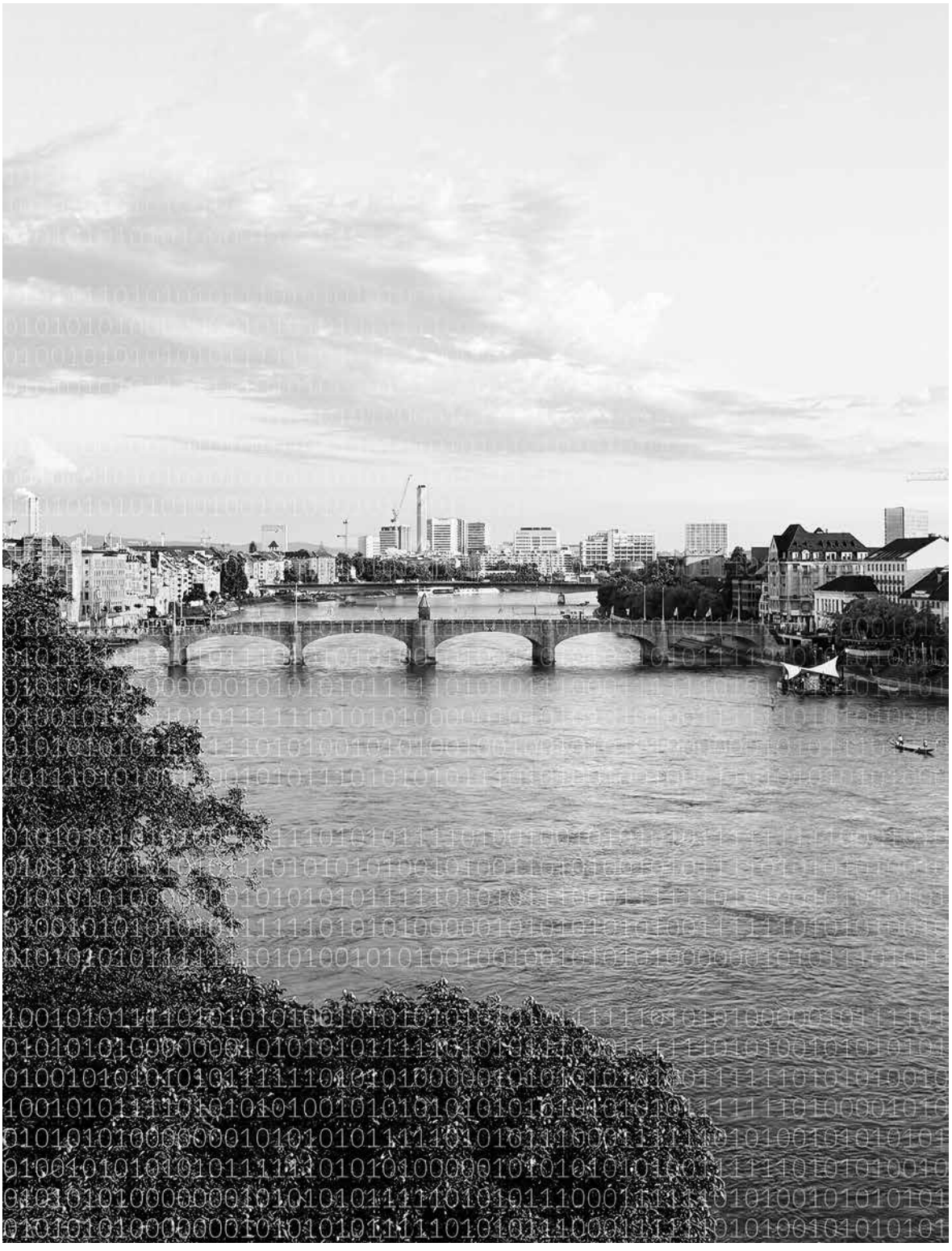
Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat



'23

Die/der Datenschutzbeauftragte erstattet der Wahlbehörde und der Öffentlichkeit periodisch und bei Bedarf Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes (§ 50 revIDG).

Fotokonzept: Basler Brücken
Fotos: B. Rudin

Inhaltsübersicht

Einleitung

Themen

Jahres-rückblick

Anhang

Einleitung

2023: Die grossen Themen bleiben

Der Rückblick auf das Jahr 2023 lässt ein paar Themen in den Vordergrund treten: Die vom Grossen Rat im Oktober 2022 beschlossene Teilrevision des Informations- und Datenschutzgesetzes trat noch nicht in Kraft, weil die dazugehörende Verordnung noch nicht revidiert ist. Die Vorbereitungen für die Umsetzung der Revision laufen und werden hier vorgestellt. Ausserdem soll auf die weiterhin herausfordernden «Grossbaustellen» hingewiesen werden.

Auf Papier

Nochmals gedruckt Sie halten meinen letzten Tätigkeitsbericht in den Händen. In den Händen, weil er nochmals gedruckt erscheint – trotz der Interpellation Daniel Seiler betreffend Drucksachen und Jahresberichte (Geschäft 23.5356)[1]. Er erscheint nochmals in dieser Form, weil nach den Rückmeldungen, die wir übers Jahr erhalten, ein Heft eher gelesen wird als ein PDF-File. Das stimmt auch mit meinem Leseverhalten überein: Ein Heft nehme ich später nochmals in die Hand und blättere es durch. Selbst wenn ich es nicht von vorne bis hinten durchlese, so stosse ich doch auf Themen, die mich interessieren (oder interessieren müssten).

In Zukunft Selbstverständlich wird meine Nachfolgerin für sich entscheiden, in welcher Form sie in Zukunft die Berichterstattungspflicht nach § 50 des Informations- und Datenschutzgesetzes (IDG[2]) erfüllen will.

Womit hat sich der Datenschutzbeauftragte beschäftigt?

IDG-Revision Ein Thema, das den Datenschutzbeauftragten (DSB) im vergangenen Jahr stark beschäftigt hat (und es auch im laufenden Jahr immer noch tut), ist die Vorbereitung auf den Zeitpunkt, in dem das revidierte IDG in Kraft treten wird. Der Grosse Rat hat die Teilrevision (revIDG) am 20. Oktober 2022 beschlossen. Der Regierungsrat legt fest, wann sie in Kraft treten wird. Zuvor muss er aber auch die Informations- und Datenschutzverordnung (IDV) revidieren, um sie an die IDG-Änderungen anzupassen. Das wird frühestens im September 2024 der Fall sein. Informationen zur «IDG-Revision auf der Kriechspur» finden Sie im nachfolgenden Teil ab S. 8 ff.

Fit sein für das neue IDG Was kommt auf die öffentlichen Organe zu, wenn die beiden Revisionen in Kraft treten? Die Änderungen betreffen zum grössten Teil nicht die einzelnen Mitarbeiter:innen der öffentlichen Organe, sondern die Leitungen, welche die Umsetzung der Neuerungen organisieren müssen, z.B. *die Informationspflicht* beim Beschaffen von (nach § 15 revIDG neu auch «gewöhnlichen») Personendaten, die *Meldepflicht bei Datenschutzverletzungen* (nach § 16a revIDG), die Festlegung der *Gesamtverantwortung*, wenn mehrere öffentliche Organe einen gemeinsamen Informationsbestand bearbeiten (nach § 6 Abs. 2 revIDG), der *Nachweis der Einhaltung der Datenschutzvorschriften* (nach § 6 Abs. 3 revIDG) sowie die Bezeichnung der *Datenschutzberater:innen* (§ 16b revIDG). Ausserdem ist durch die Leitungen dafür zu sorgen, dass die erweiterten Vorschriften betreffend die Prüfung der Datenschutzkonformität von Vorhaben (Schwellwertanalyse, Datenschutz-Folgenabschätzung nach § 12a revIDG, Vorabkonsultation nach § 13 revIDG) umgesetzt werden können. Darüber finden Sie Informationen hinten ab S. 15 ff.

Unterstützung Die/der DSB unterstützt die verantwortlichen öffentlichen Organe dabei, indem verschiedene Dokumentationen zur Verfügung gestellt werden: eine Schwellwertanalyse (SWA) für die Beantwortung der Frage, ob bei einem Vorhaben eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden muss, eine Anleitung für die SWA, die DSFA und die Vorabkonsultation sowie ein Formular für Meldung von Datenschutzverletzungen. Ausserdem bietet sie/er Unterstützung für die Datenschutzberater:innen an.

«Grossbaustellen» Den DSB haben im vergangenen Jahr weiterhin auch altbekannte «Grossbaustellen» beschäftigt. Auf fünf von ihnen – die fehlende (IT-)Governance, Projektmanagement und Projektmanagement-Kompetenz, Cybersicherheit, sichere Kommunikation und Digitale Souveränität – soll hier nochmals kurz hingewiesen werden (S. 20 ff.).

Jahresrückblick Was der DSB im vergangenen Jahr auch noch getan hat, darüber wird im Jahresrückblick berichtet (S. 26 ff.). Ein besonderes Augenmerk wird dabei auf den Kantonalen Datenmarkt und den Gang in die Cloud (Programm «Connect 365») gerichtet. Es folgen Informationen über die abgeschlossenen und laufenden Datenschutzprüfungen und zur Statistik zu den Geschäften des DSB (Statistik S. 36 f.).

Zum Schluss

Spannende Zeit Mit dem Rücktritt per Ende Juli 2024 beende ich meine Tätigkeit als DSB. Ich schaue auf 15½ tolle, ereignisreiche Jahre zurück. Als ich anfing, trat gerade die «Schengen»-Reform des baselstädtischen Datenschutzgesetzes in Kraft, die Revision, die nötig war, damit auch das Basler Gesetz den Anforderungen des EU-Datenschutzrechts genügt, so dass die Schweiz dem Schengen-Abkommen beitreten konnte. 2012 kam der Wechsel zum IDG, mit dem auch das Öffentlichkeitsprinzip eingeführt wurde. Und am 20. Oktober 2022 hat der Grosse Rat eine grössere Teilrevision des IDG beschlossen, mit der erreicht werden soll, dass das Gesetz den Anforderungen der modernisierten Europaratskonvention 108+ und dem revidierten EU-Datenschutzrecht (insbesondere der Schengen-relevanten Richtlinie [EU] 2016/689) genügt. Diese Revision sollte in naher Zukunft in Kraft treten können.

Danke! Es ist mir ein grossen Anliegen, allen zu danken, die das Datenschutz-Team in dieser Zeit beim Schutz der Privatheit der Einwohner:innen, über welche die öffentlichen Organe Daten bearbeiten, unterstützt haben. Ohne diese Unterstützung hätten wir diese Aufgabe nicht erfolgreich erfüllen können. Der Dank gilt insbesondere:

— den Mitarbeiter:innen der Verwaltung von Kanton und Gemeinden, der öffentlich-rechtlichen Anstalten und der Gerichte, die mitgeholfen haben, datenschutzkonforme Lösungen zu finden und umzusetzen;

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

— den aktuellen und ehemaligen Kolleg:innen der «Kleeblattdienststellen» für die gute Zusammenarbeit;

— den aktuellen und ehemaligen Kolleg:innen der Datenschutzaufsichtsstellen des Bundes und der anderen Kantone, insbesondere denjenigen, die aktiv im Büroausschuss und Büro von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, mitgearbeitet haben;

— dem Grossen Rat für das Vertrauen, das er mir mit der Wahl und zweifachen Wiederwahl entgegengebracht hat, und

— den Präsidien und Mitgliedern des Ratsbüros, der Datenschutz-Delegation des Büros und der Kommissionen, mit denen wir zusammenarbeiten durften, für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung.

Ein spezieller Dank Mein ganz spezieller Dank geht an alle Mitglieder des Datenschutz-Teams, an die ehemaligen ebenso wie an diejenigen im Jahr 2023 (Eva Maria Bader, Sama Bolog, Pascal Lachenmeier, Sukhwant Singh, Thomas Sterchi, Ines Weihrauch und Barbara Widmer) sowie an die Volontär:innen (im Jahr 2023 Pascal Tamm). Ihr grosses Engagement, ihre kritische Neugier, die spannenden Diskussionen und ihr wertvoller Input haben die erfolgreiche Arbeit erst möglich gemacht.

Viel Erfolg! Es ist mir zum Schluss ein Anliegen, meiner Nachfolgerin Danielle Kaufmann zusammen mit ihrem Team auch weiterhin viel Erfolg zu wünschen bei der wichtigen Aufgabe zum Schutz der Grundrechte der Einwohner:innen unseres Kantons!

Beat Rudin, ehemaliger Datenschutzbeauftragter

1 <https://grosserrat.bs.ch/ratsbetrieb/geschaefte/200112597>.
2 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Ende des Berichts (S. 38 f.) detailliert aufgeführt.


NOVARTIS

Themen

Thema 1 Die IDG-Revision auf der Kriechspur

Thema 2 Schwellwertanalyse, Datenschutz-Folgenabschätzung und Vorabkonsultation

Thema 3 Weiterhin herausfordernde «Grossbaustellen»

Thema 1

Die IDG-Revision auf der Kriechspur

Es eilt dem Kanton offensichtlich nicht, sein Datenschutzrecht an die internationalrechtlichen Anforderungen anzupassen. IDG-Ratschlagsentwurf im Januar 2019 ans Präsidialdepartement, Ratschlag an den Grossen Rat im September 2021, Grossratsbeschluss im Oktober 2022 – und die Revision der IDV ist vom Regierungsrat immer noch nicht beschlossen.

Der Grossratsbeschluss vom 20. Oktober 2022

IDG-Revisionsbeschluss Wie bereits im TB 2022 erwähnt, hat der Grosse Rat am 20. Oktober 2022 die Revision des Informations- und Datenschutzgesetzes (IDG) so beschlossen, wie es ihm die Justiz-, Sicherheits- und Sportkommission (JSSK) beantragt hat. Bevor das revidierte IDG (revIDG) in Kraft gesetzt werden kann, muss der Regierungsrat noch die IDV anpassen.

Der Grosse Rat hat am 20. Oktober 2022 die Revision des Informations- und Datenschutzgesetzes (IDG) beschlossen. Bevor das revidierte IDG (revIDG) in Kraft gesetzt werden kann, muss der Regierungsrat noch die IDV anpassen.

IDV-Planung Ursprünglich war einmal die Rede von einem Revisionsbeschluss des Regierungsrates vor den Sommerferien 2023, im Herbst 2023 wurde vom Inkrafttreten am 1. April 2024 gesprochen. Inzwischen sind die Sommerferien 2024 da, und es ist – mehr als 21 Monate nach dem Grossratsbeschluss – noch immer kein Beschluss zur IDV ergangen. Aktuell (uns mitgeteilter Planungsstand anfangs Juli 2024) soll der Regierungsratsbeschluss im September 2024 ergehen und sollen das revidierte IDG und die revidierte IDV auf den 1. Oktober 2024 in Kraft gesetzt werden. Für die Umsetzung braucht es Vorbereitung. Der DSB ist davon ausgegangen, dass ab dem Regierungsratsbeschluss drei bis vier Monate notwendig sind, um in allen öffentlichen Organen bereit zu sein für das Inkrafttreten der Revision. Geplant hat der DSB Einführungskurse für Leitungsorgane und die Datenschutzberater:innen – gemeinsam mit dem Informationssicherheitsbeauftragten des Kantons. Da der IDV-Revisionsbeschluss erst im September ergehen soll, werden diese Kurse nun in die Einarbeitungszeit der neuen DSB fallen.

Fit sein für das neue IDG

Was muss vorbereitet werden? Die Änderungen des revIDG und voraussichtlich der revIDV bringen weniger Neues für die Mitarbeiter:innen von Kanton und Gemeinden als für die öffentlichen Organe und ihre Leitungen: Sie müssen Vorkehrungen treffen, damit die folgenden Neuerungen umgesetzt werden können:

Informationspflicht bei der Datenbeschaffung (§ 15 revIDG)

Informationspflicht Nach § 15 Abs. 1 revIDG muss das verantwortliche öffentliche Organ die betroffenen Personen über jede Beschaffung von Personendaten informieren, auch wenn die Daten nicht bei ihnen, sondern bei Dritten beschafft werden. Eine Beschaffung von Personendaten liegt vor, wenn ein öffentliches Organ aktiv und gewollt Kenntnis von Daten erlangt oder die Verfügung darüber begründet. Die IDV wird konkretisieren, in welcher Form die Information erfolgen kann bzw. muss.

Umfang der Information § 15 Abs. 2 revIDG führt auf, welche Informationen für die betroffenen Personen bereitzustellen sind, insb. Angaben

— über das verantwortliche öffentliche Organ samt Kontaktdaten;

— über die bearbeiteten Daten (oder die Kategorien der bearbeiteten Daten);

— über die Rechtsgrundlage und den Zweck des Bearbeitens;

— über die Datenempfänger:innen (oder die Kategorien der Datenempfänger:innen), sofern die Daten Dritten bekannt gegeben werden; nach dem Gesetzestext sind alle Datenempfänger:innen anzugeben. Es kann aber vom verantwortlichen öffentlichen Organ nicht erwartet werden, dass es jede in der Zukunft denkbare (Einzel-)Datenbekanntgabe voraussieht und hier angibt. Korrekt ausgelegt müssen deshalb nur die

Datenempfänger:innen angegeben werden, denen wiederkehrend Personendaten bekannt gegeben werden;

— über die Rechte der betroffenen Person.

Ausnahmen von der Informationspflicht Nach § 15 Abs. 3 revIDG entfällt die Informationspflicht,

— wenn die betroffene Person bereits über die Informationen verfügt,

— wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder

— wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist; es darf aber nicht vorschnell angenommen werden, die Information sei unverhältnismässig.

Es ist nicht verboten (aber vielleicht zur Schaffung von Vertrauen durchaus zu empfehlen), die Betroffenen im Interesse der Transparenz zu informieren, auch wenn wegen einer gesetzlichen Pflicht nicht informiert werden muss.

Ausnahmen: Beispiele Die *Datengewinnung des Statistischen Amtes* aus vorhandenen Datenbeständen der öffentlichen Organe beispielsweise ist ausdrücklich gesetzlich vorgesehen (§ 6 Abs. 1 StatG), weshalb keine Informationspflicht gilt. Die Personalabteilung ist verpflichtet, die Daten der neu eingetretenen Mitarbeiter:innen der Ausgleichskasse und, wenn die entsprechenden Voraussetzungen erfüllt sind, der Pensionskasse bekannt zu geben. Über solche Bekanntgaben *muss* bei der Beschaffung nicht gestützt auf § 15 revIDG informiert werden. Es ist aber selbstverständlich *nicht* verboten (aber vielleicht zur Schaffung von Vertrauen durchaus zu empfehlen), die Betroffenen im Interesse der Transparenz zu informieren.

Vorbehalt Sollte in der IDV die Ausnahme *generell* ausgeweitet auf *alle Bekanntgaben von Personendaten zu nicht personenbezogenen Zwecken* (Statistik, Forschung, Planung), dann ist darauf hinzuweisen, dass ein gewisses Risiko besteht, dass ein Gericht diese generelle Ausnahme als zu weitgehend beurteilt, weil sie durch die gesetzlich vorgesehenen Ausnahmetatbestände (§ 15 Abs. 3 revIDG) nicht gedeckt sei.

Form der Information Das verantwortliche öffentliche Organ muss entscheiden, wie es die Informationspflicht umsetzen will, z.B.:

— mit einem Informationstext auf dem Anmelde- oder Gesuchsformular, auf Papier oder auf einem Web-Formular;

— durch die Aushändigung eines Informationsblatts oder einer Informationsbroschüre, nicht aber bloss durch das Auflegen des Blattes oder der Broschüre am Eingang.

Meldepflicht bei Datenschutzverletzungen (§ 16a revIDG)

Meldepflicht § 16a revIDG verpflichtet die öffentlichen Organe neu dazu, eine Datenschutzverletzung ohne unangemessene Verzögerung der/dem DSB zu melden. Die Leitung des öffentlichen Organs muss sicherstellen, dass bei einer Datenschutzverletzung diese Meldung erfolgt.

Datenschutzverletzung Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten (§ 16a Abs. 3 revIDG). Keine Meldepflicht besteht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt (§ 16a Abs. 4 revIDG). Das darf aber nicht vorschnell angenommen werden; im Zweifelsfall empfiehlt sich eine Rücksprache mit der/dem DSB.

Meldeformular Der DSB hat auf seiner Webseite ein Meldeformular samt Anleitung veröffentlicht. Das Formular wird sowohl für die Erstmeldung (innert höchstens 72 Stunden, nachdem das öffentliche Organ von der Datenschutzverletzung Kenntnis erlangt hat) als auch für die Folgemeldung verwendet, wenn bei der Erstmeldung noch nicht alle Informationen verfügbar waren.

Festlegung der Gesamtverantwortung (§ 6 Abs. 2 revIDG)

Gesamtverantwortung Eine wesentliche Änderung sieht auch § 6 Abs. 2 revIDG vor: Wenn mehrere öffentliche Organe einen gemeinsamen Informationsbestand bearbeiten, müssen sie neu auch festlegen, welches öffentliche Organ die Gesamtverantwortung trägt. >

Umfang Die Gesamtverantwortliche ist nicht «für alles verantwortlich», aber verantwortlich für die Verteilung der Verantwortung. Sie muss anordnen, *wer wofür verantwortlich* ist, und allenfalls weitere Vorgaben für die Umsetzung machen. Im Resultat ist sie verantwortlich für alles, was nicht einer verantwortlichen Stelle/Person zugeordnet ist. Wichtig ist, auch dafür zu sorgen, dass die (Teil-)Verantwortlichen über die für die Umsetzung notwendigen (fachlichen, personellen und finanziellen) *Ressourcen* verfügen. Und schliesslich muss die Gesamtverantwortliche auch ein Auge darauf haben, ob ihre Anordnungen umgesetzt werden, und nötigenfalls Durchsetzungsmassnahmen ergreifen.

Die Gesamtverantwortliche ist nicht «für alles verantwortlich», aber verantwortlich für die Verteilung der Verantwortung.

Bestimmung der Gesamtverantwortung Die Bestimmung richtet sich nach dem Grundsatz, der schon vor der Revision in § 6 Abs. 1 IDG enthalten war: Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet – es ist also nicht die IT. Was muss geschehen, wenn die Gesamtverantwortung noch nicht geregelt ist? Es ist jedem öffentlichen Organ, das mit anderen öffentlichen Organen einen gemeinsamen Informationsbestand bearbeitet, zu empfehlen, zu verlangen, dass die Gesamtverantwortung einer der beteiligten Stelle zugeteilt wird. Unklare Zuweisungen der Verantwortlichkeit bergen das Risiko in sich, dass notwendige Massnahmen nicht getroffen werden, weil sich keine Stelle zuständig fühlt. Deshalb haben bei der Weiterentwicklung der Fachanwendung für Migration und Wirtschaft die Departemente der beteiligten Dienststellen (des Bereichs Bevölkerungsdienste und Migration BdM und des Amtes für Wirtschaft und Arbeit AWA) vereinbart, dass die Gesamtverantwortung beim JSD liegt. Eine entsprechende Regelung haben der DSB und die Finanzkontrolle auch bezüglich des Elektronischen Logiernächte-Meldesystem ELM verlangt, wo drei Dienststellen (das Amt für Wirtschaft und Arbeit AWA, die Kantonspolizei und das Statistische Amt) aus drei Departementen (WSU, JSD und PD) die von den Hotels usw. gemeldeten Gästedaten durch eine Auftrags- und eine Unterauftragsdatenbearbeiterin bearbeiten lassen, ohne dass das Verhältnis zwischen den dreien klar geregelt ist.

Nachweis für die Einhaltung der Datenschutzvorschriften (§ 6 Abs. 3 revIDG)

Nachweispflicht Nach § 6 Abs. 3 revIDG muss jedes öffentliche Organ nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Nachweis für jedes System, mit dem Personendaten bearbeitet werden, kann durch eine Dokumentation erbracht werden, die eine Beschreibung der Bearbeitung der Personendaten, eine Darstellung der Rechtslage, eine Beschreibung der Risiken und Abhilfemassnahmen und eine Beschreibung der Prozesse und Verantwortlichkeiten umfasst. Kurz: durch die Dokumentation, die bei einer Datenschutz-Folgenabschätzung erstellt und zur Vorabkonsultation bei der/dem DSB eingereicht werden muss (vgl. hinten S. 15 ff.). Der Nachweis kann auch in einem strukturierten Datenschutz- oder Informationssicherheits-Managementsystem erfolgen, wenn ein solches vorhanden ist.

Übergangsfrist Für bestehende Datenbearbeitungssysteme ist der Nachweis für die Einhaltung der Datenschutzbestimmungen nach einer Übergangsfrist zu erbringen. Der DSB hatte eine Frist von drei Jahren als angemessen bezeichnet. Was brächte eine längere Frist? Wenn ein System vorher abgelöst wird, braucht es für das abgelöste System logischerweise den Nachweis nicht mehr. Weil das aber nicht häufig der Fall sein dürfte, wird es wohl immer schwieriger (und mühsamer), für ein älteres System den Nachweis zu erbringen. Und es ist zu befürchten, dass dann der Termin einfach vergessen oder auf den St. Nimmerleinstag verschoben wird.

Im konkreten Fall vor Ablauf der Übergangsfrist Der DSB hat vorgeschlagen, in die Übergangsbestimmung ausdrücklich die Vorschrift aufzunehmen, dass der Nachweis bei einer bestimmten Datenbearbeitung innert angemessener Frist zu erbringen ist, wenn ihn eine betroffene Person oder eine Aufsichtsorgan vor Ablauf der Übergangsfrist verlangt. Es wäre ein Irrtum zu glauben, ein öffentliches Organ müsse den Nachweis vor Ablauf nicht erbringen. § 6 Abs. 3 IDG sieht diese Einschränkung nicht vor. Es ist auch materiell falsch: Ein öffentliches Organ muss belegen können, dass es das Gesetz einhält – davon befreit ein Schweigen in einer Verordnung nicht.

Datenschutz-Folgenabschätzung (§ 12a IDG) und Vorabkonsultation (§ 13 Abs. 1 lit. b revIDG)

Verweis Zur Verstärkung des präventiven Datenschutzes vgl. hinten S. 15 ff.

Bestimmung der Datenschutzberater:innen (§ 16b revIDG)

Grossratsbeschluss Abweichend vom regierungsrätlichen Ratschlag hat der Grosse Rat auf Antrag der JSSK[1] einstimmig beschlossen, dass – neben den Dienststellen, die dies aufgrund der Schengen-relevanten Richtlinie (EU) 2016/680 tun müssen[2] – auch alle Departemente der kantonalen Verwaltung, die Gerichte und die Einwohner- und Bürgergemeinden eine:n Datenschutzberater:in (DSBer) zu bezeichnen haben (§ 16b Abs. 1 revIDG). Ausserdem soll der Regierungsrat bestimmen, welche Bereiche, Abteilungen und Stabsstellen der kantonalen Verwaltung sowie welche öffentlich-rechtlichen Anstalten des kantonalen Rechts darüber hinaus eigene Datenschutzberater:innen bezeichnen müssen (§ 16b Abs. 2 revIDG). Dabei soll er, wie die JSSK ausdrücklich festgehalten hat, die Art und die Menge der bearbeiteten Personendaten berücksichtigen sowie – ohne dass er im Gesetzestext auf die zwingende Einhaltung des übergeordneten Rechts hingewiesen werden muss – die «Schengen-relevanten Behörden» berücksichtigen.[3]

Wo Personendaten (und besonders, wo besondere Personendaten) bearbeitet werden, braucht es eine Stelle mit Datenschutz-Fachkompetenz, welche die Datenschutzrelevanz erkennt und auf die Einhaltung der entsprechenden Vorschriften hinwirken kann.

Wohl nur Minimallösung Der Regierungsrat hat sich schon im Grossen Rat gegen die Pflicht, Datenschutzberater:innen zu bezeichnen, gewehrt. Dem DSB wurde vor einem Jahr auch mitgeteilt, dass sich die Mehrheit der Departemente gegen mehr als die Minimallösung ausgesprochen haben sollen. Das lässt vermuten, dass unterhalb der Departementsstufe neben den Schengen-spezifischen Dienststellen (Kantonspolizei, Staatsanwaltschaft, Bevölkerungsdienste und Migration BdM) wohl ausschliesslich Stellen dazu verpflichtet werden dürften, die schon vorher von sich aus Datenschutzberater:innen bezeichnet haben (wie z.B. das Amt für Wirtschaft und Arbeit AWA, die Sozialhilfe, die Industriellen Werke Basel iwb, öffentliche Spitäler und die Universität Basel).

(Fehl-)Entwicklungen Dass sich der Regierungsrat (mindestens in seiner Mehrheit) sehr schwer tut mit der Einführung der Datenschutzberater:innen, war – wie vorne erwähnt – schon während der Beratung im Grossen Rat unübersehbar. Falls er nun bloss eine Minimallösung beschliessen sollte, übersieht er, dass die bisherigen (Fehl-)Entwicklungen sehr laut nach der Schaffung dieser Funktion rufen. Es braucht überall in der Verwaltung, wo Personendaten (und besonders, wo besondere Personendaten) bearbeitet werden, eine Stelle mit Datenschutz-Fachkompetenz, welche die Datenschutzrelevanz erkennt und auf die Einhaltung der entsprechenden Datenschutzvorschriften hinwirken kann. Wenn die Weichen bei einem Projekt am Anfang falsch gestellt werden, indem nicht erkannt wird, dass (besondere) Personendaten bearbeitet werden, dann wird es schwierig, das Projekt datenschutzkonform umzusetzen.

Ein erfundenes Schreckgespengst? Leider nein. Der DSB hat beispielsweise das System, das letztlich dem «ED-Hack» zum Opfer gefallen ist, wie in solchen Fällen üblich nicht vertieft geprüft, weil laut der ihm vorgelegten Schutzbedarfsanalyse nur gewöhnliche Personendaten bearbeitet werden sollten. Entweder war diese Information falsch – oder in der Umsetzung wurde nicht dafür gesorgt, dass alle, die Daten in das System hochladen konnten, wussten, wofür sie es nutzen dürfen: eben nicht für besondere Personendaten. Bei einem anderen Projekt bezüglich der Zusammenarbeit im Bereich Migration und Schwarzarbeit hat sich erst im Laufe der Zeit herausgestellt, dass darin nicht – wie ursprünglich beschrieben – anonymisierte Personendaten, sondern unanonymisierte Personendaten (und sogar unanonymisierte besondere Personendaten) bearbeitet werden sollen.

Aufgaben Die Datenschutzberater:innen beraten und unterstützen in ihrem Zuständigkeitsbereich die öffentlichen Organe bei der Bearbeitung von Personendaten, unterstützen sie bei der Vornahme der DSFA und arbeiten mit der/dem DSB zusammen (§ 16b Abs. 3 revIDG). Zur Unterstützung kann auch beitragen, dass sie zur Gewährung der Rechte der betroffenen Personen beigezogen werden (z.B. wenn diese ein Gesuch nach § 26 IDG um Zugang zu den eigenen Personendaten stellen und nach § 29 IDG geprüft werden muss, ob besondere gesetzliche Geheimhaltungsbestimmungen oder überwiegende öffentliche oder private Geheimhaltungsinteressen entgegenstehen). Sie können den Entscheid vorbereiten, aber entscheiden muss schliesslich die Leitung des öffentlichen Organs. >

Garant:innen für die Qualität bei der Schwellwertanalyse (SWA) Die DSBer haben insbesondere beim präventiven Datenschutz eine eminent wichtige Aufgabe. Wie hinten (S. 15 ff.) beschrieben, muss ein öffentliches Organ bei jedem Vorhaben den Schwellwertanalyse-Fragebogen ausfüllen. Wenn gar keine Personendaten bearbeitet werden oder zwar Personendaten bearbeitet werden, aber kein hohes Risiko für die Betroffenen entsteht, dann muss keine Datenschutz-Folgenabschätzung durchgeführt werden. Um unnötigen Verwaltungsaufwand zu vermeiden, muss das Formular nicht der/dem DSB vorgelegt werden, wenn sich kein Bedarf nach einer DSFA ergibt, sondern es wird in den Projektakten abgelegt. Wird es nicht richtig ausgefüllt, dann sind die Weichen für das Projekt von Anfang an falsch gestellt. Den DSBer kommt hier eine entscheidende Bedeutung zu: Sie sind die *Garant:innen für die Qualität*. Deshalb sieht der DSB vor, dass sie das ausgefüllte Formular auch unterschreiben müssen – wie das ja im Bereich der Informationssicherheit von den departementalen Informationssicherheitsbeauftragten (ISBD) auch verlangt wird.

Den Datenschutzberater:innen kommt hier eine entscheidende Bedeutung zu: Sie sind die Garant:innen für die Qualität.

Garant:innen für die Qualität bei der DSFA und VAK Dieselbe Bedeutung erlangen die DSBer bei der DSFA und der VAK (siehe hinten S. 19). Der DSB will eine Vorabkonsultation nur anhand nehmen, wenn die einzureichenden Dokumente nicht nur durch die Leitung des verantwortlichen öffentlichen Organs (§ 12a Abs. 1 und § 13 Abs. 1 i.V.m. § 6 revIDG), sondern – zur Qualitätssicherung – auch durch die/den zuständige:n DSBer abgenommen sind. Nur so kann sichergestellt werden, dass aus Sicht des einreichenden öffentlichen Organs die zum Schutz der Grundrechte der betroffenen Personen erforderlichen Datenschutzmassnahmen vorgesehen sind, bevor die Prüfung durch die/den DSB erfolgen soll.

Hoffnung auf die Departemente und Dienststellen Wie aus Diskussionen zu entnehmen ist, dürfte die revIDV wohl bloss die Minimallösung vorsehen. Dann wäre die Funktion der/des DSBer vermutlich in fünf Departementen einzig auf Stufe Departement vorgesehen. Ob diese DSBer die gesetzliche Aufgabe effizient und zeitgerecht erfüllen können, wird sich wohl sehr rasch zeigen. Es besteht die Hoffnung, dass die Departemente und Dienststellen bald erkennen, dass es ihnen mehr hilft, das Datenschutz-Knowhow dort zu bündeln, wo regelmässig besondere Personendaten und/oder Personendaten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen, bearbeitet werden. Die einzelnen Departemente und Dienststellen können auch mehr vorsehen, als die IDV verlangt (wenn sie denn so beschlossen wird). Es geht ja nicht um eine neue Aufgabe: Die DSBer haben Aufgaben zu erfüllen, die bereits seit 2009, seit dem Inkrafttreten der «Schengen-Revision» des DSG, zu erfüllen waren: die Vorbereitung der Vorabkontrolle – in der Terminologie des revIDG: die DSFA als Vorbereitung der VAK.

Klassifizierung (§§ 18 ff. IDV)

Toter Buchstabe Die geltende IDV enthält Klassifizierungsvorschriften (§§ 18–22 IDV). Doch der alte § 18 IDV blieb weitgehend[4] toter Buchstabe. Jedes öffentliche Organ, das schutzwürdige – was «schutzwürdig» sei, wurde nicht definiert – Informationen verfasst, sollte sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der Klassifizierungsstufen «geheim» oder «vertraulich» zuzuweisen. Die Kriterien für die Zuweisung zu den Stufen «geheim» (§ 19 IDV) und «vertraulich» (§ 20 IDV) basieren auf den Einschränkungsgründen von § 29 IDG, sie wurden aber um andere ergänzt – vielleicht gut gemeint, aber inkonsistent.[5] Völlig unbrauchbar ist die Konsequenz aus der Zuweisung zu einer Klassifikation: «Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen» (§ 22 IDV). Eine gesetzgeberische Meisterleistung – das sagt schon das Verhältnismässigkeitsprinzip (§ 9 Abs. 3 IDG i.V.m. § 21 IDG). In der Praxis wurden diese Bestimmungen, abgesehen von Informationen in Regierungsgeschäften,[6] schlicht auch gar nicht umgesetzt.

Herkommen Der Wortlaut der Klassifizierungsvorschriften stammt – jedoch mit entscheidenden Abweichungen und Anreicherungen – weitgehend aus der (alten) Informationsschutzverordnung des Bundes. Allerdings knüpft die Bundesverordnung auch klare Konsequenzen an die Klassifikation, z.B. bezüglich der Geheimnisträger:innen und bezüglich der Bearbeitung der klassifizierten Informationen, und schafft Sicherheitsorgane[7]. Darauf verzichtete die Regelung in der IDV – die einzige «Konsequenz» ist die im letzten Absatz zitierte Bestimmung von § 22 IDV, die keinerlei Mehrwert bringt.[8]

Engerer Geltungsbereich Der DSB schlägt vor, den Geltungsbereich der §§ 18–22 IDV nun sinnvollerweise auf die Regierungsgeschäfte zu reduzieren.

Dringender Bedarf nach einem Klassifizierungssystem Spätestens im Zusammenhang mit dem Gang in die Cloud, aber auch mit der Datenstrategie des Kantons wird es unumgänglich sein, eine taugliche Klassifizierung einzuführen. Diese Herausforderung wird besser heute als erst morgen in Angriff genommen. Und es wird entscheidend sein, damit auch klar zu regeln, was mit klassifizierten Informationen geschehen darf und was nicht.

Befristung der Autorisierung von Online-Zugriffen in der Verordnung

Fehlende Befristung Nach § 9b Abs. 1 und 2 IDV bedarf die Bekanntgabe von Personendaten mittels Abrufverfahren einer Autorisierung durch die Dateneigner:innen, d.h. durch die verantwortlichen öffentlichen Organe im Sinne von § 6 IDG; die Autorisierung ist der/dem DSB zur Vorabkonsultation vorzulegen. Die praktisch identische Regelung enthält § 5 DMV für die Online-Zugriffe auf den Datenmarkt («Datenauslieferungen»). Seit jeher gilt faktisch die Befristung der Autorisierungen durch die Dateneigner:innen auf maximal fünf Jahre (so schon die höchste auswählbare Frist auf den Datenmarkt-Zugriffs-Gesuchformularen seit den 1990er Jahren) – sie ist aber nicht in einem Gesetz oder einer Verordnung festgelegt.

Vorschlag des DSB Der DSB schlägt vor, die faktisch geltende Fünfjahresfrist in die IDV und in die DMV aufzunehmen. Spätestens vor Ablauf dieser Frist sei zu prüfen, ob die gesetzlichen Grundlagen den Datenzugriff im Abrufverfahren immer noch erlauben und ob die Berechtigungen noch angemessen sind. Damit würde auch eine Empfehlung der Finanzkontrolle bezüglich des Datenmarktes erfüllt.

Und wenn nicht? Es wäre für den DSB nicht nachvollziehbar, wenn diese Änderung nicht aufgenommen würde. Widerstand könnte von Stellen kommen, die überhaupt keine Befristung wollen, oder von Stellen, die eine Befristung auf weniger als fünf Jahre wollen (z.B. ein oder zwei Jahre). Der DSB plädiert – wie die Finanzkontrolle – auf jeden Fall für eine Verankerung der Frist. Sicher würde eine kurze Frist für aktuellere Verhältnisse sorgen, weil Änderungen der Rechtsgrundlagen oder der faktischen Verhältnisse schneller berücksichtigt werden können. Dem gegenüber steht aber die Frage, ob der zusätzliche Aufwand für die ein- oder zweijährige Frist diesem Gewinn angemessen wäre oder ob eine Pflicht, bei Veränderungen zeitnah für die Anpassung des Gesuchs bzw. der Autorisierung zu sorgen, nicht genügen würde.

Schriftlichkeit beim Auftrag zur Datenbearbeitung durch Dritte innerhalb des Kantons

Auftragsdatenbearbeitung Bei der Auftragsdatenbearbeitung beauftragt ein verantwortliches öffentliches Organ Dritte, für seine Zwecke bestimmte Informationen zu bearbeiten (§ 7 IDG). Es gibt also die Datenbearbeitung aus der Hand, bleibt aber dafür verantwortlich (§ 7 Abs. 2 IDG). Darum muss es sicherstellen, dass die Informationen nur so bearbeitet werden, wie es selber das tun dürfte (§ 7 Abs. 1 lit. b IDG).

Der DSB schlägt vor, die faktisch geltende Fünfjahresfrist für die Geltung von Autorisierungen von Online-Zugriffen in die Informations- und Datenschutzverordnung und in die Datenmarktverordnung aufzunehmen.

Schriftlichkeit beim Auftrag an Externe Die geltende IDV legt in ihrem § 1 fest, dass der Auftrag zum Bearbeiten von Personendaten durch Organisationseinheiten oder Private, welche dem Gesetz über die Information und den Datenschutz nicht unterstehen, schriftlich erteilt werden muss – aber eben ausschliesslich dann, wenn die Auftragsdatenbearbeiter:innen Externe sind.

Festgestellte Defizite Der DSB weist auf die Notwendigkeit einer Änderung von § 1 IDV hin. Die Erfahrung hat gezeigt, dass Probleme auch entstehen, wenn in solchen «Zusammenarbeitsformen» zwischen öffentlichen Organen, die dem IDG unterstehen, unklar ist, wer genau wofür verantwortlich ist, wenn also notwendige Punkte (AKV: Aufgaben, Kompetenzen, Verantwortlichkeiten) nicht geregelt sind. Es besteht die Gefahr, dass sowohl das auftraggebende öffentliche Organ als auch das öffentliche Organ, das die Personendaten in dessen Auftrag bearbeitet (z.B. IT BS) annehmen, dass die jeweils andere Seite für bestimmte Aspekte sorgt. Mit einer klaren schriftlichen Regelung, die nicht ausufernd lang sein muss, werden im Interesse der beiden Seiten die Verantwortlichkeiten geklärt (wie auf technischer Seite z.B. durch *Service level agreements SLA*). Damit wird verhindert, dass eine Datenschutzverletzung erfolgt, weil nicht klar war, wer für welche Schutzmassnahmen sorgen muss. Ein solches Dokument hilft auch, wenn es darum geht, den Nachweis der Datenschutzkonformität zu erbringen (§ 6 Abs. 3 revIDG). >

Vorschläge des DSB Angesichts dieser Defizite schlägt der DSB vor, die Schriftlichkeit auch bei der Auftragsdatenbearbeitung durch Dritte innerhalb des Kantons zu verlangen. Eine Lösungsvariante besteht darin, den eingeschobenen Nebensatz «welche dem Gesetz über die Information und den Datenschutz nicht unterstehen» zu streichen. Eine zweite Variante würde den Abs. 1 unverändert lassen, aber den § 1 durch einen neuen Abs. 2 ergänzen, der vorschreibt, dass beim Auftrag zum Bearbeiten von Personendaten an öffentliche Organe, die dem IDG unterstehen, die Aufgaben, Kompetenzen und Verantwortlichkeiten klar und schriftlich geregelt sein müssen.

Angesichts der aufgeführten Defizite schlägt der DSB vor, die Schriftlichkeit auch bei der Auftragsdatenbearbeitung durch Dritte innerhalb des Kantons zu verlangen.

Gegenargumente In verschiedenen Diskussionen hat sich gezeigt, dass wenig Bereitschaft besteht, § 1 IDV anzupassen. Ein Grund soll – so wurde u.a. argumentiert – sein, dass die verschiedenen öffentlichen Organe mangels Rechtspersönlichkeit gar keine Verträge untereinander schliessen könnten. Nur geht es hier nicht um «Verträge», wie sie beispielsweise mit privaten Auftragsdatenbearbeiter:innen geschlossen werden, sondern um das gemeinsame Festhalten von Verantwortlichkeiten, Qualitätsanforderungen usw., wie z.B. in den bereits erwähnten Service level agreements (SLA). Aus der Verwaltung kam auch ein Hinweis auf Art. 6 Abs. 2 VDSG, nur ist die VDSG am 1. September 2023 durch die DSV abgelöst worden (darum: aVDSG). Und deren Art. 6 handelt von den Bearbeitungsreglementen, die im Bund bei bestimmten automatisierten Bearbeitungen zu erlassen sind. Diese Reglemente müssen «insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten» (Art. 6 Abs. 2 DSV). Solche Reglemente sind in Basel-Stadt nicht vorgeschrieben. Wenn der Regierungsrat für automatisierte Bearbeitungen («automatisiert» kommt aus der Europarats-Konvention 108 und meint: Bearbeitungen durch Computer) solche Bearbeitungsreglemente einführen will, wird sich die/der DSB nicht dagegen wehren. Es wäre aber wohl einfacher, in § 1 IDV für die Regelung der Aufgaben, Kompetenzen und Verantwortlichkeiten die Schriftlichkeit auch unter öffentlichen Organen, die dem IDG unterstehen, vorzusehen.

Hoffnung auf die Departemente und Dienststellen Je mehr Zwischenfälle sich aufgrund unklarer Verantwortungszuweisung ereignen, umso eher ist zu hoffen, dass die Departemente und Dienststellen solche Regelungen von sich aus schriftlich festhalten. Auch wenn der Regierungsrat die Schriftlichkeit nicht vorschreibt – die öffentlichen Organe tun gut daran, die Verteilung der Aufgaben, Kompetenzen und Veranwortlichkeiten untereinander klar und schriftlich zu regeln.

1 Bericht 21.1239.02, S. 11 ff.
2 Der Regierungsrat hat dies im Ratschlag 21.1239.01, S. 35 und 50–53, nur vorgesehen für die Kantonspolizei, die Staatsanwaltschaft und für das Amt für Justizvollzug.
3 Bericht 21.1239.02, S. 14 (zu § 16b Abs. 2).
4 Praktisch überall ausserhalb der Regierungsgeschäfte.
5 Dazu Beat Rudin, Klassifikation: eine Etikette für alles?, digma 2015, S. 100 ff., insb. S. 103.
6 Und nur dafür hatte die Staatskanzlei bei der Schaffung der IDV die Regelung auch vorgeschlagen; verschiedene Mitglieder des Regierungsrates verlangten aber – wohl aus Furcht vor dem Öffentlichkeitsprinzip – die Ausweitung auf alle Informationen, die von öffentlichen Organen verfasst werden (PK-IDG/BS-Rudin, § 29 N 70).
7 Dazu Beat Rudin, Klassifikation: eine Etikette für alles?, digma 2015, S. 100 ff., insb. S. 102.
8 Vgl. dazu PK-IDG/BS-Rudin, § 29 N 69.

Thema 2 Schwellwertanalyse, Datenschutz-Folgenabschätzung, Vorabkonsultation

Mit der Revision des Informations- und Datenschutzgesetzes soll der präventive Datenschutz gestärkt werden. Das revIDG sieht vor, dass bei Vorhaben, bei denen voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht, eine Datenschutz-Folgenabschätzung vorzunehmen und das Vorhaben der/dem DSB zur Vorabkonsultation vorzulegen ist. Der DSB hat die entsprechenden Anleitungen ausgearbeitet.

Präventiver Datenschutz

Vorher genauer hinschauen Das revidierte IDG stärkt den präventiven Datenschutz:[1] Lieber vorher genauer hinschauen als nachher reparieren müssen. Zu diesem Zweck verlangt es – wie international-rechtlich vorgeschrieben –, dass Vorhaben für eine Personendatenbearbeitung abgeklärt wird, ob vor aussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht (§ 12 revIDG). Anschliessend muss das Vorhaben (wie bisher) der/dem DSB zur Vorabkonsultation (früher: zur Vorabkontrolle) vorgelegt werden (§ 13 revIDG).

Hohes Risiko Wann ein hohes Risiko besteht, wird durch die *Informations- und Datenschutzverordnung* (IDV) konkretisiert. Weil die Risiken sich im dynamischen IT-Umfeld sehr rasch ändern können, beauftragt das revIDG die/den DSB, eine *Liste der vorabkonsultationspflichtigen Bearbeitungsvorgänge* zu erstellen.

Umsetzungshilfen Der DSB hat für die Bewältigung dieser Pflichten Umsetzungshilfen entwickelt. Diese und die (voraussichtlichen) Regelungen in der revidierten IDV sollen hier vorgestellt werden. Wie schon vorne S. 8 ausgeführt, ist zur Zeit der Verfassung des Tätigkeitsberichts die IDV-Revision vom Regierungsrat noch nicht beschlossen.

Keine Personendaten – keine Datenschutz-Folgenabschätzung

Gar keine Personendaten Sollen mit der projektierten Anwendung (oder mit der Erneuerung einer Anwendung weiterhin) *gar keine Personendaten* bearbeitet werden, können also mangels Personenbezug gar keine Risiken für die Grundrechte der betroffenen Personen entstehen, dann entfällt die Datenschutz-Folgenabschätzung klarerweise.

Personendaten – aber hohes Risiko?

Risikokriterien in der IDV Wann bei einem Vorhaben voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen vorliegt, wird durch die IDV konkretisiert: Ein hohes Risiko für die Grundrechte der betroffenen Personen im Sinn von § 12a Abs. 1 (und § 13 Abs. 1 lit. b) revIDG dürfte insbesondere vorliegen, wenn ein Vorhaben zur Bearbeitung von Personendaten:

— ein *Abrufverfahren* vorsieht[2] (wie bisher);

— besondere Personendaten (wie bisher) oder Personendaten, die einem *Berufs- oder besonderen Amtsgeheimnis* unterstehen, betrifft;

— ein *Profiling* umfasst;

— eine *grosse Anzahl von Personen* betrifft (wie bisher);

— eine *Auftragsdatenbearbeitung durch Dritte in einem Staat ohne angemessenen Datenschutz umfasst* oder

— die Errichtung eines *Datenpools* im Sinne von § 1a umfassen soll (wie bisher),

— … und natürlich auch, wenn ein *Gesetz* oder eine *Verordnung* vorschreibt, ein bestimmtes Vorhaben sei der/dem DSB zur Vorabkontrolle vorzulegen.

Und die «neuen Technologien»? Nach der geltenden IDV können «neue Technologien» zu einem hohen Risiko führen (bisher § 2 Abs. 1 lit. c IDV). Es blieb aber bislang meist unklar, was neue Technologien sind. Was ist neu? Was gerade erfunden wurde? Eine Technologie, die im Kanton zum ersten Mal verwendet wird (welche Projektleitung bzw. welches verantwortliche öffentliche Organ weiss das schon)? Ein Technologiewechsel bei der Erfüllung einer gesetzlichen Aufgabe?

Liste der/des DSB nach § 13 Abs. 2 revIDG

Liste der vorabkonsultationspflichtigen Bearbeitungsvorgänge Deshalb hat der Regierungsrat im IDG-Revisions-Ratschlag beantragt, in § 13 Abs. 2 revIDG die/den DSB zu verpflichten, als Ersatz für diese «neuen Technologien» eine Liste der Bearbeitungsvorgänge zu erstellen, die zur Vorabkonsultation zu unterbreiten sind. Nach der Richtlinie (EU) 2016/68049, so schreibt der Regierungsrat im Ratschlag[3], sei vorzusehen, dass die/der DSB eine Liste der >

Verarbeitungsvorgänge erstellen könne, die der Pflicht zur Vorabkonsultation nach § 13 Abs. 1 revIDG unterliegen. Eine solche Liste – im Sinne einer Positiv- und/oder Negativliste – erleichtere dem verantwortlichen öffentlichen Organ den Entscheid, ob ein Vorhaben der/dem DSB zur Vorabkonsultation vorzulegen ist oder nicht, weshalb der/die DSB verpflichtet wird, eine solche zu erstellen. Der DSB favorisierte eine Kann-Bestimmung, die JSSK wollte aber an der Verpflichtung nichts ändern.[4]

Für die Verwendung von Analysetools, die Personendaten unanonymisiert an Anbieter:innen senden (wie z.B. bei Google Analytics, bei der Verwendung von Google Fonts oder Meta Pixel o.ä.), fehlt den öffentlichen Organen die gesetzliche Grundlage.

Entwurf der Liste Im Hinblick auf das Inkrafttreten des revIDG hat der DSB einen Entwurf für die Liste ausgearbeitet. Nach dem aktuellen Stand sollen folgende Bearbeitungen vorabkonsultationspflichtig sein:

— eine *automatisierte Einzelentscheidung*;

— eine *systematische Übermittlung von Personendaten*, die eine *technische Überwachung* ermöglicht, ausser wenn die Personendaten vor der Übermittlung anonymisiert werden, wenn vor der Übermittlung eine informierte Einwilligung der Betroffenen eingeholt wird und die Erteilung der Einwilligung ohne wesentliche Einschränkung der Funktionalität der angebotenen Dienstleistung verweigert werden kann;

— eine *Bearbeitung von Personendaten mit künstlicher Intelligenz*, ohne dass sichergestellt ist, dass Personendaten ausschliesslich lokal (on-prem) bearbeitet und nicht an Dritte übermittelt werden;

— *Basisdienste*, bei denen nicht ausgeschlossen werden kann, dass (direkt oder indirekt) besondere Personendaten bearbeitet werden.

Zweck Mit den vier aktuell vorgesehenen Datenbearbeitungen soll Folgendes erreicht werden können:

— *Automatisierte Einzelentscheidung:* Es besteht ein hohes Risiko für die Grundrechte der betroffenen Personen, wenn Maschinen ohne Zutun von Menschen entscheiden. In der JSSK-Beratung wurde gefordert, dass die/der DSB solche Vorhaben kritisch prüft. Das soll geschehen, indem solche Vorhaben zur Vorabkonsultation (VAK) vorgelegt werden müssen.

— *Systematische Übermittlung von Personendaten,* die eine *technische Überwachung* ermöglichen: Für die Verwendung von Analysetools, die Personendaten unanonymisiert an Anbieter:innen senden (wie z.B. bei Google Analytics, bei der Verwendung von Google Fonts oder Meta Pixel o.ä.), fehlt den öffentlichen Organen die gesetzliche Grundlage. Darum müssen Vorhaben, die solche Tools nutzen, zur VAK vorgelegt werden.

— *Bearbeitung von Personendaten mit künstlicher Intelligenz:* Auch solche Bearbeitungen können ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen. Auch wenn der Begriff der «künstlichen Intelligenz» noch kaum klar definiert ist, sollen solche Vorhaben – wie in der JSSK-Beratung gefordert – von der/dem DSB näher geprüft werden. Die Ausnahme («wenn sichergestellt ist, dass Personendaten ausschliesslich lokal (on-prem) bearbeitet und nicht an Dritte übermittelt werden») berücksichtigt Erkenntnisse, die der DSB bei konkreten Projekten bereits gewonnen hat.

— *Basisdienste:* Dieses Kriterium betrifft vor allem IT BS und die IT der Departemente. Damit soll dafür gesorgt werden, dass Basisdienste (und vor allem auch potenzielle Basisdienste) rechtzeitig zur VAK vorgelegt werden und nicht von jedem öffentlichen Organ, das sie nutzen will, einzeln vorgelegt werden müssen.

Aktualisierungen folgen Mit der Liste nach § 13 Abs. 2 revIDG soll rechtzeitig der Blick auf heikle Entwicklungen gerichtet werden. Es wird damit ermöglicht, dass neue Entwicklungen rasch erfasst werden können (und wenn sich gezeigt hat, dass datenschutzkonforme Lösungen einfach möglich sind, auch rasch wieder von der Liste gestrichen werden können). Aus diesem Grund wird diese Liste regelmässig aktuell gehalten werden müssen – z.B. wenn «künstliche Intelligenz» klarere Konturen bekommen hat oder wenn sich zeigt, dass auch bei einer *on-prem*-Bearbeitung die Grundrechte der Betroffenen gefährdet sind. Die Liste wird auf der Webseite der/des DSB veröffentlicht werden.

Schwellwertanalyse

Fragebogen und Anleitung Ob bei einem Vorhaben der Schwellwert, der dazu führt, dass eine DSFA durchgeführt werden muss, erreicht wird, ob also einer (oder mehrere) der Risikofaktoren vorliegt, soll ohne grossen Aufwand mit einer Schwellwertanalyse (SWA) eruiert werden können. Der DSB hat im Hinblick auf das Inkrafttreten des revIDG ein entsprechendes *Formular* ausgearbeitet. Ausserdem unterstützt eine *Anleitung zur Datenschutz-Folgenabschätzung und Vorabkonsultation* beim Ausfüllen des Fragebogens.

Abschluss und weiteres Vorgehen Was geschieht nach dem Ausfüllen des SWA-Fragebogens?

— Wenn bei der SWA die Aussage in der *Vorfrage zutrifft*, wenn also mit der projektierten Anwendung gar keine Personendaten bearbeitet werden sollen, dann muss *keine DSFA* vorgenommen werden. Das ausgefüllte Formular ist im Sinne einer Qualitätskontrolle von der/dem zuständigen Datenschutzberater:in (DSBer) zu prüfen, was per Unterschrift zu bestätigen ist, und dann von der Leitung des verantwortlichen öffentlichen Organs zu unterzeichnen, mit der Projektdokumentation abzulegen und auf Verlangen der/dem DSB vorzulegen.

— Wenn bei der SWA *sowohl die Vorfrage wie auch alle Fragen zu den Risikofaktoren verneint* werden (bzw. bei der Frage 1 «Das Abrufverfahren besteht einzig in einem Datenmarkt-Online-Zugriff»), dann muss *keine DSFA* vorgenommen werden. Mit dem Vorhaben sind in eigener Verantwortung die Grundschutzmassnahmen (und allenfalls weitere Schutzmassnahmen, die sich aus anderen als Datenschutz-Gründen ergeben) umzusetzen. Das ausgefüllte Formular ist im Sinne einer Qualitätskontrolle von der/dem zuständigen DSBer zu prüfen, was per Unterschrift zu bestätigen ist, und dann von der Leitung des verantwortlichen öffentlichen Organs zu unterzeichnen, mit der Projektdokumentation abzulegen und auf Verlangen der/dem DSB vorzulegen.

— Wenn aber bei der SWA die *Vorfrage* verneint wird, die *Aussage bei einer oder mehreren der Fragen zu den Risikofaktoren* jedoch *zutrifft*, dann ist eine DSFA nach § 12a revIDG vorzunehmen, wobei alle in der SWA erkannten Risikofaktoren zu behandeln sind. Die dabei zu erarbeitenden Unterlagen sind anschliessend zeitnah der/dem DSB zur VAK nach § 13 Abs. 1 lit. b revIDG vorzulegen.

Die Leitung des verantwortlichen öffentlichen Organs muss schliesslich die Massnahmen abnehmen, das verbleibende Nettorisiko (Restrisiko) übernehmen oder, falls sie das Restrisiko als untragbar erachtet, auf das Vorhaben verzichten.

Datenschutz-Folgenabschätzung (DSFA)

Durchführung der DSFA Die DSFA als Risikoanalyse dient dazu, die datenschutzrelevanten Risiken zu eruieren, zu bewerten und in der Folge die notwendigen technischen, organisatorischen und/oder rechtlichen Schutzmassnahmen festzulegen, mit denen die datenschutzrelevanten Risiken vermieden oder auf ein tragbares Mass reduziert werden. Diese Risikoanalyse ist wichtig für das verantwortliche öffentliche Organ: Deren Leitung muss schliesslich die Massnahmen abnehmen, das verbleibende Nettorisiko (Restrisiko) übernehmen oder, falls sie das Restrisiko als untragbar erachtet, auf das Vorhaben verzichten. Voraussetzung für eine DSFA sind eine geeignete Projektbeschreibung und das Vorliegen einer Rechtsgrundlagenanalyse.

Projektbeschreibung Hier ist das geplante Vorhaben verständlich zu beschreiben. Eine Zusammenfassung (z.B. «Ablösung der Geschäftsverwaltungs-Software») reicht dazu nicht aus. Auf der anderen Seite ist es auch nicht hilfreich, seitenweise Marketingbeschreibungen aus der Werbung der Anbieterin zu zitieren. Das Vorhaben muss in seinem wesentlichen Inhalt für die Verantwortlichen verständlich beschrieben werden, die in der Regel keine Spezialist:innen für beispielsweise IT sind. Für diese Beschreibung sind allenfalls diejenigen Stellen beizuziehen, die hinreichend vertiefte Kenntnis haben von den Datenbearbeitungen im geplanten Vorhaben. Damit aus Datenschutzsicht eine Beurteilung vorgenommen werden kann, ist es unerlässlich, dass die Datenbearbeitungen beschrieben werden. Relevant sein können z.B. die folgenden Aspekte:

— Welche (Kategorien von) *Personendaten* (oder Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) werden zu welchem *Zweck* durch *wen* (durch das öffentliche Organ oder in seinem Auftrag durch Auftragsdatenbearbeiter:innen) bearbeitet?

— Bei wem bzw. aus welchem anderen System werden die Daten *erhoben*, und wem werden die Daten in welcher Form (identifizierend, pseudonymisiert, anonymisiert) und zu welchem Zweck *bekannt gegeben?*

— Bei IT-Systemen, insbesondere bei komplexeren, dienen auch Datenflussanalysen, Architekturskizzen und die Beschreibung der Schnittstellen zu Um- und Untersystemen der Beschreibung des Vorhabens.

Darstellung der Rechtslage Hier ist die Rechtslage für das geplante Vorhaben darzustellen. Dazu reicht es nicht, Gesetze oder Verordnungen zu nennen. Es ist damit vielmehr zu belegen, welche Rechtsgrundlagen die *Datenbearbeitungen*, die vorne in der Projektbeschreibung aufgeführt werden, *gesetzmässig und verhältnismässig* erscheinen lassen. Falls noch keine hinreichend bestimmten Rechtsgrundlagen bestehen, sind diese im Rahmen des Projekts allenfalls zu schaffen. Für die Darstellung der Rechtslage sind allenfalls die zuständigen Rechtsabteilungen oder Rechtsdienste beizuziehen. >

Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen Wenn die SWA in einem oder mehreren Bereichen ein hohes Risiko für die Grundrechte der Betroffenen gezeigt hat oder wenn in der Schutzbedarfsanalyse (SCHUBAN) in Bezug auf ein Schutzziel oder auf mehrere Schutzziele (§ 8 Abs. 2 IDG: insb. Vertraulichkeit, Integrität und Verfügbarkeit) ein erhöhter Schutzbedarf festgestellt worden ist, dann ist vom verantwortlichen öffentlichen Organ – mit Fokus auf die erkannten Bereiche bzw. Schutzziele – eine umfassende Risikoabwägung vorzunehmen. Betroffene sind die Personen, über die im Rahmen der projektierten Anwendung Personendaten bearbeitet werden, aber auch die Mitarbeiter:innen, über die Personendaten bearbeitet werden (sog. Randdaten).

Eruierung und Bewertung der Risiken Es sind die Brutto-Risiken für die Grundrechte der Betroffenen zu eruieren und zu bewerten. Wenn die Risiken als hoch beurteilt werden, sind die (technischen, organisatorischen und rechtlichen) Schutzmassnahmen vorzusehen, die das Risiko vermeiden oder auf ein tragbares Mass vermindern.

Massnahmen Die Massnahmen sind den Risiken zuzuordnen: Mit welcher Massnahme soll welches Risiko vermieden oder vermindert werden? Ein Risiko kann durch mehrere Massnahmen angesprochen werden, und Massnahmen können verschiedene Risiken ansprechen. Massnahmen können ein Risiko in Bezug auf die Eintretenswahrscheinlichkeit und/oder das Schadensausmass beeinflussen.

Brutto- und Netto-Risiko Die Risiken werden beurteilt nach der *Eintretenswahrscheinlichkeit* und der *Schadensschwere*. Sie sind in einer *Risiko-Matrix* einzutragen, einmal in einer *Matrix mit den Brutto-Risiken* und einmal in einer *Matrix mit den Netto-Risiken*. Dabei sollen die Veränderungen durch Schutzmassnahmen erkennbar gemacht werden.

Übernahme des Netto-Risikos Das verbleibende Netto-Risiko (das Brutto-Risiko minus die Verkleinerung des Risikos durch die Schutzmassnahmen) ist von der verantwortlichen Stelle (der Leitung des öffentlichen Organs, das mit dem geplanten Vorhaben eine gesetzliche Aufgabe erfüllt, also der Dateneignerin nach § 6 IDG) zu übernehmen – oder es ist, wenn das Nettorisiko als nicht tragbar angesehen wird, auf das Vorhaben zu verzichten.

Vorabkonsultation (VAK)

Vorabkonsultation Ein Vorhaben, bei dem wegen des hohen Bruttorisikos für die Grundrechte der betroffenen Personen eine DSFA durchzuführen ist, muss *immer* auch der/dem DSB vorgelegt werden.[5] Diese/dieser hat zu beurteilen, ob – wenn die vorgesehenen Massnahmen umgesetzt werden – ein Vorhaben *datenschutzkonform umsetzbar* ist, oder zu empfehlen, dass (und allenfalls welche) weitere(n) Massnahme(n) zu ergreifen sind, damit ein Vorhaben datenschutzkonform umsetzbar ist (§ 46 IDG).

Dokumentation Zur VAK ist der/dem DSB die Dokumentation einzureichen, die im Rahmen der DSFA erstellt worden ist. Es ist möglich (und sinnvoll), die Informationen zusammenzufassen in einem Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept). In anderen Kantonen[6] sind standardmässig die ISDS-Konzepte zur VAK vorzulegen. Im ISDS-Konzept sind auch Verweise auf spezifische Teilkonzepte möglich.

Inhalt eines ISDS-Konzepts Ein ISDS-Konzept muss (aus Datenschutzsicht) folgenden Mindestinhalt aufweisen:

— eine Beschreibung des Vorhabens;
— die Darstellung der Rechtslage;
— ein Rollen- und Berechtigungskonzept;
— eine Regelung der Protokollierung (und ggf. der Auswertung der Logfiles);
— ein Backup- und Restore-Konzept;
— ein Aufbewahrungs-, Archivierungs- und Löschungskonzept;
— die Gewährleistung der Datenschutzrechte der betroffenen Personen;[7]
— spezifische Konzepte, falls Auftragsdatenbearbeiter:innen beigezogen oder gar Cloud-Dienste genutzt werden.

Informationssicherheit Datenschutzrechtlich von Bedeutung sind auch die Vorkehrungen der Informationssicherheit. Zu einem ISDS-Konzept gehören sicher Aussagen zu den folgenden Aspekten:

— Beschreibung des Gesamtsystems (inkl. Systemarchitektur und Schnittstellen, Systemgrenzen);
— Datenflüsse (inkl. Beschreibung der zu bearbeitenden Informationen);
— Zugang für Benutzer:innen, Administrator:innen, Dritte;
— Authentisierungs- und Autorisierungsmechanismen;
— Verschlüsselung;
— Software Deployment;
— Viren- und Malwareschutz u.a.m.

Hilfestellung

Anleitung Wie bereits erwähnt, wird die/der DSB für die SWA, die DSFA und die VAK eine ausführliche Anleitung zur Verfügung stellen. Sie richtet sich an Personen, die sich erstmals um diesen Prozess kümmern müssen – wer das Verfahren schon mehrfach durchgeführt hat, braucht diese Ausführlichkeit nicht mehr. Die verantwortlichen öffentlichen Organe können die/den DSB auch beiziehen, um beispielsweise zu klären, wie bei einem konkreten Projekt die Risikofaktoren zu beurteilen sind. Allerdings: Sie/er hat die *Aufsicht* über das Datenbearbeiten der öffentlichen Organe. Vorher sind für Rechtsfragen die zuständigen Rechtsdienste oder Rechtsabteilung beizuziehen und für Fragen der Informationssicherheit die/der ISBD des öffentlichen Organs.

Die Verantwortung für das Projekt, insbesondere auch für die Übernahme des Restrisikos liegt nicht bei den Datenschutzberater:innen, sondern verbleibt bei der Leitung des verantwortlichen öffentlichen Organs.

Aktueller Stand Die Entwürfe der Liste der vorabkonsultationspflichten Datenbearbeitungen nach § 13 Abs. 2 revIDG, des Fragebogens zur Schwellwertanalyse und des Merkblatts für die Datenschutz-Folgenabschätzung und Vorabkonsultation sind anfangs Juli 2024 der Staatskanzlei vorgelegt worden. Wenn aus der Verwaltung Verbesserungsvorschläge kommen, sollen diese selbstverständlich noch berücksichtigt werden. Die durch die neue DSB finalisierten Dokumente werden für die Vorbereitung der Umsetzung der Revisionen von IDG und IDV auf der Webseite der DSB zur Verfügung stehen.

Datenschutzberater:innen

Wichtige Rolle Es sei hier nochmals erwähnt (vgl. dazu vorne S. 11 f.): Die DSBer spielen in der Umsetzung des Datenschutzes in der Verwaltung eine sehr wichtige Rolle. Bei ihnen ist das Datenschutz-Knowhow gebündelt, und sie sollen alle Behörden in ihrem Zuständigkeitsbereich unterstützen können. Sie dienen im Bereich des Datenschutzes der Qualitätssicherung:

— Sie *prüfen* die SWA. Sie sollen dies mit ihrer Unterschrift dokumentieren, so dass die Leitung des verantwortlichen öffentlichen Organs darauf vertrauen darf, dass das Formular korrekt ausgefüllt worden ist;

— sie unterstützen das verantwortliche öffentliche Organ bei der *Durchführung der DSFA*, und

— sie sollen mit ihrer Unterschrift unter die Dokumentation, die der/dem DSB zur VAK eingereicht wird, dokumentieren, dass sie sie geprüft haben.

Qualitätssicherung, nicht Verantwortung für das Projekt Die DSBer müssen prüfen, ob die datenschutzrechtlichen Fragen richtig beantwortet sind (also dass nicht jemand ankreuzt, es würden bloss «gewöhnliche» Personendaten bearbeitet, wenn tatsächlich besondere Personendaten bearbeitet werden sollen). Die *Verantwortung* für das Projekt, insbesondere auch für die *Übernahme des Restrisikos* verbleibt aber bei der *Leitung des verantwortlichen öffentlichen Organs*, also bei der Stelle, die auch entscheiden muss, ob die vorgesehenen Massnahmen angemessen sind (und vielleicht auf teurere, aber aus ihrer Sicht unnötige Massnahmen verzichtet).

Zusammenarbeit mit der/dem DSB Selbstverständlich können die DSBer auch die/den DSB beiziehen (§ 16b Abs. 3 lit. c revIDG). Geplant ist auch, ein Gefäss für den regelmässigen Erfahrungsaustausch zwischen DSBer und DSB zu schaffen.

1 Siehe dazu auch schon die Ausführungen in TB 2022 des DSB/BS, S. 8 ff., und v.a. TB 2020/2021 des DSB/BS, S. 13 ff.
2 Ausnahme: Beschränkt sich das Vorhaben ausschliesslich auf einen Online-Zugang zum kantonalen Datenmarkt (i.S.v. § 5 Abs. 1 lit. a Ziff. 1 DMV), so findet die Vorabkonsultation im Rahmen des Autorisierungs-Workflow-Systems AWS statt.
3 Ratschlag 21.1239.01, S. 26.
4 JSSK-Bericht 21.1239.02, S. 10 f.
5 Anders im Bund: Nach Art. 23 DSG muss eine geplante Bearbeitung dem EDÖB nur dann vorgelegt werden, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung *trotz* der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat.
6 Im Kanton Bern beispielsweise werden die Vorgaben zentral vom Kantonalen Amt für Informatik und Organisation (KAIO) erlassen und wird deren Einhaltung durch die Datenschutzaufsicht (DSA) geprüft, der das ISDS-Konzept vorzulegen ist.
7 Recht auf Zugang zu den eigenen Personendaten (§ 26 IDG), Anspruch auf Berichtigung bzw. Vernichtung unrichtiger Personendaten (§ 27 Abs. 1 lit. a IDG), auf Unterlassung eines widerrechtlichen Bearbeitens (§ 27 Abs. 1 lit. b IDG), auf Beseitigung der Folgen eines widerrechtlichen Bearbeitens, insb. Löschung der Daten oder Bekanntgabesperrung (§ 27 Abs. 1 lit. c revIDG), auf Feststellung der Widerrechtlichkeit (§ 27 Abs. 1 lit. d IDG) samt jeweilige Mitteilung an Personen und Stellen, denen die Daten zuvor bekannt gegeben worden sind (§ 27 Abs. 1ter revIDG), Recht auf Sperrung der Bekanntgabe von Personendaten an Private (§ 28 Abs. 1 lit. IDG).

Thema 3 Weiterhin herausfordernde «Grossbaustellen»

Verschiedene Themen sind in den letzten Tätigkeitsberichten des Datenschutzbeauftragten immer wieder angesprochen worden – und ein paar dieser grossen «Baustellen» bestehen weiterhin. Hier soll ein Blick auf den aktuellen Stand der grössten Pendenzen geworfen werden.

Alles erledigt?

Leider nicht Es wäre ja das Ziel, bei einer Amtsübergabe alles erledigt zu haben. Schön wär's. Aber ein paar Themen bleiben auf der Pendenzenliste.

Keine (IT-)Governance

Überbleibsel der «alten» Governance Basel-Stadt hat nicht gar keine (IT-)Governance. Ein Blick in die Informationssicherheitsverordnung (ISV)[1] zeigt, dass gewisse Rollen und Aufgaben definiert sind. Diese Bestimmungen wurden nicht ausser Kraft gesetzt, als der konzeptionelle Überbau, die IT-Governance, vor dem Departementsvorsteherinnen-Wechsel im Finanzdepartement aufgehoben wurde. Seither fehlt das *übergeordnete Steuerungs- und Regelungssystem.*[2]

Die (IT-)Governance muss vorgeben, mit welcher Führung, in welchen Organisationsstrukturen und mit welchen Prozessen sichergestellt wird, dass die IT die «Unternehmensstrategie» unterstützt.

Steuerung und Verantwortung Eine IT-Strategie legt fest, wie die Informatik die staatliche Aufgabenerfüllung effektiv unterstützen und voranbringen soll. Sie muss begleitet sein von einer *(IT-)Governance*. Diese muss vorgeben, mit welcher *Führung*, in welchen *Organisationsstrukturen* und mit welchen *Prozessen* sichergestellt wird, dass die IT die «Unternehmensstrategie» unterstützt. Im Kern muss die IT-Governance festlegen, wer wofür verantwortlich ist: Welche Stellen oder Gremien, vom Regierungsrat und der regierungsrätlichen IT-Delegation über die Konferenz für Organisation und Informatik (KOI), die Informatik-Leiter:innen-Konferenz (ILK), die IT BS, die/den Chief Information Security Officer (CISO, ISB) bis zu den Departementen, der Departements-IT, den departementalen Informationssicherheitsbeauftragten (ISBD), den Dateneigner:innen, dem Digital Lab usw. sollen welche *Aufgaben, Kompetenzen und Verantwortlichkeiten* erhalten? Wer kann/muss wem Vorgaben machen, wer muss kontrollieren und an wen berichten, ob diese Vorgaben auch umgesetzt werden? Wie sorgt der Regierungsrat dafür, dass er die IT, von der immer grössere und wichtigere Teile der staatlichen Aufgabenerfüllung abhängig sind, steuern und letztlich auch verantworten kann? Insbesondere wenn keine (umfassende) Zentralisierung der IT gewünscht wird, müssen die Abgrenzungen und das Zusammenwirken zwischen den verschiedenen beteiligten Stellen und Gremien möglichst klar geregelt sein. Und was dabei auch nicht vergessen werden darf: Wie wird die Finanzierung geregelt?

Dringende Pendenz Solange dieser konzeptionelle Überbau fehlt, ist die Steuerung und Verantwortungsübernahme bezüglich der IT schwierig. Die einzelnen Stellen können sich noch so Mühe geben, da drohen gefährliche Lücken und verschlingen Überschneidungen Ressourcen. Viele Bereiche warten dringend auf diese grundsätzliche Ordnung der Aufgaben, Kompetenzen und Verantwortlichkeiten. Grosse Vorhaben, z.B. das Programm «Connect 365» (der Gang in die Cloud) oder die verstärkte Nutzung von Künstlicher Intelligenz, sind angewiesen auf eine IT-Governance und ihre Umsetzung. Da sollten auch die Oberaufsichtskommissionen des Grossen Rates ihre Verantwortung mit Nachdruck wahrnehmen.

Beispiel Was eine fehlende (IT-)Governance bewirkt, soll hier an einem Beispiel illustriert werden. Wenn eine Applikation – nach der Werbung eine «Unified Communications-Komplettlösung für Ihre Unternehmens-Kommunikation: intuitive Kommunikation, kompromisslose Mobilität, effizientes Teamwork, höchste Erreichbarkeit, maximale Integration»

– eingeführt werden soll: Wer hat welche Rolle, welche Aufgabe, welche Verantwortung? Führt IT BS diese Lösung für die gesamte Verwaltung ein? Oder führt jedes Departement (oder gar jede einzelnen Dienststelle) dieses Tool ein? Gibt es (zentrale) Vorgaben dazu oder löst das jedes Departement oder jede Dienststelle für sich? Wer definiert die Voreinstellungen? Wer sieht alles, mit wem ich wann und wie lange telefoniert habe? Diese und weitere Fragen stellen sich Mitarbeiter:innen und kommen damit zur/zum DSB. Und da stellt sich die Frage: Hätte diese Anwendung vorher zur Vorabkonsultation vorgelegt werden müssen? Und: von wem? Mit einem übergeordneten Steuerungs- und Regelungssystem, einer (IT-)Governance, müsste klar werden, wer sich um was kümmern muss.

Allein die Einführung von Vorgaben macht das Projektmanagement noch nicht besser. Es braucht dringend auch Projektmanagement-Kompetenz, also Menschen, die geübt sind im Führen von Projekten.

Projektmanagement – Projektmanagement-Kompetenz

Festlegen und umsetzen Es tut sich was in Sachen Verbesserung des Projektmanagement.[3] Der Projektleitfaden ist angepasst worden und auch die für den präventiven Datenschutz relevanten Elemente (Projektbeschreibung, Rechtsgrundlagenanalyse, Datenschutz-Folgenabschätzung und Vorabkonsultation – vgl. dazu vorne S. 15 ff.) sollen eingebaut werden, sobald das revIDG in Kraft tritt. Jetzt müssen diese Projektmanagement-Vorgaben auch noch umgesetzt werden. Während in anderen Kantonen (z.B. im Kanton Basel-Landschaft) ein Vorgehen, das die Projektmanagement-Vorgaben nicht einhält, zurückgewiesen wird, war in unserem Kanton bis vor kurzem die Einhaltung der Vorgaben sozusagen freiwillig, auf jeden Fall ohne schmerzende Konsequenzen. Das führt auch dazu, dass die/der DSB zu oft Ressourcen zur Unterstützung des Projektmanagements einsetzen muss, statt die fertigen Unterlagen für die Vorabkonsultation prüfen zu können.

Projektmanagement-Kompetenz Doch die Einführung von Vorgaben allein macht das Projektmanagement noch nicht besser. Es braucht dringend auch Projektmanagement-Kompetenz, also Menschen, die geübt sind im Führen von Projekten. Das können Interne oder Externe sein. Ein möglicher Lösungsansatz könnte darin bestehen, dass für Projekte ab einer bestimmten Grösse (zentral oder departementsweise) Projektmanagements-Spezialist:innen zur Verfügung gestellt werden (oder noch besser: «gebucht» werden müssen). Sie brauchen keine fundierten Fachkenntnisse. Sie müssen also, um z.B. ein Projekt der Sozialhilfe oder des Migrationsamtes leiten zu können, nicht aus der Sozialhilfe oder dem Migrationsbereich kommen, aber Projektleitungs-Kompetenz mitbringen. Sie müssen keine Rechtsgrundlagenanalyse vornehmen oder ein fachliches Pflichtenheft verfassen können, aber wissen, wo sie diese herbekommen.

Kosten sparen Es dürfte sich lohnen, eine solche Lösung in Betracht zu ziehen. Wenn ein grösseres Vorhaben auch nur schon beim Go-Live nicht kompetent geführt wird, drohen nicht nur höhere Kosten, sondern auch ein Scheitern eines Projektes.[4] Ein kompetentes und straffes Projektmanagement hilft, unnötige Kosten zu sparen.

Cybersicherheit

Steigende Risiken Immer mehr ist die staatliche Aufgabenerfüllung nicht nur abhängig von der IT. Die Systeme, Netzwerke und Programme waren schon bisher und sind nun zunehmend digitalen Angriffen ausgesetzt. Mit Cyberangriffen wird versucht, auf vertrauliche Informationen zuzugreifen, sie zu ändern oder zu vernichten, Geld zu erpressen oder schlicht die normalen Geschäftsabläufe zu stören. Staatliche Daten sind (zusammen mit Gesundheitsdaten) weit oben in der Rangliste der beliebten und lohnenden Angriffsziele, und die Angriffe werden immer gewiefter und innovativer. Da sollten wir es den Angreifern nicht auch noch leicht machen.

Umfassende Sicherheitsorganisation Eine hundertprozentige Sicherheit gibt es auch im Cyberraum nicht – oder wohl besser: Die gibt es im Cyberraum erst recht nicht. Aber Kanton, Gemeinden und die öffentlichen Unternehmen müssen sich wohl oder übel wappnen. Es ist nicht eine Massnahme – es braucht ein ganzes Bündel an Massnahmen. Ein Security Operations Center (SOC) ist eine (zentrale) Massnahme, um Angriffe zu erkennen und auf sie reagieren zu können. Es braucht aber viel mehr – hier nur eine kleine Auswahl:

— organisatorische Massnahmen wie z.B. die Klassifizierung von Informationen (und die Regelung des Zugangs zu klassifizierten Informationen), >

— technische Massnahmen wie die Definition von Sicherheitsverfahren und von Sicherheitsstufen für ICT-Mittel;

— physische Massnahmen wie Sicherheitszonen;

— personelle Massnahmen wie Personensicherheitsprüfungen und

— den Aufbau einer Sicherheitsorganisation.

Kantonales Informations- und Cybersicherheitsgesetz?

Reicht die ISV? Ob es reicht, dafür die Informationssicherheitsverordnung anzupassen, kann bezweifelt werden. Der Regierungsrat und der Grosse Rat sollten unbedingt prüfen, ob es zur Durchsetzung der einschneidenden Massnahmen – zum Beispiel die Sicherheitsprüfungen für Personen, die im Rahmen ihrer Funktion Zugang zu sicherheitsrelevanten Informationen haben – nicht wie im Bund[5] oder im Kanton Bern[6] ein Gesetz bräuchte. Wichtig ist auf jeden Fall, dass wegen der fatalen Abhängigkeit von der Vernetzung die Bedeutung der Sicherheit erhöht wird. Dabei ist nicht nur der Regierungsrat in der Pflicht – auch der Grosse Rat muss seinen Teil der Verantwortung übernehmen und die Oberaufsicht auch in diesem Bereich wirksam wahrnehmen.

Sichere Kommunikation

Postkarten? Gerne, aber nicht mit (besonderen) Personendaten Eine weitere Baustelle besteht nun seit Jahren im Bereich der «sicheren Kommunikation». E-Mail hat der Briefpost schon lange den Rang abgelaufen, Fax ist verschwunden, telefoniert wird immer noch, es ist jedoch ein anderes Netz und andere Technik. Seit der Pandemie nicht mehr wegzudenken ist der Videocall. Es gibt kaum eine staatliche Aufgabenerfüllung, in der die Kommunikation, teils mit sehr heiklen Daten, keine tragende Rolle spielt. Die sichere Kommunikation stellt jedoch seit Jahren ein Thema dar und ist im Detail auch ein eher schwer zu erfassendes Problem.

Zentrale Lösung fehlt Eine zentrale Lösung für eine sichere Übermittlung von Personendaten und insbesondere auch von besonderen Personendaten fehlt bis heute. Es kann nicht sein, dass die einzelnen Dienststellen sich um die Verschlüsselung kümmern müssen. Für die sichere digitale Übermittlung sollte ein Set von möglichen Lösungen (verschlüsselte E-Mails, Downloadportale oder Filesharing-Plattformen) bereitstehen und unkompliziert genutzt werden können – nicht nur für die Kommunikation der öffentlichen Organe untereinander, sondern auch von und zu den Einwohner:innen.

Für die sichere digitale Übermittlung sollte ein Set von möglichen Lösungen bereitstehen und unkompliziert genutzt werden können – nicht nur für die Kommunikation der öffentlichen Organe untereinander, sondern auch von und zu den Einwohner:innen.

Digitale Souveränität

Abhängigkeit Ein fünfter Punkt betrifft die «digitale Souveränität». Kanton und Gemeinde müssen sich bewusst sein, dass sie sich in eine sehr grosse Abhängigkeit begeben, wenn sie «alles» über einen (Quasi-)Monopolisten beziehen. Das betrifft nicht nur finanzielle Aspekte, sondern auch die Schwierigkeit, wieder auszusteigen, wenn das Angebot von der Leistung, vom Preis oder von den Vertragsbestimmungen (z.B. in Bezug auf den Datenschutz) her einmal nicht mehr stimmen sollte. Das betrifft aber zugegebenermassen nicht nur den Kanton oder die Gemeinden, sondern generell den Staat und die Wirtschaft in Europa. Aber auch hinter diesem «die anderen auch» sollten sich die öffentlichen Organe nicht verstecken, sondern aktiv an Strategien arbeiten, diese Abhängigkeiten so weit möglich zu verringern. So hat beispielsweise der Bundesrat beschlossen, dass mittel- bis langfristig die Abhängigkeit von Office-Produkten des Herstellers Microsoft reduziert werden soll.[7]

1 §§ 4–10 ISV. Die ISV wird nicht im Zusammenhang mit der IDG-Revision angepasst. Sie wird erst im Rahmen der Umsetzung der neuen (IT-)Governance revidiert werden können.

2 Vgl. die Ausführungen zur (fehlenden) IT-Governance in früheren Tätigkeitsberichten: TB 2022 des DSB/BS, S. 22 f.; TB 2017-2019 des DSB/BS, S. 31 f.

3 Vgl. die Ausführungen zum Projektmanagement in früheren Tätigkeitsberichten: TB 2022 des DSB/BS, S. 23; TB 2020-2021 des DSB/BS, S. 17 ff.

4 Vgl. als Illustration für dieses Risiko den Bericht von PwC: 2024 – Externe Evaluation zum Projekt citysoftnet, 2. Mai 2024 (<https://www.bern.ch/mediencenter/medienmitteilungen/aktuell_ptk/citysoftnet-stadt-will-erkenntnisse-aus-bericht-umsetzen/dokument/bericht-citysoftnet-2024-2013-externe-evaluation.pdf/download>), und die dazugehörende Medienmitteilung des Gemeinderats der Stadt Bern (<https://www.bern.ch/mediencenter/medienmitteilungen/aktuell_ptk/citysoftnet-stadt-will-erkenntnisse-aus-bericht-umsetzen/dokument/bericht-citysoftnet-2024-2013-externe-evaluation.pdf/download>).

5 Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), SR 128.

6 Im Kanton Bern das ein Informations- und Cybersicherheitsgesetz beim Grossen Rat in Beratung: Siehe die Medienmitteilung des Regierungsrates des Kantons Bern vom 17. August 2023: Gesetz über die Informations- und Cybersicherheit geht an den Grossen Rat (<https://www.be.ch/de/start/dienstleistungen/medien/medienmitteilungen.html?newsID=7add8317-b2a0-4d52-8a38-8c7689430ff7>).

7 Vgl. die Medienmitteilung des Bundesrates vom 22. April 2024: Migration auf Microsoft 365: Einführung bei den ersten Verwaltungseinheiten (<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-100118.html>) mit Verweis auf die Medienmitteilung des Bundesrates vom 15. Februar 2022: Bund führt Microsoft 365 ein (<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-93076.html>).

Jahresrückblick

2023:
Blick auf die wichtigsten Geschäfte

Statistik

Jahresrückblick

2023: Blick auf die wichtigsten Geschäfte

Was hat das Team des Datenschutzbeauftragten im vergangenen Jahr gemacht? Mit welchen Fragen wurde es konfrontiert? Und welche Defizite hat es aufgedeckt? Wo Verbesserungen erreicht? Eine kurze Tour d'Horizon durch ein Jahr Beratung und Kontrolle.

Beratungstätigkeit

Querschnittsthema Die Beratungstätigkeit bindet etwa drei Viertel der Ressourcen der/des DSB. Thematisch wurde auch im vergangenen Jahr die gesamte Breite der Staatstätigkeit erfasst. Nur exemplarisch seien hier einige Themen kurz erwähnt:

— *Stellungnahmen in Rechtsetzungsverfahren*[1] sowohl auf kantonaler als auch (z.T. im Rahmen von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten) auf Bundesebene, so u.a. zu Teilrevisionen des kantonalen Gesundheitsgesetzes (GesG), des Hundegesetzes, des Epidemiengesetzes des Bundes (EpG), zu mehreren Schengen-Weiterentwicklungen u.a.m.

— *Vorabkonsultationen*[2] (nach dem geltenden IDG noch: Vorabkontrollen) zu 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, so etwa zu Projekten der Pensionskasse Basel-Stadt (PKBS), zum New Generation Identity and Access Management System (NGI) der Universität Basel, zu einem Pilotversuch der Post mit dem Einwohneramt Basel zur Digitalisierung der Wohnsitzbescheinigung usw.

— Vorabkonsultationen bei der Einrichtung, Ausweitung oder Verlängerung von *Videoüberwachungen*,[3] so u.a. beim Gesundheitsdepartement, beim Strafgericht, beim Institut für Rechtsmedizin, bei den iwb und – in der Öffentlichkeit stark beachtet – die Videoüberwachung der Kantonspolizei auf dem Dreirosen-Areal.

— Stellungnahmen im Zusammenhang mit dem Recht auf Zugang zu den eigenen Personendaten und mit dem allgemeinen Informationszugangsrecht (Öffentlichkeitsprinzip), zum Beispiel zuhanden der Staatsanwaltschaft und zuhanden von Medienschaffenden, etwa zu E-Mails im Präsidialdepartement betreffend den Nahostkonflikt.

— Beratungen im Zusammenhang mit Meldungen von Datenschutzverletzungen (noch nicht gestützt auf die neu zu schaffende Meldepflicht bei Datenschutzverletzungen (*Data breach notifications*)[4], sondern auf den Grundsatz von Treu und Glauben), zum Beispiel im Winter 2022/2023 beim Angriff einer Hackergruppe auf eine Datenplattform des Erziehungsdepartements («ED-Hack») (zur entsprechenden Datenschutzprüfung hinten S. 31 unter «Kontrolltätigkeit»).

Der DSB hat wiederholt den Vorschlag gemacht, dass sich der Kanton einheitliche Vertragsvorlagen gibt. Er hat der Konferenz der Rechtsdienste vorgeschlagen, ein solches Projekt zu starten, statt dass jedes Departement oder jeder Rechtsdienst für sich allein etwas entwickelt.

Vertragsmanagement

Ausgangslage Immer wieder werden der/dem DSB einzelne Entwürfe zu Verträgen oder Vertragsbestandteilen zur Stellungnahme unterbreitet. Gerade im Zusammenhang mit Auftragsdatenbearbeitungen haben Dienststellen solche Texte entworfen: mehr oder weniger vollständig, oft mehr oder weniger gut kopiert von deutschen Vorbildern – einfach daran zu erkennen, dass auf die DSGVO der EU verwiesen wird statt auf das IDG.

Geheimnisschutz oder Datenschutz? Dabei ging es inhaltlich nur zum Teil um Datenschutz, also um den Schutz der Daten über (künftig ausschliesslich natürliche[5]) Personen, also über die Kantonseinwohner:innen oder Verwaltungsmitarbeiter:innen. Wenn bei einem Beschaffungsvertrag Details aus der Offerte (auf Seiten der beauftragten Privaten) oder Informationen über die staatliche Auftraggeberin geheim gehalten werden sollen, dann steht nicht der Datenschutz im Vordergrund, sondern der Schutz von (Geschäfts-)

Geheimnissen. Diese Vertragsbestimmungen sind nicht von der/dem DSB zu begutachten, sondern von den jeweiligen Rechtsdiensten.

Ansatz Der DSB hat wiederholt den Vorschlag gemacht, dass sich der Kanton einheitliche Vertragsvorlagen gibt. Er hat der Konferenz der Rechtsdienste vorgeschlagen, ein solches Projekt zu starten, statt dass jedes Departement oder jeder Rechtsdienst für sich allein etwas entwickelt. Denkbar wäre eine Lösung wie im Kanton Zürich, der schon seit rund 20 Jahren eigene «*Allgemeine Geschäfts-Bedingungen» (AGB)* vorgibt, oder dass der Kanton vorschreibt, dass die AGB der Schweizerischen Informatikkonferenz SIK verwendet werden und für die verschiedenen Konstellationen zusätzlich *einzelne Musterverträge* oder einzelne Vertragsteile, etwa Datenschutz- oder Geheimhaltungsvereinbarungen oder -klauseln, ausarbeitet. Aber nicht die/der DSB kann solche Vorlagen erstellen, weil die nötigen Informationen, für welche Konstellationen solche Vorlagen zu erstellen sind, nicht bei ihr/ihm, sondern nur bei den Dienststellen oder Departementen vorhanden sind.

Konzept für vertragliche Regelungen Ausserdem empfehlen wir bei grösseren Projekten dringend, ein Vertragskonzept zu erstellen: Was soll/muss wann mit wem in welchem Vertrag geregelt werden? Das bedingt (ebenfalls), die Rechtsdienste oder -abteilungen rechtzeitig beizuziehen.

Kantonaler Datenmarkt (KDM)

Bei genauerem Hinschauen Es hat sich bei genauerem Hinschauen durch das Datenmarkt-Team von IT BS in Zusammenarbeit mit dem DSB gezeigt, dass die «Altlasten» im KDM noch grösser sind als bisher angenommen.[6] Es gibt eine sehr grosse Zahl von Mitarbeiter:innen aus der Verwaltung, die Zugriff auf die sog. «Personenauskunft» (alle Personen im Datenmarkt) haben, ohne dass sich dafür Autorisierungen finden lassen bzw. auffindbare Autorisierungen längst abgelaufen sind. Es hat sich ausserdem gezeigt, dass bei einer grossen Zahl von Einwohner:innen aus früheren Zeiten Angaben zur Konfession erfasst sind, die vom Staat gar nicht erfasst werden dürfen.

Konfession Erlaubt ist nach dem Registerharmonisierungsgesetz des Bundes die Erfassung der «*Zugehörigkeit zu einer öffentlich-rechtlich oder auf andere Weise vom Kanton anerkannten Religionsgemeinschaft*» (Art. 6 lit. l RHG). Öffentlich-rechtlich anerkannt sind in Basel-Stadt die vier in der Kantonsverfassung (§ 126 Abs. 1 KV) erwähnten Religionsgemeinschaften[7] sowie die (aktuell ebenfalls) vier vom Grossen Rat gestützt auf § 133 KV anerkannten Kirchen und Religionsgemeinschaften (sog. «kleine Anerkennung»)[8]. Für die Erfassung anderer Angaben zur Konfession existiert in unserem Kanton keine Rechtsgrundlage.

Aufräumen (1) Nun hat sich aber gezeigt, dass bei noch über 50 000 Personen, die im Datenmarkt erfasst sind,[9] *andere Eintragungen* existieren.[10] Sie stammen teilweise aus früheren Einwohnerkontrollsystemen. Der DSB hat die dringende Empfehlung abgegeben, die unzulässigen Eintragungen zu entfernen. IT BS arbeitet an der Umsetzung dieser Empfehlung. Es haben sich in diesem Zusammenhang weitere Fragen gestellt, z.B. ob alle Empfänger:innen des Attributs «Konfession» dieses zu Recht beziehen.

Bis bei den Datenmarkt-«Aufräumarbeiten» die weit über 200 zu prüfenden Autorisierungen inkl. der laufend wieder anfallenden Autorisierungen bearbeitet und verbessert sind, wird es mehrere Jahre dauern.

Aufräumen (2) Auch die andere vorne erwähnte «Altlast», die abgelaufenen, nicht dokumentierten oder inexistenten Autorisierungen für laufende Onlinezugangsrechte im Datenmarkt, wird zurzeit bereinigt. Nach und nach werden alle Bezugsrechte im elektronischen System (KDM Renova) erfasst. Undokumentierte Berechtigungen werden abgeschaltet, oder es wird das Autorisierungsverfahren nachgeholt. Bis diese weit über 200 zu prüfenden Autorisierungen inkl. der laufend wieder anfallenden Autorisierungen bearbeitet und verbessert sind, wird es mehrere Jahre dauern. Der DSB hat dem mehrere Jahre dauernden «Aufräum-Projekt» zugestimmt, weil damit unnötige sich über Jahre fortsetzende Wellen an zu bearbeitenden Gesuchen vermieden werden können.

Kurzer Prozess? Könnten nicht einfach alle Zugriffsmöglichkeiten, die nicht mehr auf gültigen Autorisierungen basieren, gesperrt werden? Damit würde ein unrechtmässiger Zustand kurzerhand beseitigt. Doch weil etliche Dienststellen für die Erfüllung ihrer

>

gesetzlichen Aufgaben Daten aus dem Datenmarkt benötigen (und ihr Autorisierungsgesuch auch bewilligt werden könnte), können diese Zugriffsberechtigungen verständlicherweise nicht von einem Tag auf den anderen gesperrt werden.

Verantwortung Nach § 3 DMV trägt die Konferenz für Organisation und Informatik (KOI) als Vertreterin der dateneinliefernden Organe die *Gesamtverantwortung* für den kantonalen Datenmarkt. Fast mustergültig sind in § 3 Abs. 3 DMV ihre Aufgaben aufgelistet.[11] Doch kann die KOI, als Kollektiv, so wie es zusammengesetzt ist, diese Gesamtverantwortung tragen?

— *Festlegung der Anforderungen*, welche das Gesamtsystem erfüllen muss, und Sicherstellung der Einhaltung dieser Anforderungen (lit. a): Dazu würde auch die Kontrolle gehören, ob nur autorisierte Zugriffsrechte bestehen.

— Sicherstellung des Verfahrens zur *Vernichtung von Daten* (lit. c): Die Daten von längst Verstorbenen und längst Weggezogenen sind immer noch im Datenmarkt verfügbar.

— Sicherstellung der *Gewährleistung der Rechte der betroffenen Personen* (lit. f): Die Person, bei der als Konfession unrechtmässig (und ausserdem unzutreffenderweise) Muslim eingetragen war, musste ihre Rechte über den DSB geltend machen.

— *Sicherstellung der Einhaltung der Rechte und Pflichten* der Dateneigner:innen (lit. j): Es wird nicht aktiv kontrolliert, ob Daten rechtmässig eingeliefert werden[12] (oder wie die vorne erwähnten Eintragungen beim Attribut «Konfession» trotz fehlender Rechtsgrundlage immer noch im KDM zum Download vorgehalten werden).

Die Person, bei der als Konfession unrechtmässig (und ausserdem unzutreffenderweise) Muslim eingetragen war, musste ihre Rechte über den DSB geltend machen.

Achtung Pulverfass Um den Datenmarkt wird Basel-Stadt ab und zu benieden. Damit wird gleichsam das eGovernment-Prinzip «Once only» schon umgesetzt, das in vielen anderen Verwaltungen erst ein Zukunftsprojekt ist. Wenn aber der Datenmarkt nicht regelkonform beherrscht wird, dann ist das ein *Pulverfass für die künftige Digitalisierung*. Es gilt, das eGovernment-Prinzip «Once only» rechtzeitig um wichtige Datenschutzprinzipien wie z.B. die Datensparsamkeit zu ergänzen, so dass auch die Verhältnismässigkeit berücksichtigt ist. Es wird notwendig sein, ein Lösch- und Archivierungskonzept zu entwickeln und umzusetzen. Der DSB unterstützt die laufenden Aufräumarbeiten mit recht grossem Ressourceneinsatz.

Der Gang in die Cloud (M365)

Verschiedene Vorhaben Viele öffentliche Organe drängen in die Cloud,[13] nicht nur die Kantonsverwaltung als Ganzes, auch die Schulen und verschiedene selbständige öffentlich-rechtliche Anstalten. Stark beschäftigt haben den DSB im vergangenen Jahr (und sie tun es auch im Jahr 2024 noch) die Vorhaben von IT BS für die Kantonsverwaltung und vom Erziehungsdepartement (ED) für die Schule (für Unterrichtszwecke, nicht für die Schulverwaltung, den Schulpsychologischen Dienst usw.).

Die Kantonsverwaltung plant, M365 von Microsoft für alle Daten ausser für jene mit einem sehr hohen Schutzbedarf zu nutzen. Damit ist mehr geplant als im Bund und in verschiedenen anderen Kantonen.

Unterschiede Diese beiden Vorhaben unterscheiden sich vor allem dadurch, für welche Daten M365 von Microsoft genutzt werden dürfen soll:

— *Die Kantonsverwaltung* plant, M365 von Microsoft für alle Daten ausser für jene mit einem sehr hohen Schutzbedarf zu nutzen. Genutzt werden darf M365 also auch für Daten mit einem bloss erhöhten (nicht sehr hohen) Schutzbedarf. Darunter fallen auch besondere Personendaten i.S.v. § 3 Abs. 4 IDG und *Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen*. Damit ist mehr geplant als im Bund und in verschiedenen anderen Kantonen.[14]

— In den *Schulen* soll M365 grundsätzlich *nur für «gewöhnliche» Personendaten* genutzt werden dürfen. Die Mitarbeiter:innen dürfen damit *keine besonderen Personendaten* bearbeiten. Weil es aber vorkommen kann, dass Personen, die keinem Weisungsrecht des ED unterstehen, per E-Mail besondere Personendaten (z.B. Eltern ein ärztliches Zeugnis mit Gesundheitsdaten) an die Lehrer:innen senden, obwohl für deren Zustellung anderen Kanäle angeboten werden, können *ausnahmsweise besondere Personendaten* drin sein. Diese Gefahr soll mit zusätzlichen Massnahmen reduziert werden.

Stellungnahmen der/des DSB Die entsprechenden Stellungnahmen der/des DSB erfolgen erst im Jahr 2024.

Abgeltung oder Finanzhilfe?

Beizug von Dritten Der Kanton und die Gemeinden können zur Erfüllung ihrer gesetzlichen Aufgaben – ganz untechnisch gesprochen – Private beiziehen. Die Art, wie das geschieht, hat jedoch weitreichende Konsequenzen.

Aufgabenübertragung Kanton oder Gemeinden können die *Erfüllung einer öffentlichen Aufgabe* an *Private übertragen*. Damit werden diese Privaten datenschutzrechtlich selber zu einem öffentlichen Organ des übertragenden Kantons oder der übertragenden Gemeinde.[15] In diesem übertragenen Bereich gilt damit für ihr Bearbeiten von Personendaten das IDG – nicht mehr das DSG, sie sind selber verantwortlich im Sinne von § 6 IDG und unterstehen der Aufsicht der/des DSB des Kantons, nicht mehr des EDÖB.

Auftragsdatenbearbeitung Bei der Auftragsdatenbearbeitung überträgt ein öffentliches Organ ein *Bearbeiten von Personendaten* für seine Zwecke (d.h. für die Erfüllung seiner gesetzlichen Aufgabe[n]) an Dritte, an eine natürliche oder juristische Person des Privatrechts (oder an ein anderes öffentliches Organ) (§ 3 Abs. 8 revIDG). Die Privaten werden hier – anders als bei der Aufgabenübertragung – nicht selber zum öffentlichen Organ, sondern bleiben Private. Das auftraggebende öffentliche Organ bleibt nach § 7 Abs. 2 IDG verantwortlich, auch wenn es die Daten nicht selber bearbeitet, sondern bearbeiten lässt.

Klarheit Für die beigezogenen Privaten muss deshalb zweifelsfrei feststehen, ob sie nun Auftragsdatenbearbeiter:innen werden oder ob ihnen die Erfüllung einer öffentlichen Aufgabe übertragen wird und sie damit selber zu öffentlichen Organen werden.

Staatsbeitragsrecht Diese Unterscheidung ist nicht nur datenschutzrechtlich von Bedeutung. Auch das Staatsbeitragsgesetz (StBG) macht diese Unterscheidung: Staatsbeiträge werden als Finanzhilfe oder Abgeltung gewährt (§ 2 Abs. 1 StBG).

Abgeltung Eine Abgeltung ist eine Entschädigung, welche die finanziellen Lasten mildern oder ausgleichen soll, die sich aus der Erfüllung gesetzlich vorgeschriebener Aufgaben ergeben, die auf ein:e Empfänger:in ausserhalb der kantonalen Verwaltung übertragen werden (§ 4 Abs. 1 StBG). Das ist der gleiche Fall wie die Aufgabenübertragung nach § 3 Abs. 1 lit. c IDG. Dem entspricht auch die Regelung von § 4 Abs. 3 StBG, wonach, wer eine gesetzliche Aufgabe übertragen erhält, den jeweils anwendbaren gesetzlichen Verschwiegenheitspflichten unterliegt. Die personalgesetzliche Pflicht zur Verschwiegenheit (§ 19 PG) gilt damit ebenso wie Schweigepflichten der im konkreten Aufgabenbereich anwendbaren Fachgesetze (etwa des Steuergesetzes (§ 138 StG), des Sozialhilfegesetzes (§ 28 Abs. 1 SHG), des Sozialversicherungsrechts (Art. 33 ATSG), das Stimmgeheimnis (§ 43 Abs. 3 KV) usw.

Finanzhilfe Eine Finanzhilfe ist ein geldwerter Vorteil, der Empfänger:innen ausserhalb der kantonalen Verwaltung gewährt wird, um freiwillig erbrachte Leistungen im öffentlichen Interesse zu erhalten oder zu fördern (§ 3 Abs. 1 StBG) – früher Subvention genannt. Finanzhilfen können mit Bedingungen und Auflagen verbunden werden (§ 3 Abs. 4 StBG), aber gesetzliche Schweigepflichten gelten nicht ohne Weiteres für Finanzhilfe-Empfänger:innen (wenn nicht das entsprechende Gesetz selber diese Pflicht auf beigezogene Private ausweitet). Schweigepflichten können – und je nach der Leistung, die gefördert werden soll: sollen – aber vertraglich auferlegt werden.

Ob einer privaten Organisation die Erfüllung einer öffentlichen Aufgabe übertragen wird oder nicht, kann nicht die/der DSB entscheiden. Das muss vom öffentlichen Organ, das diese private Organisation beizieht, entschieden werden.

Entscheid Ob einer privaten Organisation die Erfüllung einer öffentlichen Aufgabe übertragen wird oder nicht, kann *nicht die/der DSB* entscheiden. Das muss vom öffentlichen Organ, das diese private Organisation beizieht, entschieden werden – und zwar bevor die vertragliche Regelung unterschrieben ist. Der DSB hat sich mit der Finanzverwaltung, die das «Handbuch für Steuerung und Ausgaben»[16] führt, kurzgeschlossen, so dass auch die Musterverträge entsprechend unterschieden werden. Ausserdem hat sich der DSB in letzter Zeit als «Wanderprediger» betätigt und mehrere Dienststellen und Departemente darauf aufmerksam gemacht, dass sie klar entscheiden und in den vertraglichen Regelungen festhalten müssen, ob es eine Aufgabenübertragung ist oder eben nicht. >

Konsequente Umsetzung Der Entscheid muss dann auch konsequent umgesetzt sein. Es darf nicht innerhalb eines Aufgabenübertragungsvertrags von Finanzhilfe oder in einem Auftragsdatenbearbeitungsvertrag von Abgeltung die Rede sein. Wenn – was zum Beispiel im Behindertenhilfebereich durchaus vorkommt – die gleiche Organisation verschiedene Angebote macht, mit dem einem Angebot eine öffentliche Aufgabe übertragen erhält, mit dem anderen Angebot aber bloss als Auftragsdatenbearbeiterin beigezogen wird, dann müssen mit dieser Organisation zwei verschiedene Verträge abgeschlossen werden.

Blosser Leistungseinkauf Im erwähnten «Handbuch für Steuerung und Ausgaben» wird als dritte Art des Beizugs von Dritten noch der Einkauf von Leistungen erwähnt.[17] Wie diese dritte Art datenschutzrechtlich von den anderen beiden abgegrenzt wird, wird in Zukunft noch auszuarbeiten sein.

Diskretion am Schalter

Wenn andere mithören Aufgrund von Meldungen aus der Bevölkerung hat sich der DSB um konkrete Schaltersituationen gekümmert, beispielsweise am Standort Clarahof der Kantonspolizei. Es ist betroffenen Personen nicht zuzumuten, dass «ihr Fall» an einem Schalter im offenen Raum in aller Lautstärke behandelt wird. Bei der betroffenen Verkehrsabteilung stiess das Anliegen auf offene Ohren. Es wurden verschiedene Massnahmen geprüft und umgesetzt. Gewisse, vor allem bauliche Massnahmen stossen aber auf (ebenfalls bauliche) Hindernisse. Ihre Umsetzung war nicht oder nicht sofort möglich.

Besondere Berichtspunkte

Gesetzlicher oder grossrätlicher Auftrag Die/der DSB muss – aufgrund einer gesetzlichen Grundlage oder weil der Grosse Rat diese Erwartung ausgedrückt hat, zu folgenden Punkten gesondert Bericht erstatten:

— zu laufenden und abgeschlossenen Pilotversuchen (siehe sogleich hinten unter «Pilotversuche»);

— zum Kantonalen Bedrohungsmanagement (siehe hinten unter «Kantonales Bedrohungsmanagement»).

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.[18] 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 die/den DSB eng begleitet wird.[19] Sie/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 Im Jahr 2023 lief kein auf § 9a IDG gestützter Pilotversuch. Der DSB hat aber schon zu mehreren Vorhaben der Verwaltung Stellung genommen, bei denen allenfalls Pilotversuche sinnvoll sein könnten, bevor die erforderliche formellgesetzliche Grundlage geschaffen werden kann. Am weitesten fortgeschritten war die Beratung bei den Vorbereitungen zu einem Pilotversuch über den Einsatz von unbemannten Luftfahrzeugen (Drohnen) bei der Kantonspolizei.[20]

Nachdem das Kantonale Bedrohungsmanagement seinen Betrieb im Frühjahr 2023 aufgenommen hat, hat der DSB nach dem Abschluss des ersten Betriebsjahres eine erste Prüfung begonnen.

Kantonales Bedrohungsmanagement (KBM)

KBM Per 1. März 2023 ist die vom Grossen Rat am 15. Mai 2021 beschlossene Revision des Polizeigesetzes zum Kantonalen Bedrohungsmanagement in Kraft getreten. Die Kantonspolizei hat im Sinne eines Bedrohungsmanagements konkrete, zielgerichtete von Personen ausgehende Gewaltbereitschaft zu erkennen, die geeignet ist, die physische, psychische oder sexuelle Integrität Dritter ernsthaft zu gefährden, und hierfür präventive Massnahmen zu treffen (§ 2 Abs. 2bis PolG).

Berichtsauftrag Der Grosse Rat hat es abgelehnt, für das KBM eine Dienstaufsicht analog dem Staatsschutzkontrollorgan zu schaffen. Dafür wurde § 61i PolG eingefügt. Er verpflichtet die/den DSB, der Wahlbehörde – also dem Grossen Rat – «jährlich einen speziellen Bedrohungsmanagement-Bericht im Sinne

von § 50 IDG vor(zulegen). Der Bericht äussert sich insbesondere über die durchgeführten Kontrollen gemäss § 45 IDG aufgrund der Aufgaben der oder des Datenschutzbeauftragten gemäss § 44 IDG.»

Datenschutzaufsicht ist nicht Dienstaufsicht Der DSB hat bereits im Tätigkeitsbericht 2020-2021[21] ausführlich darauf hingewiesen, dass die Datenschutzaufsicht nach § 61i PolG eben gerade nicht eine Dienstaufsicht ist. Aus dem erwähnten TB: «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 bestimmte 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.»[22]

Erste Prüfung im 2024 Nachdem das KBM seinen Betrieb im Frühjahr 2023 aufgenommen hat, hat der DSB nach dem Abschluss des ersten Betriebsjahres eine erste Prüfung begonnen. Über sie wird im nächsten Tätigkeitsbericht informiert. Nach § 45 Abs. 3 IDG sind die Berichte, welche die/der DSB im Rahmen der Kontrolltätigkeit erstellt, und die ihnen zugrunde liegenden Materialien nicht öffentlich zugänglich im Sinne von § 25 Abs. 1 IDG. Über die wichtigsten Feststellungen und Beurteilungen der Datenschutzprüfungen erstattet die/der DSB dem Grossen Rat periodisch Bericht nach § 50 IDG (siehe sogleich hinten unter «Kontrolltätigkeit»). Im gleichen Rahmen wird auch die Berichterstattung nach § 61i PolG über die Datenschutzprüfungen beim KBM erfolgen.

Das USB soll aufzeigen, wie in zwei Bereichen (Zugriffsberechtigungen im Klinikinformationssystem [KIS] und Archivierung/Löschung von Personendaten) Verbesserungen erreicht werden sollen, z.B. mit kompensierenden Massnahmen.

Kontrolltätigkeit

Datenschutzprüfungen (Audits) Der DSB hat im Jahr 2023 sieben[23] Datenschutzprüfungen (2022: 6) abgeschlossen (bzw. eine davon abgebrochen). Weitere sieben Kontrollen waren am Laufen, konnten aber im Berichtsjahr noch nicht abgeschlossen werden.

Abgeschlossene Datenschutzprüfung beim Statistischen Amt Die Prüfung beim Statistischen Amt konzentrierte sich auf die Erfassung und Bearbeitung von Personendaten. Sie führte zu zwei Feststellungen und Empfehlungen mit hoher und sechs mit mittlerer Priorität. Die Feststellung mit hoher Priorität betreffen die Bereiche Pseudonymisierung von Personendaten sowie Überprüfung des Schutzbedarfs und der Risikobeurteilung in Bezug auf Vertraulichkeit und Integrität.

Abgeschlossene Datenschutzprüfung beim UZB Die Prüfung beim Universitären Zentrum für Zahnmedizin Basel (UZB) nahm im Bereich der sozialen Zahnmedizin das Management der Datenweitergabe an Dritte (externe Schnittstellen) und die Gewährung des Zugangs der Patient:innen zu den eigenen Personendaten unter die Lupe. Sie führte zu drei Feststellungen und Empfehlungen mit hoher bzw. mittlerer Priorität in den Bereichen Beschreibung der Prozesse/Verfahren und Zuständigkeiten, Vorgaben an den IT-Dienstleister und die Dokumentation der Organisation und Prozesse bei der Gewährung des Rechts auf Zugang zu den eigenen Personendaten.

Follow-up-Audit beim USB Im Vorjahr wurde beim Universitätsspital (USB) ein Follow-up-Audit zur Datenschutzprüfung von 2018 gestartet. Eine erste Auswertung ergab, dass für gewisse 2018 festgestellte Grundprobleme noch immer keine aus Sicht des Datenschutzes hinreichenden Lösungen getroffen worden sind. In Abstimmung mit der Leitung des USB wurde daraufhin 2023 die Prüfung abgebrochen. Der DSB hat aber drei Hauptanliegen zum Risikomanagement (Risikoeignerschaft), zu Steuerungs- und Ausnahmeprozessen und zur Unabhängigkeit der/des CISO formuliert. Vereinbart wurde ausserdem, dass >

das USB aufzeigen soll, wie in zwei Bereichen (Zugriffsberechtigungen im Klinikinformationssystem [KIS] und Archivierung/Löschung von Personendaten) sowohl mit den aktuellen Anwendungen als auch mit dem System, welches das KIS ablösen soll, Verbesserungen erreicht werden sollen, z.B. mit kompensierenden Massnahmen. Diese Antworten stehen noch aus.

Abgeschlossene Datenschutzprüfung beim «ED-Hack» Der DSB hat den gravierenden Cybersicherheitsvorfall beim Erziehungsdepartement untersucht. Die Prüfung hat zu sieben Feststellungen und Empfehlungen in folgenden Bereichen geführt:

— Etablierung einer aktiven und hinreichend granularen Überwachung aller IT-Systeme;

— Verbesserung bei den Log- und Backup-Files;

— Ermittlung des Schutzbedarfs bei der Vorbereitung von Vorabkonsultationen der/des DSB;

— Umsetzung der von der Finanzkontrolle 2019 verlangten Informationssicherheit-Massnahmen;

— Abschluss einer Datenschutzvereinbarung mit einer Auftragsdatenbearbeiterin;

— Prüfung des möglichen Befalls weiterer IT-Systeme;

— Kommunikationskonzept für den Krisenfall.

Zwei abgeschlossene SIS-Kontrollen Regelmässig führt die/der DSB sog. «SIS-Kontrollen» durch. Dabei geht es um stichprobenbasierte Audits, bei denen Interviews mit Mitarbeiter:innen solcher Verwaltungsstellen durchgeführt werden, die auf das Schengener Informationssystem (SIS) zugreifen. Im Berichtsjahr 2023 konnten die SIS-Kontrollen bei der Abteilung Sicherheitspolizei (Kantonspolizei) und bei der Kriminalpolizei (Staatsanwaltschaft) abgeschlossen werden. Die Prüfungen fokussierten sich auf die Einhaltung der rechtlichen Vorgaben bei der Nutzung des SIS einschliesslich der generellen Kenntnis datenschutzrechtlicher Vorgaben und Rahmenbedingungen für die Nutzung von Informationssystemen.

Ob die tiefere Gutheissungs- und höhere Abweisungsquote bei den Informationszugangsgesuchen an der schlechteren Qualität der Gesuche lag oder an der geringeren Bereitschaft der Verwaltung, allfällige Geheimhaltungsinteressen weniger hoch als die Zugangsinteressen zu gewichten, kann ohne Kenntnis der Ablehnungsgründe nicht beurteilt werden.

Abgeschlossene VIS-Kontrolle Die kantonalen Datenschutzaufsichtsstellen sind gehalten, alle vier Jahre eine Kontrolle zur Nutzung des Visa-Informationssystems (VIS) zu prüfen. Der DSB hat 2023 eine ent-sprechende Kontrolle bei den Abteilungen Einreisen sowie Asyl und Rückkehrförderung im Migrationsamt durchgeführt. Sie hat zu drei Feststellungen und Empfehlungen geführt, und zwar in den Bereichen Schulungen zum Datenschutz und zu Datenbanknutzungen, Verbesserungen bei der E-Mail-Verschlüsselung und Regelung der Weitergabe von Informationen (inkl. der zu verwendenden Kommunikationsmittel).

Laufende Audits Ende 2023 waren darüber hinaus weitere Datenschutzprüfungen am Laufen, die Schlussberichte aber noch nicht abgeschlossen:

— eLM (Elektronisches Logiernächte-Management) beim Amt für Wirtschaft und Arbeit (u.a.) (gemeinsam mit der Finanzkontrolle);

— Industrielle Werke Basel IWB: Datentrennung;

— IT BS: Benutzer- und Berechtigungskonzept;

— IT BS: IAM (gemeinsam mit der Finanzkontrolle);

— Gerichte: Einsatz des Videoconferencing-Tools Webex;

— SIS-Kontrolle bei der Jugendanwaltschaft (Staatsanwaltschaft) und

— SIS-Kontrolle bei der Verkehrspolizei (Kantonspolizei).

Informationszugangsgesuche

Berichtspflicht Nach § 31 Abs. 2 IDV soll die Staatskanzlei die Statistik über die bei der kantonalen Verwaltung schriftlich eingereichten Informationszugangsgesuche nach dem Öffentlichkeitsprinzip der oder dem DSB zur Berichterstattung nach § 50 IDG zustellen. Daraus kann abgeleitet werden, dass im Tätigkeitsbericht über die Umsetzung des Öffentlichkeitsprinzips zu berichten sei. Allerdings bekommt die/der DSB nicht mehr Informationen, als er aus dem Jahresbericht des Regierungsrates[24] entnehmen kann, weshalb eine Interpretation nicht möglich ist.

Zugangsstatistik Die Informationszugangsgesuchs-Zahlen für das Jahr 2023 finden sich – über die gesamte Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts.[25]

Erledigung Die Zahl der eingegangenen Gesuche war gegenüber der Vorperiode um zwei Drittel höher (50 / Vorjahr 2022: 30). Der Anteil der ganz oder teilweise gutgeheissenen Gesuche war gegenüber dem Vorjahr geringer (64% / Vorjahr 2022: 73%). Der Anteil

der ganz abgewiesenen Gesuche stieg um rund einen Fünftel: Fast jedes dritte Gesuch wurde abgelehnt (30% / Vorjahr 2022: 23%). Die Zahl der am Jahresende noch nicht erledigten Gesuche ist weiterhin tief (6% / Vorjahr 2022: 3%). Ob die tiefere Gutheissungs- und höhere Abweisungsquote an der schlechteren Qualität der Gesuche lag oder an der geringeren Bereitschaft der Verwaltung, allfällige Geheimhaltungsinteressen weniger hoch als die Zugangsinteressen zu gewichten, kann ohne Kenntnis der Ablehnungsgründe nicht beurteilt werden.

Sinnvoller wäre, die Umsetzung des Öffentlichkeitsprinzips durch die Verwaltung einmal extern evaluieren zu lassen – und zwar im Hinblick auf die reaktive Informationstätigkeit (nach § 25 IDG) wie auch auf die (pro-)aktive Informationstätigkeit (nach § 20 IDG).

Evaluation statt «Interpretation»? Es ist zu überlegen, ob es in Zukunft unter diesen Umständen noch Sinn macht, die Zahlen aus dem regierungsrätlichen Jahresbericht hier wiederzugeben und zu «interpretieren». Sinnvoller wäre, die *Umsetzung des Öffentlichkeitsprinzips durch die Verwaltung* einmal *extern evaluieren zu lassen* – und zwar im Hinblick auf die reaktive Informationstätigkeit (nach § 25 IDG) wie auch auf die (pro-)aktive Informationstätigkeit (nach § 20 IDG). Die Ängste, die bei der Einführung des Öffentlichkeitsprinzips noch verbreitet waren, sollten ja in der Zwischenzeit etwas abgebaut worden sein. Deshalb könnte der Kanton das Öffentlichkeitsprinzip durchaus auch etwas prominenter sichtbar machen: Während zum Beispiel in der Fusszeile auf jeder einzelnen Seite der Webseite des Kantons Basel-Landschaft der Link zum «Öffentlichkeitsprinzip»[26] steht, müssen Interessierte auf der Basler Webseite entweder wissen, dass es eine solche Seite bei der Staatskanzlei gibt, die aber nur für die Zugangsgewährung zu Geschäften des Regierungsrates zuständig ist, oder sie gelangen über die Themensuche auf diese Seite.

Statistik zu den Geschäften des Datenschutzbeauftragten

Kennzahlen Die Kennzahlen für das Jahr 2023 finden sich im Statistikteil dieses Tätigkeitsberichts (S. 36).

Neu eröffnete Geschäfte Es wurde gleichsam eine Punktlandung: Im Jahr 2023 wurde genau gleich viele Geschäfte eröffnet wie zwei Jahre zuvor (583, +2%).[27] Damit wurde der leichte Rückgang im Vorjahr (2022: 571, -2%) wieder ausgeglichen.

Anteil komplexer Beratungsgeschäfte Erfasst wird mit den Kennzahlen auch der Anteil komplexer Geschäfte am Total der Beratungsgeschäfte, weil diese Geschäfte logischerweise mehr Ressourcen des DSB binden. Komplex ist ein Geschäft, wenn in der Geschäftskontrolle zehn oder mehr Bearbeitungsschritte dokumentiert sind. Dieser Anteil ist im Jahr 2023 leicht gefallen (17% / 2022: 19%), ist aber immer noch etwas höher als das langjährige Mittel.[28]

Erledigung innert 14 Tagen Von den nicht-komplexen Beratungsgeschäften, also mit höchstens neun Bearbeitungsschritten, wurden im letzten Jahr deutlich weniger innert 14 Tagen abgeschlossen (35% / 2021: 43%).

Schulungen Der DSB hat im Jahr 2023 anderthalbmal so viele Schulungen (12 / 2022: 8) durchgeführt wie im Jahr zuvor, unter anderem zweimal das ganztägige Seminar «Datenschutz und Öffentlichkeitsprinzip – kurz erklärt», mehrere Schulungen für Mitarbeiter:innen des Einwohneramtes und des Amtes für Wirtschaft und Arbeit. Es zeigt sich das Interesse der öffentlichen Organe, rechtzeitig zu erfahren, was die IDG-Revision mit sich bringt – so beispielsweise auch der Gemeinderat von Bettingen.

Initiant:innen und involvierte Stellen Wie bei der Zahl der neu eröffneten Geschäfte wurden auch bei den Stellen, die sich an den DSB gewandt haben,[29] die Veränderungen des Vorjahres mehr oder weniger wieder rückgängig gemacht. Es kamen wieder etwas mehr Geschäfte von den kantonalen öffentlichen Organen (64% / 2022: 60%), etwas weniger von ausserkantonalen Stellen (8% / 2022: 11%) und Privatpersonen (14% / 2022: 18%). Verdoppelt hat sich der Anteil der Medien (4% / 2022: 2%). Nur kleine Verschiebungen gab es bei den in die Geschäfte involvierten Stellen: Bei den Departementen, die am meisten involviert waren, liegt das Justiz- und Sicherheitsdepartement (15% / 2022: 16%) vor dem Finanzdepartement (9% / 2022: 10%), dem Departement für Wirtschaft, Soziales und Umwelt (8% / 2022: 6%), dem Präsidialdepartement und dem Erziehungsdepartement (beide 7% / 2022: 5%).[30] In dieser Statistik viel

>

vorzukommen hat nichts mit der fehlenden Qualität des Verwaltungshandelns zu tun – eher im Gegenteil: In diesen Departementen hat es Stellen und Personen (z.B. Datenschutzberater:innen), die Datenschutzprobleme erkennen und mit der/dem DSB angehen.

Weil – auf Wunsch der Verwaltung – die Kennzahlen mit dem Budget 2025 neu definiert werden, werden die Zahlen bezüglich der Geschäftsfälle (neu: Beratungen) nicht mehr direkt mit den Zahlen aus früheren Jahren vergleichbar sein.

Ausblick Die nächsten Zahlen für das Jahr 2024 und 2025 werden nur sehr begrenzt vergleichbar sein. Nicht nur fallen Geschäfte weg, die aus der Tätigkeit des bisherigen DSB im Büroausschuss von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, anfielen. Es werden – auf Wunsch der Verwaltung – die Kennzahlen mit dem Budget 2025 neu definiert werden. Aus diesem Grund werden die Zahlen bezüglich der Geschäftsfälle (neu: Beratungen) nicht mehr direkt mit den Zahlen aus früheren Jahren vergleichbar sein.

Personelle Ressourcen des Datenschutzbeauftragten

Headcount Der Headcount des DSB war unverändert. Weil für die ersten drei Quartale des Jahres 2023 kein:e Volontär:in gefunden werden konnte, wurde die Volontärin aus dem zweiten Halbjahr 2022 für neun Monate als juristische Mitarbeiterin angestellt.

Belastung Aufgrund der starken Zunahme von interdisziplinär zu behandelnden Digitalisierungsprojekten stösst das Team des DSB an seine Belastungsgrenze. Darauf wurde bereits in den letzten beiden Tätigkeitsberichten hingewiesen.[31] Mit dem Budget 2024 hat der Grosse Rat der/dem DSB eine Personalaufstockung um 150% bewilligt. Der «alte» DSB wird die Ausschreibung und Besetzung dieser Stellen aber seiner Nachfolgerin überlassen.

1 Nach § 13 Abs. 1 lit. a revIDG sind auch Rechtsetzungsprojekte, die das Bearbeiten von Personendaten betreffen oder die für den Umgang mit Informationen erheblich sind, der/dem DSB zur Vorabkonsultation vorzulegen. Bisher war die Stellungnahme zu solchen Vorhaben bloss bei den Aufgaben der/des DSB erwähnt (§§ 44 lit. f IDG).

2 § 13 Abs. 1 IDG und § 13 Abs. 1 lit. b revIDG. Vgl. zur Vorabkonsultation auch vorne S. 15 ff., insb. S. 18.

3 § 18 Abs. 4 IDG. Siehe dazu auch den Überblick über die Videoüberwachungsanlagen öffentlicher Organe im Kanton Basel-Stadt (Stand: 30. Juni 2022) im TB 2020-2021, S. 39 ff.

4 § 16a revIDG; vgl. dazu Ratschlag 21.1239.01, Ziff. 3.2.17 (S. 32 ff.) und TB 2022 des DSB/BS, S. 11 f.

5 § 3 Abs. 3 revIDG.

6 Vgl. dazu die Darstellung im TB 2022 des DSB/BS, S. 36.

7 Die Evangelisch-reformierte Kirche (ERK), die Römisch-Katholische Kirche (RKK), die Christkatholische Kirche (CRK) und die Israelitische Gemeinde (IGB).

8 Aktuell sind dies die Christengemeinschaft, die Neuapostolische Kirche Schweiz, Bezirk Basel, die Kulturvereinigung der Aleviten und Bektaschi und des Alevitischen Kulturzentrums Regio Basel und die Evangelisch-Lutherische Kirche Basel und Nordwestschweiz.

9 Erfasst sind nicht nur die aktuell in Basel-Stadt angemeldeten Einwohner:innen, sondern auch Verstorbene, weggezogene ehemalige Einwohner:innen und sog. Zugehörige (z.B. Grundeigentümer:innen, die nicht in Basel-Stadt angemeldet sind, Organe juristischer Personen, die ihren Sitz in Basel-Stadt haben oder hatten), total also ca. 1.08 Mio. natürliche Personen.

10 So zum Beispiel ‹anglikanisch›, ‹buddhistisch›, ‹muslimisch›, ‹sunnitisch›, ‹schiitisch› oder auch ‹römisch-katholisch, ausgetreten›.

11 Die KOI hat nach § 3 Abs. 3 DMV insbesondere die folgenden Aufgaben: a) Festlegung der Anforderungen, welche das Gesamtsystem erfüllen muss und Sicherstellung der Einhaltung dieser Anforderungen; b) Festlegung der Qualitätsstandards; c) Sicherstellung des Verfahrens zur Vernichtung von Daten; d) Festlegung des vorzuhaltenden Schutzes des Gesamtsystems; e) Risikomanagement; f) Sicherstellung der Gewährleistung der Rechte der betroffenen Personen; g) Sicherstellung der Berücksichtigung von Sperrcodes; h) Sicherstellung, dass allen Daten ein:e Dateneigner:in zugewiesen wird; i) Sicherstellung eines bedarfsgerechten Abrufverfahrens; j) Sicherstellung der Einhaltung der Rechte und Pflichten der Dateneigner:innen.

12 Ein Beispiel in Abklärung: Darf die Abteilung Verkehr der Kantonspolizei (in anderen Kantonen das «Strassenverkehrsamt») Daten von Motorfahrzeughalter:innen («Max Mustermann ist Halter des Fahrzeugs XY mit dem Kennzeichen BS 987 654») via Datenmarkt anderen öffentlichen Organen zugänglich machen, wenn nach Auskunft des «Lieferanten», des Bundesamtes für Strassen ASTRA, das Strassenverkehrsamt anderen Stellen diese Daten nur im Einzelfall bekanntgeben darf, wenn diese schriftlich ein hinreichendes Interesse geltend gemacht haben (Art. 89g Abs. 3 lit. c SVG)?

13 Vgl. dazu die Ausführungen in den letzten Tätigkeitsberichten: TB 2017/2018/2019 des DSB/BS, S. 11 ff.; TB 2020-2021 des DSB/BS, S. 21 ff. und 32 ff.; TB 2022 des DSB/BS, S. 24 f.

14 Vgl. zum Einsatz im *Bund* die im Internet veröffentlichte Einsatzrichtlinie Microsoft 365 (<https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/CEBA/E031-Einsatzrichtlinie%20Microsoft%20365%20.pdf.download.pdf/E031-Einsatzrichtlinie%20Microsoft%20365%20.pdf>); zum Einsatz im *Kanton Zürich* den Regierungsratsbeschluss vom 30. März 2022 (<https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf>) und die Würdigung von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten (https://www.privatim.ch/de/kein-freipass-fur-microsoft-365/); zum Einsatz im *Kanton Bern* die Berichterstattung über den Beschluss des Regierungsrates des Kantons Bern, den zugrundeliegenden Bericht des Kantonalen Amtes für Informatik und Organisation (KAIO) und die Stellungnahme der Datenschutzaufsichtsstelle (über <https://www.inside-it.ch/regierungsbeschluss-berner-kantonsverwaltung-kriegt-microsoft-cloud-20230630>).

15 § 3 Abs. 1 IDG: «Öffentliche Organe im Sinne dieses Gesetzes sind: c) Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist.»

16 Handbuch für Steuerung und Ausgaben, im Intranet unter <https://finanzen.intranet.bs.ch/steuerung-und-ausgaben>.

17 Handbuch für Steuerung und Ausgaben (Fussnote 13), Ziff. 10.1.3.

18 Vgl. dazu die Ausführungen in TB 2016 des DSB/BS, S. 41, sowie PK-IDG/BS-Husi, § 9a N 6 ff.

19 Bericht 13.0739.02, S. 5 f.

20 Der Regierungsrat konnte am 30. April 2024 die Verordnung über den Einsatz von unbemannten Luftfahrzeugen bei der Kantonspolizei als Pilotversuch (Drohnenverordnung) (SG 153.275) erlassen. Der damit geregelte Pilotversuch läuft vom 15. Mai 2024 bis zum 15. Mai 2026 (§ 15 Drohnenverordnung).

21 TB 2020-2021, S. 19 f.

22 TB 2020-2021, S. 20.

23 Im Jahresbericht 2023 des Regierungsrates (S. 304) sind acht Datenschutzprüfungen angegeben. Bei einer der dort erfassten Prüfungen hat sich nach der Erfassung herausgestellt, dass doch noch Anpassungen an den Feststellungen nötig sind. Sie ist deshalb hier unter den noch laufenden Prüfungen aufgeführt, und die Zahl der abgeschlossenen Datenschutzprüfungen muss auf sieben korrigiert werden.

24 Jahresbericht 2023 (des Regierungsrates), S. 73.

25 Tabelle C im Statistikteil (S. 36).

26 <https://www.baselland.ch/themen/o/offentlichkeitsprinzip>.

27 Tabelle A im Statistikteil (S. 36).

28 Tabelle B im Statistikteil (S. 36).

29 Grafik D im Statistikteil (S. 37).

30 Grafik E im Statistikteil (S. 37).

31 TB 2020-2021 des DSB/BS, S. 48 f., TB 2022 des DSB/BS, S. 38 f.

Statistische Auswertungen 2023 (mit Vorjahresvergleich)

A Geschäfte

	2023		2022		2021		2020	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	583		571		583		543	
prozentuale Veränderung gegenüber Vorjahr		2		-2		7		5

B Indikatoren gemäss Budget

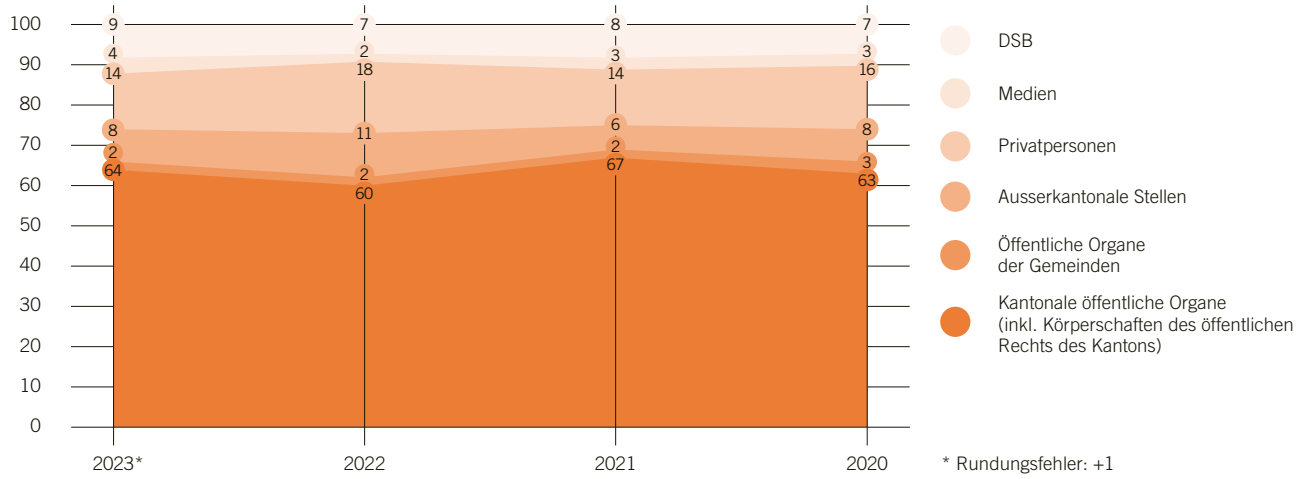
	2023		2022		2021		2020	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		17		19		16		14
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		35		43		44		48
Durchgeführte Audits								
Anzahl durchgeführte Audits	7		6		1		0	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	12		8		9		6	

C Öffentlichkeitsprinzip

	2023		2022		2021		2020	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	50		30		31		36	
prozentuale Veränderung gegenüber Vorjahr		67		-3		-14		50
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche	25	50	19	63	13	42	18	50
Anzahl teilweise gutgeheissener Gesuche	7	14	3	10	3	10	2	6
Anzahl ganz abgewiesener Gesuche	15	30	7	23	14	45	11	31
Anzahl noch nicht rechtskräftig entschiedener Gesuche	3	6	1	3	1	3	4	11
zurückgezogen	0	0	0	0	0	0	1	3

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 2023 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2023, S. 73

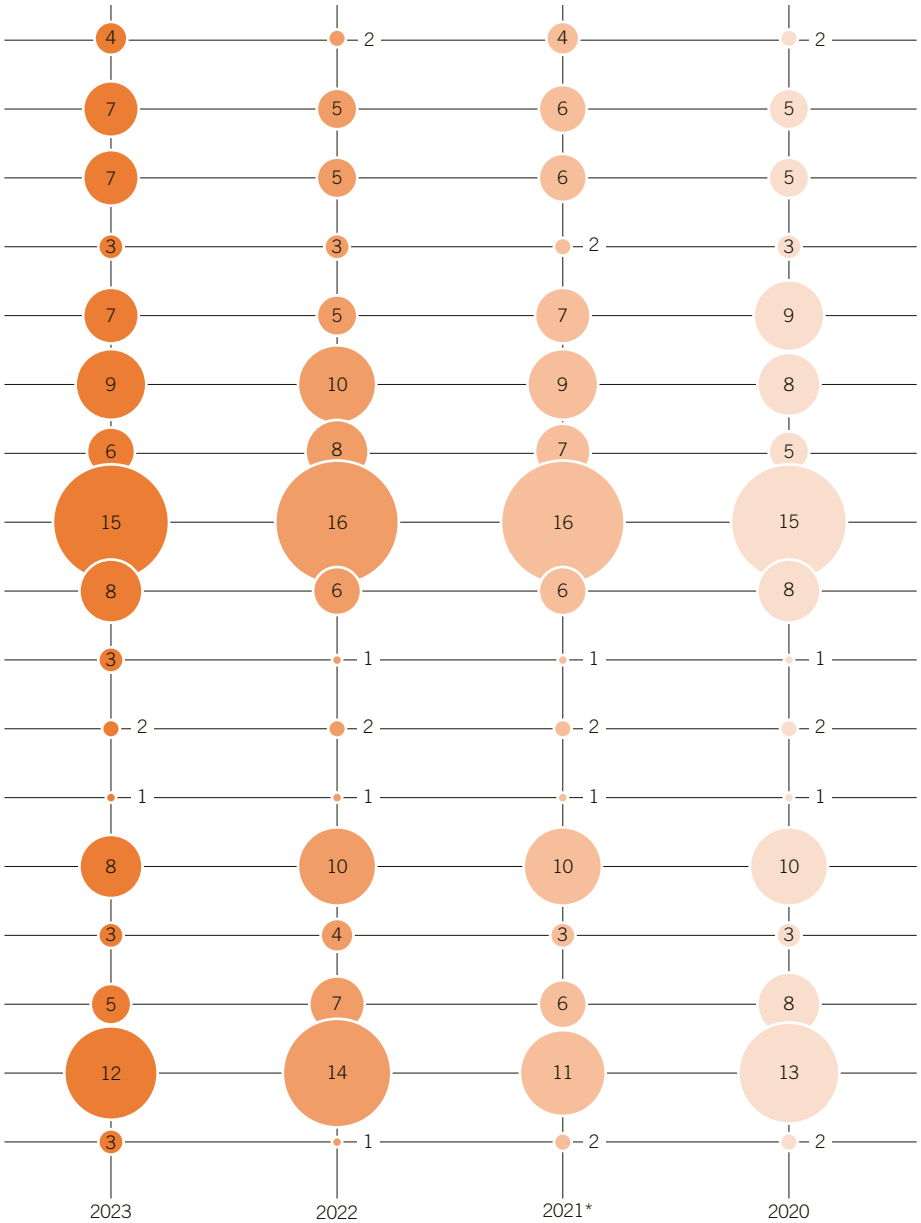
D Initiant:innen: Veranlasser:innen der Geschäfte (A) in %



* Rundungsfehler: +1

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.



* Rundungsfehler: +1

Anhang

Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

Kanton Basel-Stadt:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

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.

ISV Verordnung vom 13. Dezember 2016 über die Informationssicherheit (ISV), SG 153.320.

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

PG Personalgesetz vom 17. November 1999, SG 162.100.

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

revIDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz), in der Fassung des Grossratsbeschlusses vom 20. Oktober 2022 (noch nicht in Kraft).

StatG Gesetz vom 21. Mai 2014 über die öffentliche Statistik (StatG), SG 453.200.

StBG Staatsbeitragsgesetz vom 11. Dezember 2013 (StBG), SG 610.500.

StG Gesetz vom 12. April 2000 über die direkten Steuern (Steuergesetz, StG), SG 640.100.

SHG Sozialhilfegesetz vom 29. Juni 2000, SG 890.100.

Materialien

Bericht 21.1239.02 Bericht 21.1239.02 vom 15. September 2022 der Justiz-, Sicherheits- und Sportkommission zum Ratschlag 21.1239.01 zu einer Änderung des Gesetzes über die Information und Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze (Anpassung an die europäischen Datenschutzreformen und weitere Anpassungen) sowie zum Anzug 21.5704.01 Thomas Gander und Konsorten zur Schaffung von rechtlichen Grundlagen für die Anwendung von algorithmus-basierter Instrumente in der Polizeiarbeit.

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.

Ratschlag 21.1239.01 Ratschlag 21.1239.01 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).

Ratschlag 13.0739.01 Ratschlag 13.0739.01 des Regierungsrates vom 21. Mai 2013 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.

Ratschlag 08.0637.01 Ratschlag 08.0637.01 des Regierungsrates vom 11. Februar 2009 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz).

Bund:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

ATSG Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG), SR 830.1.

aVDSG Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) (per 1. September 2023 abgelöst durch die DSV).

BGÖ Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ), SR 152.3.

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

DSG Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG), SR 235.1.

DSV Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV), SR 235.11.

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

RHG Bundesgesetz vom 23. Juni 2006 über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (Registerharmonisierungsgesetz, RHG), SR 431.02.

SVG Strassenverkehrsgesetz vom 19. Dezember 1958 (SVG), SR 741.01.

Europarat, Europäische Union: Rechtsgrundlagen

Rechtsgrundlagen

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.

Richtlinie 95/46/EG Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23.11.1995, S. 31 ff.

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>.

Literatur

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.

Abkürzungen

AGB Allgemeine Geschäfts-Bedingungen
AKV Aufgaben, Kompetenzen, Verantwortlichkeiten
AWA Amt für Wirtschaft und Arbeit
ASTRA Bundesamtes für Strassen
BdM Bereich Bevölkerungsdienste und Migration
CISO Chief Information Security Officer (Informationssicherheitsbeauftragte:r)
CRK Christkatholische Kirche (CRK)
DSB Datenschutzbeauftragte:r
DSBer Datenschutzberater:in(nen)
DSFA Datenschutz-Folgenabschätzung
DVS Digitale Verwaltung Schweiz
ED Erziehungsdepartement
EDÖB Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
eLM elektronisches Logiernächte-Management
ERK Evangelisch-reformierte Kirche
EU Europäische Union
IAM Identity and Access Management
IGB Israelitische Gemeinde Basel
ILK Informatik-Leiter:innen-Konferenz
ISB Informationssicherheitsbeauftragte:r des Kantons
ISBD departementale:r Informationssicherheitsbeauftragte:r
ISDS-Konzept Informationssicherheits- und Datenschutz-Konzept
ISO Steuerungsorgan für Informationssicherheit (aufgehoben)
iwb Industrielle Werke Basel
JSD Justiz- und Sicherheitsdepartement
JSSK Justiz-, Sicherheits- und Sportkommission (des Grossen Rates)
KBM Kantonales Bedrohungsmanagement
KDM Kantonaler Datenmarkt
KOI Konferenz für Organisation und Informatik
RKK Römisch-Katholische Kirche
SG Systematische Gesetzessammlung (des Kantons Basel-Stadt)
SIK Schweizerische Informatikkonferenz
SIS Schengener Informations-System
SLA Service level Agreement
SR Systematische Rechtssammlung (des Bundes)
SWA Schwellwertanalyse
UZB Universitäres Zentrum für Zahnmedizin Basel
VAK Vorabkonsultation
VIS Visa-Informations-System

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. (em.) Dr. iur., Advokat

Team
Eva Maria Bader (Sekretariat)
Sama Bolog, MLaw (1.1.–30.9.2023)
Pascal Lachenmeier, Dr. iur., Advokat
Sukhwant Singh, Master in IT Business Engineering
Thomas Sterchi, Wirtschaftsinformatiker HF
Ines Weihrauch, lic. iur., Advokatin
Barbara Widmer, Dr. iur., LL.M., CIA

Volontär:in(nen):
Pascal Yanick Tamm, MLaw
(1.10.2023 - 31.3.2024)

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