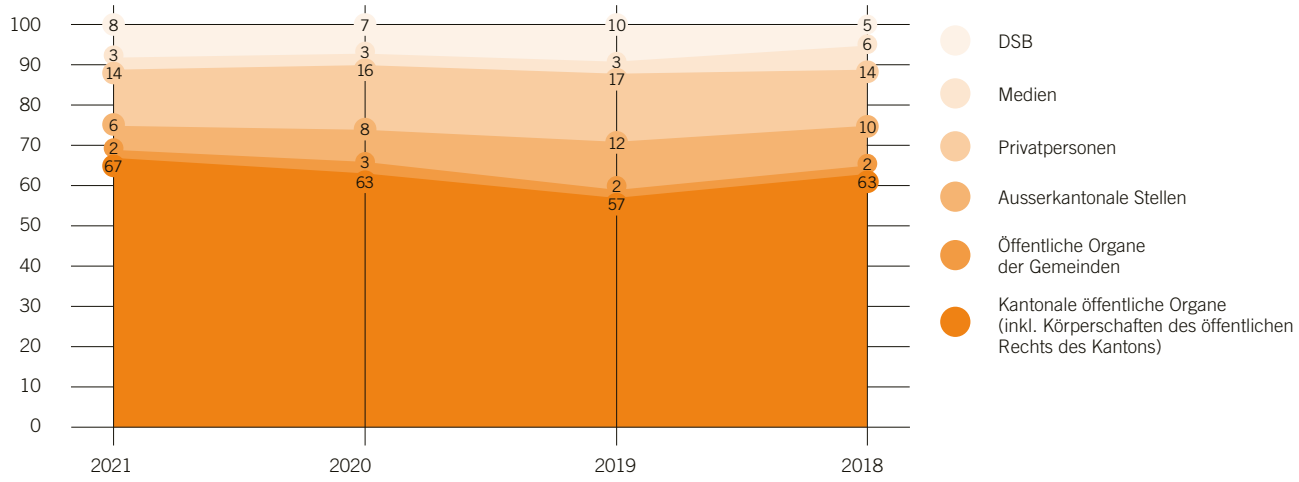
	2021		2020		2019		2018	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		16		14		13		13
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		44		48		40		55
Durchgeführte Audits								
Anzahl durchgeführte Audits	1		0		4		2	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	9		6		5		9	

C Öffentlichkeitsprinzip

	2021		2020		2019		2018	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	31		36		24		23	
prozentuale Veränderung gegenüber Vorjahr		-14		50		4		-38
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche	13	42	18	51	16	67	12	52
Anzahl teilweise gutgeheissener Gesuche	3	10	2	6	0	0	2	9
Anzahl ganz abgewiesener Gesuche	14	45	11	31	4	17	9	39
Anzahl noch nicht rechtskräftig entschiedener Gesuche	1	3	4	11	4	17	0	0

Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen (nicht enthalten sind jeweils die Zahlen zur Staatsanwaltschaft):
Jahresbericht 2020 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2020, S. 71
Jahresbericht 2021 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2021, S. 70

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %

«Involviert» sind die Stellen oder Personen, die ein Geschäft initiiert haben (D), und die Stellen, um deren Datenbearbeiten es geht. Beschwert sich eine Privatperson über eine Dienststelle eines Departements, so ist die Privatperson die Initiantin (D); unter E erscheint das Geschäft zusätzlich beim entsprechenden Departement.

Die Fälle dienen der Sensibilisierung der öffentlichen Organe, die vergleichbare Fragen zu beantworten haben. Sie knüpfen zwar an Fällen an, die der Datenschutzbeauftragte behandelt hat, sind aber «abgespeckt», aus mehreren Fällen kombiniert und/oder um zusätzliche Sachverhaltselemente angereichert worden. Sie haben sich also nicht genau so ereignet.

Fälle

Fall 1 Gesundheitsfragebogen vor der Einsicht in amtliche Dokumente

Fall 2 Identitätskontrolle im Museum (Covid-19-Zertifikat)

Fall 3 Verwendung von Contact Tracing-Daten zur Strafverfolgung

Fall 1 Gesundheitsfragebogen vor der Einsicht in amtliche Dokumente

Eine Dienststelle hat (viel) Kundenkontakt. Als der erste Lockdown über sie «hereinbricht», organisiert sie sich, um ihre Dienstleistungen auch unter den erschwerten Bedingungen erbringen zu können. Sie verlangt von Besucher:innen, auf einem Fragebogen Gesundheitsdaten anzugeben. Darf sie das?

Bei einer Dienststelle können berechtigte Personen (u.a.) Eingaben machen, Dokumente einsehen oder Besprechungen mit den Fachleuten der Dienststelle durchführen. Beim ersten Lockdown (Mai 2020) organisiert sie sich, um ihre Dienstleistungen auch unter den erschwerten Bedingungen erbringen zu können. Sie verlangt zu diesem Zweck von den Besucher:innen Antworten auf folgende drei Fragen:

— Sind sie positiv getestet worden oder hatten Sie Kontakt mit einer positiv getesteten Person?
— Fühlen Sie sich krank?
— Gehören Sie einer besonders gefährdeten Personengruppe (insb. …) an?
— Wer eine Frage mit Ja beantwortete, war – so auf jeden Fall der Eindruck, der bei den Personen, die den Fragebogen erhielten, entstand – vom Einsichtsrecht ausgeschlossen.

Datenschutzrechtlich stellt sich die Frage, ob ein öffentliches Organ Personendaten erheben darf. Dazu braucht es eine gesetzliche Grundlage[1] – bei besonderen Personendaten, z.B. bei Daten über die Gesundheit[2], eine Grundlage in einem Gesetz im formellen Sinn[3], und die Datenbearbeitung verhältnismässig sein.[4]

Bei dem Fall, der über die Ombudsstelle zum DSB kam, waren schon mal etliche Fragen offen: Sammelt die Dienststelle die Fragebogen ein? Was tut sie damit? Legt sie die ausgefüllten Fragebogen ab? Schliesst sie Personen, die eine Frage mit Ja beantwortet haben, vom Einsichts- (und damit evtl. sogar vom Einsprache-)recht aus (was wohl widerrechtlich wäre)? Wenn sie das tun wollte, müsste sie sich wie erwähnt auf eine gesetzliche Grundlage stützen können. Eine solche war schlicht nicht ersichtlich. Auch die Pflicht des Staates als Arbeitgeberin, für die Gesunderhaltung der Mitarbeiter:innen zu sorgen, hätte eine solche Datenerhebung nicht gesetz- und verhältnismässig gemacht. Oder lässt sie die Einsicht verlangenden Personen den Fragebogen für sich ausfüllen und fordert sie, wenn sie eine Frage mit Ja beantwortet haben, auf, sich mit ihr in Verbindung zu setzen, damit eine (kontaktlose) Abwicklung der Einsicht und allenfalls Einsprache möglich gemacht wird?

Bei der zweiten Variante erhebt die Dienststelle gar keine Gesundheitsdaten. Diese Variante ist zulässig. Sie hilft sicherzustellen, dass die Dienstleistungen der Dienststelle trotz der Pandemie aufrechterhalten werden können und die berechtigten Personen auch ihre Rechte angemessen ausüben können.

Allerdings war die erste Frage aus epidemiologischer Sicht nicht korrekt: Dass jemand positiv getestet worden war oder je mit einer positiv getesteten Person Kontakt gehabt hat, ist später, also nach Ablauf der Isolations- oder Quarantänefrist, kein Grund mehr für einen Ausschluss von einer Einsichtnahme vor Ort.

Die erste Variante – so, wie sie von Personen, die den Fragebogen erhielten, verstanden wurde – wäre nicht zulässig gewesen. Eine gesetzliche Grundlage für die Erhebung von Gesundheitsdaten war hier nicht gegeben. Auch die Pflicht des Staates als Arbeitgeberin, für die Gesunderhaltung der Mitarbeiter:innen zu sorgen, hätte eine solche Datenerhebung nicht gesetz- und verhältnismässig gemacht – wie die zweite Variante zeigt, kann der Zweck ja mit weniger einschneidenden Massnahmen erreicht werden.

Die Dienststellenleitung hat denn auf Nachfrage auch erklärt, dass der Fragebogen nur als Anregung zur Selbstbefragung gedacht war. Dann war aber mindestens die Kommunikation gegenüber den Einsichtsinteressierten oder Einspracheberechtigten alles andere als gut. Das wurde umgehend korrigiert.

Ergebnis

Die Erhebung von Gesundheitsdaten bedarf einer (formell-) gesetzlichen Grundlage. Die kann auch in mittelbarer Form vorliegen, wenn das Gesetz nur die vom öffentlichen Organ zu erfüllende Aufgabe klar festlegt und die Bearbeitung der besonderen Personendaten zur Erfüllung dieser Aufgabe zwingend notwendig ist. Das war hier nicht der Fall. Es hat gereicht, die Einsicht verlangenden Personen, die sich z.B. krank fühlen, aufzufordern, sich zwecks Organisation einer coronagerechten Einsichtnahme mit der Amtsstelle in Verbindung zu setzen.

1 § 9 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 14 ff.
2 § 3 Abs. 4, insb. lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 33 ff., insb. 37.
3 § 9 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 25 ff.
4 § 9 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 ff.

Fall 2 Identitätskontrolle im Museum (Covid-19-Zertifikat)

Im Herbst 2021 wurde die Covid-19-Zertifikatspflicht ausgeweitet. Bestimmte Orte durften nur noch mit einem gültigen Zertifikat besucht werden. Ein Zertifikat konnte ausgestellt werden aufgrund von Impfungen, einem Test oder dem Nachweis einer Covid-19-Erkrankung). Darf eine öffentliche Einrichtung das Zertifikat kontrollieren und einen Identitätsausweis verlangen?

Unter diese ausgeweitete Zertifikatspflicht fielen beispielsweise die Museen. Da stellte sich den Verantwortlichen die Frage: Dürfen sie von den Besucher:innen überhaupt einen Ausweis verlangen und die Personalien überprüfen, um festzustellen, ob es sich um die Person handelt, deren Zertifikat vorgewiesen wird?

Personendaten (oder besondere Personendaten) dürfen bearbeitet werden, wenn eine unmittelbare oder mittelbare gesetzliche Grundlage dies vorsieht und die Datenbearbeitung verhältnismässig[1] ist. Eine *unmittelbare* gesetzliche Grundlage regelt unmittelbar das Bearbeiten von (besonderen) Personendaten.[2] Statuiert die gesetzliche Grundlage bloss eine Aufgabe, die nur erfüllt werden kann, indem (besondere) Personendaten bearbeitet werden, stellt dies eine *mittelbare* gesetzliche Grundlage dar.[3]

Die Zertifikatspflicht für Museen findet sich (bzw. fand sich in relevanten Zeitpunkt) in Art. 13 Abs. 2 der Covid-19-Verordnung besondere Lage (Stand am 13. September 2021)[4], die der Bundesrat gestützt auf Art. 6 Abs. 2 lit. a und b des Epidemiengesetzes (EpG) erlassen hat. Danach müssen öffentlich zugängliche Einrichtungen und Betriebe in den Bereichen Kultur, Unterhaltung, Freizeit und Sport, in denen den Besucher:innen nicht ausschliesslich Aussenbereiche offenstehen, bei Personen ab 16 Jahren den Zugang auf Personen mit einem Zertifikat beschränken. Wenn das Museum nicht einfach darauf vertrauen will, dass die Besucher:innen diese Vorgabe einhalten, dann muss dies kontrolliert werden, was nur geht, wenn die Zertifikate und die Identität der Besucher:innen angeschaut (und verglichen) werden. Im Anhang 2 (Vorgaben für Schutzkonzepte für öffentlich zugängliche Einrichtungen und Betriebe sowie Veranstaltungen, die bei Personen über 16 Jahren den Zugang auf Personen mit einem Zertifikat einschränken) wird in Ziffer 2 lit. a^{bis} denn auch konkretisiert, dass Personen anhand eines geeigneten Identitätsnachweises mit Foto zu überprüfen sind.

Die Aufsichtsorgane der Museen dürfen (bzw. müssen) also zum vorgewiesenen Zertifikat einen Identitätsnachweis mit Foto verlangen und prüfen, ob Name, Vorname und Geburtsdatum mit den Angaben auf dem Zertifikat und die Foto auf dem Ausweis (Pass, Identitätskarte, Führerausweis) mit der das Zertifikat vorweisenden Person übereinstimmen. Ausdrücklich festgehalten ist ausserdem, dass die Daten zu keinen anderen Zwecken bearbeitet werden dürfen; nicht erlaubt wäre also das Erstellen einer Liste, wer das Museum besucht hat, um diesen Kulturinteressierten künftig beispielsweise Werbung zukommen zu lassen (was das anfragende Museum auch nicht vorhatte).

Ergebnis

Wenn der Bund, gestützt auf das Epidemiengesetz, in einer Verordnung den Zugang zu bestimmten Einrichtungen vom Vorliegen eines Zertifikats abhängig macht, dann darf (bzw. muss) diese Einrichtung das Zertifikat und die Identität der vorweisenden Person kontrollieren. Mehr darf mit diesen Daten aber nicht getan werden.

1 § 9 Abs. 3 IDG (gilt auch für das Bekanntgeben von [besonderen] Personendaten); vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 ff.
2 § 9 Abs. 1 und 2, jeweils lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 16. Grundsätzlich dasselbe gilt nach § 21 Abs. 1 und 2, jeweils lit. a IDG für das Bekanntgeben von (besonderen) Personendaten.
3 § 9 Abs. 1 und 2, jeweils lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 17. Grundsätzlich dasselbe gilt nach § 21 Abs. 1 und 2, jeweils lit. b IDG für das Bekanntgeben von (besonderen) Personendaten.
4 Fassung gemäss Ziff. I der Verordnung vom 8. September 2021 (Ausweitung der Verwendung des Covid-19-Zertifikats), in Kraft vom 13. September 2021 bis zum 24. Januar 2022 (AS 2021 542 547).

Fall 3 Verwendung von Contact Tracing-Daten zur Strafverfolgung

Im Herbst 2021 ermittelte die Staatsanwaltschaft in einem schweren Delikt. Die beiden beteiligten Personen – potentieller Täter und Opfer – sollen sich vorher in einem Unterhaltungsbetrieb getroffen haben. Da bei einem solchen Betrieb aus epidemiologischen Gründen Contact Tracing-Daten erhoben werden mussten, haben Medienschaffende die Frage gestellt, ob diese Contact Tracing-Daten zur Ermittlung der Täterschaft beigezogen werden dürften.

Zur Bekämpfung der Weiterverbreitung von Covid-19 mussten (u.a.) Restaurations-, Club- und Barbetriebe Kontaktdaten (Vorname und Name, Wohnort und Telefonnummer) ihrer Besucher:innen aufnehmen. Wenn nun Strafuntersuchungsbehörden bei einem schweren Strafdelikt die Täterschaft zu ermitteln haben und bekannt oder möglich ist, dass sich der potentielle Täter vorher in einem solchen Betrieb aufgehalten hat, darf dann die Untersuchungsbehörde die Herausgabe der Contact Tracing-Daten verlangen? Die Strafbehörden verfügen nach Art. 192 ff. der Strafprozessordnung (StPO) über weitgehende Befugnisse zur Erhebung von Beweismitteln, kann sich also für die Erhebung auf eine (formell-)gesetzliche Grundlage stützen.

Grundlage für die Datenerhebung durch den Betrieb bildet Art. 11 der Covid-19-Verordnung besondere Lage. Diese Bestimmung (in Kraft bis 24. Januar 2022) regelt die Erhebung der Kontaktdaten, die Information der betroffenen Personen (Abs. 1) und die Bekanntgabe der Daten auf Anfrage an die (für die Rückverfolgung von Covid-19-Ansteckungen) verantwortliche kantonale Behörde zwecks Identifizierung und Benachrichtigung ansteckungsverdächtiger Personen (Abs. 2). Abs. 3 hält schliesslich ausdrücklich fest: Die Daten «dürfen zu keinen anderen Zwecken als denjenigen nach dieser Verordnung bearbeitet werden, müssen bis 14 Tage nach dem Besuch der Einrichtung oder des Betriebs oder nach der Teilnahme an der Veranstaltung aufbewahrt und anschliessend sofort vernichtet werden.»

Art. 11 Abs. 3 Covid-19-Verordnung besondere Lage schliesst also eine Verwendung für einen anderen Zweck aus. Aber: Diese Regelung steht nur auf Verordnungsstufe, weshalb sie nach den juristischen Kollisionsregeln durch eine Regelung (des Bundes) auf Gesetzesstufe übersteuert werden könnte – zum Beispiel eben von einer StPO-Bestimmung.

Allerdings – so die Auskunft des Datenschutzbeauftragten an die Medienschaffenden – würde er der für das Contact Tracing verantwortlichen kantonalen Stelle (wenn die Daten schon bei ihr sind) von einer Herausgabe der Contact Tracing-Daten abraten. Sind die Daten nur beim Gastbetrieb vorhanden (weil das Contact Tracing keine Veranlassung hatte, die Daten herauszuverlangen), dann könnte der Gastbetrieb sich mittels Beschwerde gegen die Herausgabeverfügung (Editionsverfügung) wehren, wenn die Strafverfolgungsbehörde die Daten herausverlangt und er der Meinung ist, dass sie das nicht dürfe. Allerdings müsste er im Falle des Unterliegens dafür die Kosten tragen.

Hätte der Gastbetrieb die Daten herausgeben müssen (was aber letztlich nicht der Fall war, weil die Staatsanwaltschaft die Täterschaft auf anderem Weg ermitteln konnte), dann wären genau die Befürchtungen wahrgeworden, die gegen die Einführung der Kontaktdaten-Erhebung durch Gastbetriebe geäussert wurden. Das würde zu einem riesigen Vertrauensverlust gegenüber den aus epidemiolgischer Sicht als notwendig erachteten Massnahmen führen. Ausserdem wäre die Abgrenzung, für welche Straftaten ein Zugriff gerechtfertigt wäre, äusserst schwierig. Es wäre zu befürchten, dass mit der Herausgabe dieser Daten ein eigentlicher Dammbruch erfolgen würde.

Ergebnis

Die Strafverfolgungsbehörde muss abwägen zwischen der Verfolgung einer Straftat und dem Unterlaufen von Massnahmen zur Pandemiebekämpfung. Wenn es andere Möglichkeiten zur Ermittlung der Täterschaft gibt, würde der Datenschutzbeauftragte der Staatsanwaltschaft raten, die anderen Möglichkeiten zu nutzen. Allerdings hat der DSB nach der Regelung im IDG kein Recht, der Staatsanwaltschaft in hängigen Strafverfahren Empfehlungen abzugeben.[1]

1 § 2 Abs. 2 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 2 N 18 ff.

Anhang

Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

Kanton Basel-Stadt:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

aDSG Gesetz vom 18. März 1992 über den Schutz von Personendaten (Datenschutzgesetz), SG 153.260 (in Kraft bis 31. Dezember 2011).

DMV Verordnung vom 4. Juli 2017 über den Datenmarkt (Datenmarktverordnung, DMV), SG 153.310.

GesG Gesundheitsgesetz vom 21. September 2011 (GesG), SG 300.100.

IDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz), SG 153.260.

IDV Verordnung vom 5. August 2011 über die Information und den Datenschutz (Informations- und Datenschutzverordnung), SG 153.270.

KV/BS Verfassung des Kantons Basel-Stadt vom 23. März 2005, SG 111.100.

PolG Gesetz vom 13. November 1996 betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG), SG 510.100.

V-BWIS Verordnung vom 21. September 2010 über den Vollzug des Bundesgesetzes zur Wahrung der inneren Sicherheit, SG 123.200 (recte: Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit)

Materialien, Berichte

E-IDG Entwurf zur Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) gemäss dem Ratschlag 21.1239.01.

Ratschlag 21.1239.01 Ratschlag 21.1239.01 des Regierungsrates vom 29. September 2021 zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze (Anpassung an die europäischen Datenschutzreformen und weitere Anpassungen).

Bericht 13.0739.02 Bericht 13.0739.02 der JSSK vom 16. Oktober 2013 Bericht 13.0739.02 der Justiz, Sicherheits- und Sportkommission vom 16. Oktober 2014 zum Ratschlag betreffend Änderung des Gesetzes über die Information und den Datenschutz (IDG) zwecks Schaffung einer gesetzlichen Grundlage für die Bearbeitung von besonderen Personendaten im Rahmen von Pilotversuchen.

Bund:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

BV Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.

Covid-19-Verordnung besondere Lage Verordnung vom 23. Juni 2021 über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie (Covid-19-Verordnung besondere Lage), SR 818.101.26 (Stand am 13. September 2021).

DSG Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

EpG Bundesgesetz vom 28. September 2012 über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EpG), SR 818.101.

PBG Bundesgesetz vom 20. März 2009 über die Personenbeförderung (Personenbeförderungsgesetz, PBG), SR 745.1.

revDSG Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG) (Referendumsvorlage: BBl 2020 7639, Inkrafttreten voraussichtlich am 1. September 2023).

SDSG Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3.

StGB Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.

StPO Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung), SR 312.0.

VDSG Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11 (wird voraussichtlich per 1. September 2023 abgelöst durch eine neue DSV).

Materialien

E-DSG Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 7193 (E-DSG: BBl 2017 7206 / Botschaft dazu: BBl 2017 6941)

Europarat, Europäische Union, USA:
Rechtsgrundlagen

Rechtsgrundlagen

CLOUD Act Clarifying Lawful Overseas Use of Data Act (CLOUD Act); H.R. 4943

DSGVO (oder: Verordnung [EU] 2016/679) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119, 4.5.2016, S. 1-88.

Europarats-Konvention 108 Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981, SR 0.235.1 (für die Schweiz in Kraft getreten am 1. Februar 1998).

Europarats-Konvention 108+ Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten in der Fassung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens.

Richtlinie (EU) 2016/680 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 119, 4.5.2016, S. 89–131.

Tätigkeitsberichte

TB (Jahr) des DSB/BS Tätigkeitsbericht (Jahr) des Datenschutzbeauftragten des Kantons Basel-Stadt, abrufbar unter: https://www.dsb.bs.ch/ueber-uns/taetigkeitsberichte.html

Anhang

Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

Literatur

BSK-Strafrecht I-Autor:in Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht I, Art. 1-110 StGB, Jugendstrafgesetz, 3. Auflage, Basel 2013.

PK-IDG/BS-Autor(in) § xx N yy Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014.

Häfelin/Müller/Uhlmann Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 8., überarbeitete Auflage, Zürich/St. Gallen 2020.

Abkürzungen

AS Amtliche Sammlung (des Bundesrechts)
BAG Bundesamt für Gesundheit
BBl Bundesblatt
BKB Basler Kantonalbank
BVB Basler Verkehrs-Betriebe
CM Care Management (Abteilung in HR BS)
DPA Data Protection Amendment (Zusatzvereinbarung zum Datenschutz)
DSB Datenschutzbeauftragte:r
DSFA Datenschutz-Folgenabschätzung
DVS Digitale Verwaltung Schweiz
EDÖB Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte:r
EuGH Europäischer Gerichtshof
HERMES Hermes (Projektmanagement-Methode)
HR BS Human Resources Basel-Stadt (vormals: Zentraler Personaldienst Basel-Stadt)
IGB Israelitische Gemeinde Basel
ISB Informationssicherheits-Beauftragte:r (des Kantons)
ISB(D) Informationssicherheits-Beauftragte:r (eines Departements)
ISDS-Konzept Informationssicherheits- und Datenschutz-Konzept
ISMS Informationssicherheits-Managementsystem
ISO (frühere) Fachabteilung Informatiksteuerung und -organisation)
IWB Industrielle Werke Basel
JSSK Justiz-, Sicherheits- und Sportkommission (des Grossen Rates Basel-Stadt)
KBM Kantonales Bedrohungsmanagement
KOI Konferenz für Organisation und Informatik
M365 Microsoft 365
MIOL Microsoft Ireland Operations Ltd.
MS Microsoft
PET Privacy Enhancing Technologies (Technologien zur Verbesserung des Datenschutzes)
PM.BS Projektmanagement für den Kanton Basel-Stadt
RPA Robotic Process Automation
SaaS Software as a Service
SCC Standard Contractual Clauses (Standard-Vertragsklauseln)n
SG Systematische Gesetzessammlung (des Kantons Basel-Stadt)
SIK Schweizerische Informatikkonferenz
SGF Systematische Gesetzessammlung (des Kantons Freiburg)
SIS Schengener Informationssystem
SLSP Swiss Library Service Platform
SR Systematische Rechtssammlung (des Bundes)
Suva Schweizerische Unfallversicherungsanstalt
UZB Universitäres Zentrum für Zahnmedizin Basel

Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 205, 4010 Basel
Tel. 061 201 16 40
datenschutz@dsb.bs.ch
www.dsb.bs.ch

Datenschutzbeauftragter
Beat Rudin, Prof. Dr. iur., Advokat

Team
per 31.12.2021:
Eva Maria Bader (Sekretariat)
Pascal Lachenmeier, Dr. iur., Advokat
Sukhwant Singh, Master in IT Business Engineering
Thomas Sterchi, Wirtschafts-informatiker HF
Ines Weihrauch, lic. iur., Advokatin
Barbara Widmer, Dr. iur.,LL.M., CIA

früher im Berichtszeitraum:
Deborah De Col, MLaw
(befristet 01.11.–15.12.2021)

Volontär:innen:
Alina Schneider, MLaw
(1.1.2020–30.6.2020)
Aurin Schweizer, MLaw
(1.7.2020–31.12.2020)
Deborah De Col, MLaw
(1.1.2021–30.6.2021)
Matthias Plattner, MLaw
(1.7.2021–31.12.2021)

Bericht an den Grossen Rat
Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt
ISSN 1664-1868

Bezug
Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 205, 4010 Basel
Tel. 061 201 16 40
datenschutz@dsb.bs.ch
www.dsb.bs.ch

Gestaltung
Andrea Gruber,
gruber gestaltung, Basel

Druck
Druckerei Dietrich AG, Basel