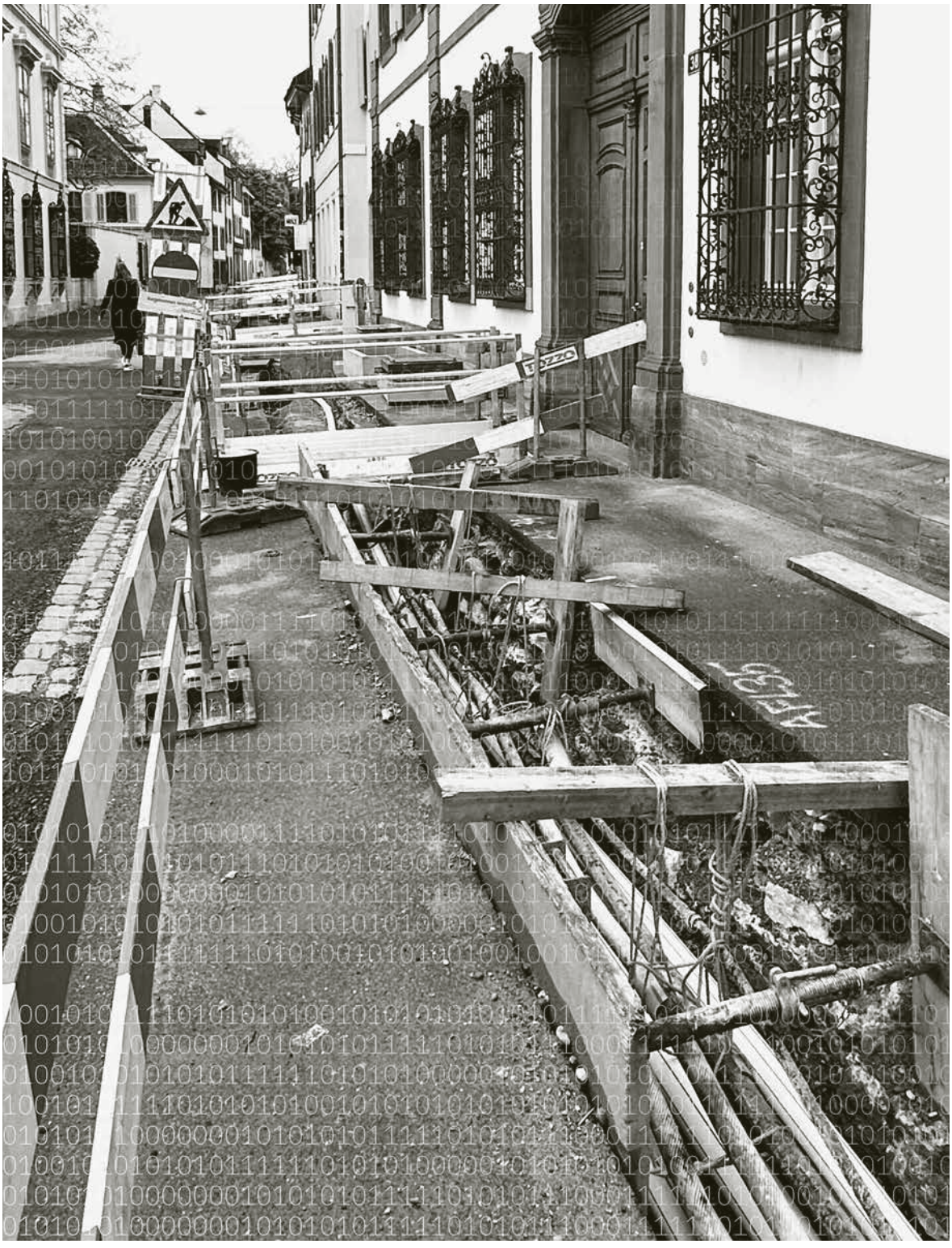
Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat



'22

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

Fotokonzept: Baustellen
Fotos: B. Rudin

Inhaltsübersicht

Einleitung

4 2022: IDG-Revision und «Baustellen» bei der Digitalisierung

Trends

8 Revidiertes IDG: Neue Aufgaben und Pflichten

18 Revidiertes IDG: Unterstützung durch die Datenschutzberater:innen

22 Die grössten «Baustellen» und Herausforderungen bei der Digitalisierung

29 Anwendbares Datenschutzrecht beim Vollzug von Bundesrecht

Jahres-rückblick

42 2022: Kurzer Blick auf die wichtigsten Geschäfte

50 Statistische Auswertung 2022

Anhang

42 Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

43 Impressum

Einleitung

2022: IDG-Revision und «Baustellen» bei der Digitalisierung

Der Rückblick auf das Jahr 2022 lässt ein paar Themen in den Vordergrund treten: Die vom Grossen Rat beschlossene (aber wegen der noch ausstehenden Revision der dazugehörenden Verordnung noch nicht in Kraft getretene) Teilrevision des Informations- und Datenschutzgesetzes sowie die «Baustellen» und Herausforderungen bei der Digitalisierung der Verwaltung.

Teilrevision des Informations- und Datenschutzgesetzes

Beschluss des Grossen Rates Im Herbst des Jahres 2022 konnte der Grosse Rat die Revision des Informations- und Datenschutzgesetzes (IDG) abschliessen. Der Datenschutzbeauftragte war an allen Sitzungen der vorberatenden Justiz-, Sicherheits- und Sportkommission (JSSK) mit dabei, zusammen mit der Vertretung des Präsidialdepartements.

Grund für die Revision Die Revision war notwendig geworden, weil der Europarat mit seiner modernisierten Konvention 108+ und die Europäische Union mit dem Erlass der Datenschutz-Grundverordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 neue Anforderungen an die Datenschutzregelung gestellt haben. Die Schweiz hat das Protokoll zur Änderung der Europarats-Konvention 2019 unterzeichnet; die Bundesversammlung hat es im Juni 2020 genehmigt und die notwendigen Änderungen mit einer Totalrevision des Bundes-Datenschutzgesetzes vorgenommen, das am 1. September 2023 in Kraft treten wird. Die Kantone sind zuständig für die Umsetzung im kantonalen Recht. Die Schengen-relevante Richtlinie (EU) 2016/680 wurde der Schweiz am 1. August 2016 notifiziert, womit die Zweijahresfrist zur Umsetzung im Schweizer Recht begann. Als Übergangslösung hat der Bund ein Schengen-Datenschutzgesetz (SDSG) erlassen, das am 1. März 2019 in Kraft trat und gilt, bis das Bundes-Datenschutzgesetz in Kraft tritt. Auch hier müssen die Kantone ihr Recht selber anpassen – bzw. hätten es ebenfalls bis am 1. August 2018 angepasst haben müssen.

Weiteres Vorgehen Mit der Revision des IDG (revIDG) wurden nun die notwendigen Anpassungen auf Gesetzesstufe vorgenommen. Gleichzeitig wurden bei einigen wenigen IDG-Bestimmungen Anpassungen oder Präzisierungen vorgenommen, die sich in der Praxis als erforderlich und sinnvoll gezeigt haben. In Vorbereitung ist nun die Anpassung der Informations- und Datenschutzverordnung (IDV). Sobald diese abgeschlossen ist, kann das revidierte IDG in Kraft gesetzt werden. Es ist zu hoffen, dass es im Herbst 2023 so weit ist.

Wichtigste Abweichung vom Entwurf des Regierungsrates Der Grosse Rat ist mit seinem Beschluss am 20. Oktober 2022 weitestgehend dem Ratschlag 21.1239.01 des Regierungsrates gefolgt. Was diese *Neuerungen* im revidierten IDG für die öffentlichen Organe bedeuten, stellen wir im ersten Teil (S. 8 ff.) dar. In einem Punkt hat der Grosse Rat aber auf einstimmigen Antrag seiner Justiz-, Sicherheits- und Sportkommission einen abweichenden Entscheid gefällt, der für die bessere Umsetzung der Datenschutzanliegen wichtig sein wird: Er hat beschlossen, dass nicht nur die Staatsanwaltschaft, die Kantonspolizei und der Justizvollzug betriebliche *Datenschutzberater:innen* bezeichnen müssen, sondern auch alle Departemente, die Gerichte und Gemeinden und nach dem Entscheid durch den Regierungsrat auch weitere öffentliche Organe, die regelmässig sensitive oder sehr viele Personendaten bearbeiten (§ 16b revIDG).

Datenschutzberater:innen Mit dieser Änderung soll das Datenschutz-Knowhow dort gebündelt werden, wo es im Verwaltungsalltag gebraucht wird (siehe unten S. 18 ff.). Die *Aufgaben*, welche die Datenschutzberater:innen zu erfüllen haben, sind *nicht neu* – sie bestehen seit der Schengen-Revision des Vorgängergesetzes des IDG. Auch was jetzt unter dem Namen «Datenschutz-Folgenabschätzung» vorgeschrieben ist, ist nichts Neues: Es ist das, was schon bisher zur Vorbereitung der seit 2008 vorgeschriebenen Vorabkontrolle (neu unter dem Namen «Vorabkonsultation») erledigt werden musste.

Was hat der Datenschutzbeauftragte sonst noch getan?

Beratung und Kontrolle Der Datenschutzbeauftragte (DSB) hat nebst der Begleitung der JSSK bei der Beratung der IDG-Revision entsprechend seinem gesetzlichen Auftrag einerseits die öffentlichen Organe von Kanton und Gemeinden wie auch die betroffenen Personen beraten und andererseits die Umsetzung der IDG-Normen durch die öffentlichen Organe kontrolliert. Ein besonderes Augenmerk haben wir auf die «Baustellen» und Herausforderungen bei der Digitalisierung der Verwaltung geworfen: auf die weiterhin fehlende IT-Governance, auf neue technologische Entwicklungen, welche die Verwaltung herausfordern und nach unserer Meinung dringend zentrale Vorgaben benötigen. Von IT BS wurden wir in die Arbeiten am neuen Projektleitfaden einbezogen, der das Projektmanagement verbessern und die Elemente des präventiven Datenschutzes (Datenschutz-Folgenabschätzung und Vorabkonsultation) implementieren soll. Bei einer «Baustelle», den «Aufräumarbeiten» im Kantonalen Datenmarkt, haben wir den Druck erhöht.

Kennzahlen Erstmals seit sieben Jahren hat die Zahl der neu eröffneten Geschäfte nicht zugenommen: Es waren 12 Geschäfte weniger als vor einem Jahr (bei einer Gesamtzahl von über 570). Stark zugenommen hat aber der Anteil der komplexen Beratungsgeschäfte, nämlich um fast einen Fünftel von 16% aller Beratungsgeschäfte im Vorjahr auf 19%. Dazu gehören gerade auch die grösseren Digitalisierungsvorhaben. Diese Geschäftslast hat das Team des DSB an seine Belastungsgrenzen gebracht. Aus Ressourcengründen konnten wir etwas weniger Geschäfte selber an die Hand nehmen.

Der Bericht

Zwei Teile Mit diesen Hinweisen auf die behandelten Themen sind wir bereits mitten im Bericht. Er gliedert sich in zwei Teile:

— Im ersten Teil (S. 8 ff.), gleich nach der Einführung, zeigen wir Themen auf, die uns im vergangenen Jahr beschäftigt haben: wie erwähnt die Neuerungen aufgrund der IDG-Revision, die Chance, die sich mit den Datenschutzberater:innen in den Departementen und bestimmten weiteren Amtsstellen ergeben, die «Baustellen» und Herausforderungen der Digitalisierung und die Frage des anwendbaren Datenschutzrechts, wenn ein öffentliches Organ des Kantons (konkret ging es um die Pensionskasse) Bundesrecht vollzieht.

— Im zweiten Teil (S. 34 ff.) stellen wir dar, was wir in dieser Zeit in der Beratungs- und Kontrolltätigkeit getan haben und was uns dabei besonders herausgefordert hat. Abgeschlossen wird dieses Kapitel durch die Statistik (S. 40 f.).

Anders als in früheren Jahren wird aus Zeitgründen auf einen dritten Teil mit illustrativen Fällen verzichtet. Wir wünschen Ihnen trotzdem eine spannende Lektüre!

Zum Schluss

Danke! Unsere Aufgabe nach dem Informations- und Datenschutzgesetz (IDG)[1], nämlich für den Schutz der Privatheit der Einwohner:innen, über welche die öffentlichen Organe Personendaten bearbeiten, und ihres Informationszugangsrechts nach dem Öffentlichkeitsprinzip zu sorgen, könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb:

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

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

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

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

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

— der Volontärin Sama Bolog und dem Volontär Colin Carter für ihre kritische Neugier und ihre aktive Mitarbeit in ihrem jeweils sechsmonatigen Volontariat und

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

Beat Rudin, Datenschutzbeauftragter

1 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Schluss des Berichts (S. 42 f.) detailliert aufgeführt.


ZIEGLER
ZIEGLER
ZIEGLER
ZIEGLER
ZIEGLER
ZIEGLER
ZIE

Trends

Trend 1 Revidiertes IDG: Neue Aufgaben und Pflichten

Trend 2 Revidiertes IDG: Unterstützung durch die Datenschutzberater:innen

Trend 3 Die grössten «Baustellen» und Herausforderungen bei der Digitalisierung

Trend 4 Anwendbares Datenschutzrecht beim Vollzug von Bundesrecht

Trend 1 Revidiertes IDG: Neue Aufgaben und Pflichten

Das Informations- und Datenschutzgesetz (IDG) muss an die neuen europarechtlichen Anforderungen angepasst werden. Der Grosse Rat hat die Revision am 20. Oktober 2022 verabschiedet (revIDG) und ist dabei in ein paar Punkten vom regierungsrätlichen Entwurf abgewichen. Am 7. Dezember 2022 ist die Referendumsfrist ungenutzt verstrichen. Zurzeit wird die Anpassung der Informations- und Datenschutzverordnung (IDV) vorbereitet. Was sind die wesentlichsten Neuerungen?

Europarechtliche Datenschutz-Vorgaben

Europarats-Konvention und EU-Schengen-Richtlinie Die europäischen Datenschutzreformen brachten neue Anforderungen mit sich, die auch in der Schweiz umzusetzen sind:

— die Anforderungen der *Europarats-Konvention 108+* (ER-Konv 108+), weil die Schweiz diese Konvention ratifiziert hat;

— die Anforderungen der *Richtlinie (EU) 2016/680 für die justizielle und polizeiliche Zusammenarbeit*, weil diese Richtlinie Schengen-relevant ist und deshalb nach dem Schengen-Assoziierungs-Abkommen (SAA) als Weiterentwicklung des Schengen-Besitzstands («Schengen-Acquis») im nationalen Recht umzusetzen ist.

EU-Datenschutz-Grundverordnung? Die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) ist für die Schweiz nicht direkt verbindlich, weil sie nicht Mitgliedstaat der EU ist. Trotzdem ist die DSGVO nicht unbeachtlich: Ein Datentransfer von öffentlichen Stellen oder Unternehmen in der EU an Empfänger:innen in ein Drittland (wie die Schweiz) ist nur ohne Weiteres zulässig, wenn die EU-Kommission im Sinne von Art. 45 DSGVO anerkennt, dass dieses Drittland über ein angemessenes Datenschutzniveau verfügt.[1]

Vom Ratschlag zum Grossratsbeschluss

Ablauf Mit dem Ratschlag 21.1239.01 hat der Regierungsrat am 29. September 2021 dem Grossen Rat eine Revision des Informations- und Datenschutzgesetzes beantragt, um die europarechtlichen Vorgaben im kantonalen Recht zu erfüllen. Die grossrätliche Justiz-, Sicherheits- und Sportkommission hat den regierungsrätlichen Antrag von Januar bis September 2022 beraten und dem Grossen Rat mit Bericht 21.1239.02 vom 15. September 2022 Antrag auf eine in wenigen Punkten abweichende Revision des IDG gestellt. Der Grosse Rat hat in seiner Sitzung vom 20. Oktober 2022 die IDG-Revision so beschlossen, wie es die JSSK beantragt hatte. Die Gesetzesänderung wurde am 26. Oktober 2022 im Kantonsblatt veröffentlicht. Die Referendumsfrist ist am 7. Dezember 2022 ungenutzt verstrichen.

Änderungen Der Grossratsbeschluss weist gegenüber dem regierungsrätlichen Antrag folgende Präzisierungen auf:

— Für öffentliche Organe, die im wirtschaftlichen Wettbewerb stehen, wird die Aufsicht gleich wie im Bund, wo die Aufsicht öffentlich-rechtlich bleibt, geregelt (§ 2 Abs. 2 revIDG). Die Aufsicht bleibt bei der/dem kantonalen DSB, auch wenn ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt (§ 2 Abs. 2 Satz 3 revIDG). Damit wird eine *Einheitlichkeit der Aufsicht* für die öffentlichen Organe von Kanton und Gemeinden geschaffen, auch dann, wenn die Daten wie von einem privaten Unternehmen bearbeitet werden dürfen.

— Die Definition des *Profilings* wird in Anlehnung an den Bund um das zusätzliche Tatbestandsmerkmal «automatisierte Datenbearbeitung» sowie unter Berücksichtigung der Formulierung des revidierten Datenschutzgesetzes des Bundes um die Vorhersage des Verhaltens ergänzt (§ 3 Abs. 7 revIDG).

— Mehrere IDG-Bestimmungen delegieren den Erlass von *konkretisierenden Bestimmungen* an den Regierungsrat. Neu wird für alle diese Bereiche einheitlich festgelegt, dass diese kantonalen Verordnungsbestimmungen jeweils für die Gerichte, die Gemeinden, die weiteren Körperschaften und selbstständigen Anstalten sinngemäss nur dann zur Anwendung kommen, soweit diese keine eigenen Regelungen erlassen (Nachweis der Einhaltung der Datenschutzbestimmungen: § 6 Abs. 3 revIDG; Informationssicherheit: § 8 Abs. 4 revIDG, Videoüberwachung: § 18 Abs. 5 revIDG sowie behördliche Informationstätigkeit: § 20 Abs. 4 revIDG).

Ergänzung Der Grosse Rat hat die Pflicht, *Datenschutzberater:innen* zu bezeichnen, über die Bereiche im engeren Schengen-Kontext (Staatsanwaltschaft, Justizvollzug, Polizei) hinaus erweitert. Dazu mehr hinten S. 18 ff.

Die wichtigsten Neuerungen

Das Wichtigste im Überblick In der Folge sollen hier die wichtigsten Neuerungen, welche die öffentlichen Organe des Kantons betreffen, dargestellt werden.

Begriffsdefinitionen: Zusätzliche besondere Personendaten

Erhöhte Voraussetzungen Schon bisher galten strengere Anforderungen, wenn öffentliche Organe nicht nur «gewöhnliche» (einfache, triviale) Personendaten bearbeiten, sondern (auch) besondere Personendaten, also Daten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht («sensitive Personendaten»). Die Kategorie dieser sensitiven Personendaten wird nun entsprechend den europarechtlichen Vorgaben[2] erweitert um die folgenden drei neuen Datenarten:

Ein öffentliches Organ darf ein Profiling nur vornehmen, wenn ein Gesetz ausdrücklich dazu ermächtigt oder verpflichtet oder wenn es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist.

Genetische Daten Mit dem Einfügen der Klammer «(genetischen Daten)» zum schon bisher verwendeten Begriff «Erbgut» wird klargestellt, dass damit dasselbe gemeint ist wie in den europarechtlichen Erlassen.

Angaben über das Sexualleben und die sexuelle Orientierung Da mit der schon bisher erwähnten «Geheimsphäre» nicht zwingend auch Angaben zum Sexualleben bzw. zur sexuellen Orientierung mitverstanden werden, werden diese beiden Kategorien neu in die Bestimmung eingefügt.

Biometrische Daten Unter «biometrischen Daten» werden mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person verstanden, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten). Darunter fallen zum Beispiel daktyloskopische Daten, Handvenen-Muster, Stimm-Muster, Iris-Muster und durch Gesichtserkennungsprogramme gewonnene Daten – aber nicht jedes Foto eines Gesichts!

Profiling

Begriff Der Begriff «Profiling» wird neu ins IDG aufgenommen. In Anlehnung an die Begriffsbestimmung im Bundes-DSG wird das Profiling als eine *«automatisierte Datenbearbeitung»* definiert. Automatisiert bedeutet in diesem Zusammenhang maschinengestützt. Diese automatisierte Bearbeitung kann auch bei nicht sensitiven Personendaten, ja sogar bei (noch) nicht personenbezogenen Informationen zu einer Gefahr für die Persönlichkeitsrechte werden. Die Verwendung des Begriffs *«Informationen»* – in Abweichung zur Verwendung des Begriffs «Personendaten» in der Bundesdefinition (Art. 5 lit. g revDSG) – ist insofern wichtig, weil Informationen, die ursprünglich nicht personenbezogen vorliegen und damit keine Personendaten darstellen, erst durch die Verknüpfung mit Personendaten selber zu Personendaten werden können. Die Bearbeitung von solchen «Noch-nicht-Personendaten» darf deshalb nicht von der Profiling-Definition ausgenommen werden.

Zweck Es geht beim Profiling um eine automatisierte Auswertung von Informationen mit dem Ziel, wesentliche *persönliche Merkmale zu analysieren* oder *Entwicklungen vorherzusagen*, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel. Auch wenn einzelne Aspekte (z.B. persönliche Vorlieben, Interessen, Zuverlässigkeit) des Auswertungszwecks eher auf privatrechtliche Bearbeitungen zugeschnitten sind, bleiben sie in der Begriffsdefinition erhalten, damit die in der Privatwirtschaft schon verbreiteten und künftig auch in der Verwaltung denkbaren Anwendungen (z.B. automatisierte Bewertungen von Bewerbungen) mit dieser Definition bereits erfasst wären.

Konsequenz Das Profiling wird behandelt wie besondere Personendaten: Ein öffentliches Organ darf ein Profiling nur vornehmen, wenn ein Gesetz ausdrücklich dazu ermächtigt oder verpflichtet oder wenn es für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe zwingend notwendig ist (§ 9 Abs. 1 revIDG). Und bekannt geben darf ein öffentliches Organ Resultate eines Profilings nur, wenn ein Gesetz im formellen Sinn dazu ausdrücklich verpflichtet oder ermächtigt oder dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend

>

notwendig ist oder wenn im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf (§ 21 Abs. 2 revIDG).

Informationspflicht beim Beschaffen von (auch «gewöhnlichen») Personendaten

Ausweitung Das revidierte IDG weitet – wie europarechtlich schon seit 2010 vorgesehen[3] – die Informationspflicht aus (§ 15 revIDG). Öffentliche Organe müssen die Betroffenen aktiv informieren, wenn sie über diese Personendaten beschaffen (und nicht, wie bisher, nur, wenn sie besondere Personendaten beschaffen). Eine Beschaffung von Personendaten liegt vor, wenn ein öffentliches Organ aktiv und gewollt Kenntnis von Daten erlangt oder die Verfügung darüber begründet.

Der Aufwand für die Umsetzung der Informationspflicht ist überblickbar: In den meisten Fällen, reicht es, die entsprechenden Angaben auf dem Formular anzubringen.

Inhalt der Information Um Transparenz für die Betroffenen sicherzustellen, ist auch zu informieren, wenn die Daten bei Dritten, also bei anderen öffentlichen Organen oder Privaten (z.B. bei Personen, die im gleichen Haushalt leben, bei der Arbeitgeberin, bei einer Versicherung usw.) beschafft werden. Die Betroffenen sind nach § 15 Abs. 2 revIDG insbesondere zu informieren über:

— das verantwortliche öffentliche Organ (samt Kontaktdaten) (lit. a);

— die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten (lit. b);

— die Rechtsgrundlage der Datenbearbeitung (lit. c);

— den Zweck der Datenbearbeitung (lit. c);

— die Datenempfänger:innen oder die Kategorien der Datenempfänger:innen (wenn die Daten weitergegeben werden) (lit. d) und

— die Rechte der betroffenen Person (lit. e).

Form der Information Der Aufwand für die Umsetzung dieser Informationspflicht ist überblickbar: In den meisten Fällen, nämlich überall dort, wo Personendaten systematisch, beispielsweise auf einem Anmelde- oder Gesuchsformular – ob auf Papier oder auf einem Web-Formular – erhoben werden, reicht es, die entsprechenden Angaben auf dem Formular anzubringen.[4] Wo Daten durch Mitarbeiter:innen in einem Gespräch erhoben werden, kann die Information durch die (vorgängige oder gleichzeitige) Aushändigung eines Informationsschreibens erfolgen – es würde aber nicht reichen, eine Informationsbroschüre einfach beim Eingang zur Amtsstelle aufzulegen.

Keine Informationspflicht Die Informationspflicht entfällt:

— wenn die betroffene Person über die Information, die ihr zukommen müsste, bereits verfügt (insbesondere also, wenn sie in einer früheren Phase der Beschaffung bereits einmal informiert worden ist);

— wenn die Beschaffung oder Bekanntgabe der Personendaten gesetzlich ausdrücklich vorgesehen ist (d.h. wenn die betroffenen Personen aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden, sog. Fiktion der Gesetzeskenntnis), oder

— wenn die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist (wenn z.B. bei Dritten Daten einer Person, die sich ohne Adresse ins Ausland abgemeldet hat, beschafft werden müssten).

Einschränkungen der Informationspflicht Die Informationspflicht beim Erheben von Personendaten kann eingeschränkt werden. Dies ist unter den gleichen Voraussetzungen wie beim Zugang zu den eigenen Personendaten (§ 26 IDG) zulässig. Dafür ist § 29 IDG einschlägig. Er legt fest, dass das öffentliche Organ die Bekanntgabe von oder den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben hat, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht. Bisher sah § 15 Abs. 3 IDG vor, dass die Datenerhebung nur erkennbar sein muss, «soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird». Diese Einschränkung ist im neuen § 15 revIDG nicht mehr ausdrücklich vorgesehen. Die gleiche Wirkung wird aber über § 29 Abs. 2 lit. e IDG erreicht: Die Datenbekanntgabe ist einzuschränken, wenn sie «die zielkonforme Durchführung konkreter behördlicher,

insbesondere polizeilicher Massnahmen beeinträchtigt». Dabei ist auch der Grundsatz der Verhältnismässigkeit zu beachten: Einschränkungen sind nur zulässig, soweit und solange sie zum Schutz der Geheimhaltungsinteressen erforderlich sind. Nicht jeder noch so geringe Effekt und nicht jede noch so geringe Beeinträchtigung reicht aus, um ein Geheimhaltungsinteresse überwiegen zu lassen.[5] Und zeitlich: Sobald der Einschränkungsgrund wegfällt, ist die Information der betroffenen Person nachzuholen.

Meldepflicht bei Datenschutzverletzungen

Risiko für die betroffenen Personen Datenschutzverletzungen werden in der digitalen Welt des 21. Jahrhunderts zunehmend zu einem grösseren Problem. Wenn eine Verwaltungsstelle der Pflicht zur Sicherstellung der Informationssicherheit nicht nachkommt oder die getroffenen Massnahmen durch Systemfehler, durch Unachtsamkeit der Betreiber oder durch Angreifer ausgehebelt werden, tragen potenziell die betroffenen Personen den Schaden. Eine Verletzung des Schutzes von Personendaten kann, wenn nicht rechtzeitig und angemessen reagiert wird, einen physischen, materiellen oder immateriellen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre Personendaten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person. Zur Verbesserung der Transparenz werden weltweit Meldepflichten bei Datenschutzverletzungen eingeführt (*«Data breach notifications»*) – so auch durch die für Bund und Kantone verbindlichen europarechtlichen Rechtsakte.[6]

Nicht ganz neu Bisher kannte das IDG keine ausdrückliche Meldepflicht, doch wurde eine solche aus dem Grundsatz von Treu und Glauben abgeleitet.[7] Neu muss das verantwortliche öffentliche Organ eine Datenschutzverletzung ohne unangemessene Verzögerung *der oder dem DSB melden* (§ 16 Abs. 1). Ohne unangemessene Verzögerung bedeutet, dass eine Meldung in der Regel *spätestens innert 72 Stunden*, nachdem die Verletzung dem öffentlichen Organ bekannt geworden ist, zu melden ist.[8]

Zweck Mit der Meldepflicht soll sichergestellt werden, dass bei einer Datenschutzverletzung rechtzeitig und angemessen reagiert wird. Dafür muss ein solcher Vorfall – natürlich zusätzlich zur Information der eigenen vorgesetzten Stelle – primär der oder dem DSB gemeldet werden (§ 16a Abs. 1 revIDG), ausser wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt (Abs. 4). Allenfalls müssen auch die betroffenen Personen informiert werden – insbesondere dann, wenn sie selber Vorkehren zu ihrem Schutz treffen können (oder sogar müssen), indem sie beispielsweise Zugangsdaten oder Passwörter ändern.

Mit der neu eingeführten Meldepflicht soll sichergestellt werden, dass bei einer Datenschutzverletzung rechtzeitig und angemessen reagiert wird.

Datenschutzverletzung Eine Datenschutzverletzung liegt vor, wenn die Informationssicherheit so verletzt wird, dass bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten (§ 16a Abs. 3 revIDG). So stellen beispielsweise die folgenden Vorfälle Datenschutzverletzungen dar:

— ein erfolgreicher Hacker-Angriff auf eine Datenbank einer Dienststelle;

— ein Fehler bei der Anbindung eines Servers ans Internet, so dass plötzlich vertrauliche Bewerbungsdaten öffentlich zugänglich sind;

— der Versand einer Liste mit Daten über sonderpädagogische Bedürfnisse von Schüler:innen durch eine Schulleitung an alle Lehrer:innen einer Schule, auch an solche, die sie zur Aufgabenerfüllung nicht benötigen;

— der Versand von unverschlüsselten Nachrichten mit personenbezogenen Inhalten (Einsatzdaten von Blaulichtorganisationen), die dann in Echtzeit auf einer öffentlich zugänglichen Seite veröffentlicht werden;

— der Versand von unverschlüsselten sensitiven Daten über eine Klientin, die Zugang zu den eigenen Personendaten verlangt hat, an eine andere Person.

>

Inhalt der Meldung Zur Meldung gehören:

— die Beschreibung der Verletzung: Was ist geschehen? Wer ist betroffen?

— die Beschreibung der wahrscheinlichsten Folgen der Verletzung: Welches sind die Auswirkungen der Verletzung auf die staatliche Aufgabenerfüllung und – aus Datenschutzsicht: vor allem – auf die Grundrechte der betroffenen Personen?

— die Darstellung der Massnahmen, die zur Wiederherstellung des Schutzes bzw. zur Abmilderung der Folgen der Verletzung bereits getroffen worden sind oder getroffen werden sollen, so u.a.: Wie wird das Andauern der Verletzung verhindert? Wer wird informiert? Soll eine Strafanzeige eingereicht werden? Soll die Verletzung weiter untersucht werden (wobei zu beachten ist, dass mit Untersuchungshandlungen allenfalls Datenspuren und Beweise verwischt oder vernichtet werden können)?

Meldeformular Die oder der DSB wird auf der Website ein Meldeformular zur Verfügung stellen.

Aufgabe der/des DSB Aufgabe der oder des DSB ist es primär zu prüfen, ob rechtzeitig und angemessen auf die Verletzung reagiert wird. Im Fokus steht insbesondere die Frage, welches Risiko für die Grundrechte betroffener Personen besteht und welche weiteren Kommunikationsmassnahmen zu treffen sind, beispielsweise ob die betroffenen Personen und/oder die Öffentlichkeit zu informieren sind.

Bei Auftragsdatenbearbeitungen In diesen Fällen haben die Auftragsdatenbearbeiter:innen das auftraggebende öffentliche Organ *unverzüglich* zu informieren. Eine sehr rasche Information ist erforderlich, da das auftraggebende öffentliche Organ, das nach § 7 Abs. 2 IDG ja verantwortlich bleibt, seinerseits seinen Melde- und Informationspflichten in der Regel innert 72 Stunden nachkommen muss. Sinnvollerweise wird die Pflicht zur unverzüglichen Meldung – am besten mit einer einzuhaltenden Frist – im Vertrag mit den Auftragsdatenbearbeiter:innen festgehalten.

Ausnahmen von der Meldepflicht Die Meldepflicht entfällt nur, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt (§ 16a Abs. 4 revIDG). Da aber die Meldung an die/den DSB dem Zweck dient, aus einer Aussensicht zu prüfen, welches Risiko für die Grundrechte betroffener Personen besteht, darf auf die Meldung nur verzichtet werden, wenn mit Gewissheit feststeht, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt, beispielsweise weil der Datenabfluss bei einem Hacking noch verhindert werden konnte. Im Zweifelsfall ist die/der DSB beizuziehen.

Die Betroffenen sind zu informieren, wenn es die Umstände erfordern, beispielsweise wenn sie (oder sogar nur sie) Massnahmen ergreifen können (oder müssen), um einen Schaden durch die Datenschutzverletzung abzuwenden.

Information der betroffenen Personen Die betroffenen Personen sind zu informieren, wenn es die Umstände erfordern, beispielsweise wenn – wie oben erwähnt – sie (oder sogar nur sie) Massnahmen ergreifen können (oder müssen), um einen physischen, materiellen oder immateriellen Schaden durch die Datenschutzverletzung abzuwenden. Die Benachrichtigung kann hingegen unterbleiben, wenn durch nachträgliche Vorkehrungen sichergestellt werden konnte, dass das Risiko für die Grundrechte der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Wenn das öffentliche Organ nicht selber aufgrund der Umstände zum Schluss kommt, die betroffenen Personen zu informieren (oder dies im Moment der Meldung an die Aufsichtsstelle schon getan hat), kann die/der DSB verlangen, dass dies getan wird – nötigenfalls in Form einer Weisung nach § 47 IDG.

Einschränkung der Information der Betroffenen Die Benachrichtigung der betroffenen Personen kann unter den Voraussetzungen von § 29 IDG ganz oder teilweise unterbleiben oder aufgeschoben werden, also wenn eine besondere gesetzliche Geheimhaltungspflicht besteht oder öffentliche oder private Geheimhaltungsinteressen gegenüber dem Interesse der Betroffenen, über die Datenschutzverletzung informiert zu werden, überwiegen.

Stärkere Beachtung des zeitlichen Aspektes der Verhältnismässigkeit

Verhältnismässig Jedes Bearbeiten von Personendaten muss verhältnismässig sein (§ 9 Abs. 3 IDG). Verhältnismässig ist ein Datenbearbeiten, wenn es zur Erreichung des Zwecks (d.h. der Erfüllung der gesetzlichen Aufgabe) *geeignet* und *erforderlich* und den betroffenen Personen *zumutbar* ist.[9] Wenn der Zweck mit milderen Massnahmen (ganz ohne Personendaten, mit weniger Personendaten, mit Daten über weniger Personen, mit weniger sensitiven Daten[10], mit weniger lange aufbewahrten Personendaten) auch erreicht werden kann, ist die Erforderlichkeit nicht gegeben.

Auch zeitlich Insbesondere der zeitliche Aspekt der Erforderlichkeit wurde in der Vergangenheit oft zu wenig beachtet: Nach einer Querschnitts-Prüfung zu Datenlöschung und -vernichtung hat der DSB «anhand der von den Dienststellen zurückgemeldeten Informationen unter anderem festgestellt, dass die konzeptionellen Grundlagen bezüglich den Aufbewahrungsfristen weitgehend fehlen und in der Folge die Daten in der Mehrzahl der Systeme nicht gelöscht werden.»[11] Für die wenigsten Informationsbestände existierten demnach Aufbewahrungs- und Löschungskonzepte, geschweige denn Massnahmen, mit denen ein solches Konzept umgesetzt wird. Der unerwünschten Folge, dass Daten auch noch aufbewahrt wurden, wenn sie für die Erfüllung der gesetzlichen Aufgaben längst nicht mehr benötigt wurden, schiebt die IDG-Revision – gestützt durch die europarechtlichen Vorgaben[12] – nun einen Riegel.

Neu wird ausdrücklich festgehalten, dass Personendaten nur so lange bearbeitet werden dürfen, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist.

Pflicht, eine Frist festzulegen Neu wird ausdrücklich festgehalten, dass Personendaten nur so lange bearbeitet werden dürfen, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist (§ 9 Abs. 4 revIDG[13]). Ausserdem ist für jeden Informationsbestand, der Personendaten enthält, eine Frist festzulegen:

— für die Vernichtung beziehungsweise

— für die Überprüfung, ob die Daten zur Aufgabenerfüllung noch erforderlich sind (§ 16 Abs. 2 revIDG[14]).

Regelungsort Die Frist für die Archivierung oder Löschung/Vernichtung bzw. für die Überprüfung, ob die Personendaten für die Aufgabenerfüllung noch erforderlich sind, muss verbindlich, aber nicht zwingend auf Gesetzesstufe festgelegt werden. Dass das Archivrecht eine Anbietepflicht vorsieht, reicht für sich allein nicht.[15] Die Umsetzung selber kann auch in einem Datenschutzmanagementsystem (DSMS), wie es zum Nachweis der Einhaltung der Datenschutzvorschriften dient (§ 7 Abs. 3 revIDG), erfolgen.[16]

Nachweis der Datenschutzkonformität

Nachweispflicht In den neuen europarechtlichen Rechtsgrundlagen wird verlangt, dass die verantwortlichen öffentlichen Organe oder die Auftragsdatenbearbeiter:innen die Einhaltung der Datenschutzbestimmungen nachweisen können müssen.[17] Diese Pflicht wird neu in § 6 Abs. 3 revIDG übernommen.

Form des Nachweises Wie dieser Nachweis erbracht werden muss, ist nicht auf Gesetzesstufe festgelegt. Es soll kein bürokratischer Leerlauf geschaffen werden. Grössere Systeme können heute schon in verantwortlicher Weise nur mit einem *Datenschutzmanagementsystem (DSMS)* oder einem (um Datenschutzaspekte angereichertem) *Informationssicherheits-Managementsystem (ISMS)* betrieben werden. Diese Managementsysteme basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Für die Datenbearbeitungen, bei denen kein solches DSMS (oder angereichertes ISMS) geführt wird, ist festzulegen, welche Dokumente notwendig sind, um den erforderlichen Nachweis erbringen zu können (z.B. Informationssicherheits- und Datenschutzkonzept, Zugriffskonzept, Löschungskonzept usw.).

Konkretisierung auf Verordnungsstufe Der Regierungsrat muss für die Kernverwaltung auf Verordnungsstufe festlegen, in welchen Fällen ein solches DSMS (oder angereichertes ISMS) obligatorisch sein soll (z.B. wenn besondere Personendaten oder Personendaten, die einem Berufs- oder einem besonderen Amtsgeheimnis unterstehen, bearbeitet werden) bzw. wie der Nachweis für «kleinere» Systeme zu erbringen ist. Diese Regelung gilt auch für die Gerichte, die Gemeinden, die weiteren Körperschaften und die selbständigen Anstalten sinngemäss, soweit diese keine eigenen Regelungen erlassen, die dem Zweck

>

bereits bestehende Systeme wird zu bestimmen sein, bis wann das Nachweissystem bereitstehen muss (z.B. innert zweier Jahre nach Inkrafttreten des revIDG). Wenn eine betroffene Person oder die Aufsichtsbehörde vor Ablauf dieser Frist dies verlangt, muss der Nachweis selbstverständlich vorher schon erbracht werden.

Gestaltungsprinzipien «Privacy by design» / «Privacy by default»

Inbegriff des präventiven Datenschutzes Je mehr die Digitalisierung die staatliche Tätigkeit durchdringt, umso wichtiger wird es, die Technologie von Anfang an datenschutzkonform auszugestalten. Dazu dienen die beiden Gestaltungsprinzipien *«Privacy by design»* (Datenschutz durch Technikgestaltung) und *«Privacy by default»* (datenschutzfreundliche Voreinstellungen).[18] Sie sind gleichsam der Inbegriff des präventiven Datenschutzes, mit dem schon vorweg nach Möglichkeit verhindert werden soll, dass die Grundrechte der betroffenen Personen verletzt werden. Die bisher in § 14 IDG erwähnten Prinzipien der Datenvermeidung und Datensparsamkeit sind in den erwähnten Prinzipien mitenthalten.

Je mehr die Digitalisierung die staatliche Tätigkeit durchdringt, umso wichtiger wird es, die Technologie von Anfang an datenschutzkonform auszugestalten.

Datenschutz durch Technikgestaltung Das Prinzip *«Privacy by design»* (§ 14 Abs. 1 revIDG) verlangt, dass bei Datenbearbeitungen von Anfang an Massnahmen getroffen werden, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen.[19] Das bedeutet, dass eine Aufgabenerfüllung, wenn dies möglich ist, im Sinne der Datenvermeidung als Ausfluss des Verhältnismässigkeitsprinzips ganz ohne Personendaten, mit weniger Personendaten, mit Daten über weniger Personen, mit weniger sensitiven Daten[20] oder mit weniger lang aufbewahrten Personendaten erfolgt, dass technische Möglichkeiten wie die Anonymisierung oder Pseudonymisierung genutzt werden und dass weitere datenschutzfreundliche Technologien («Privacy enhancing technologies»/PET) verwendet werden. Umzusetzen ist dies etwa dadurch, dass Personendaten nur erhoben werden, wenn eine Rechtfertigung dafür besteht, dass nur die für die Aufgabenerfüllung tatsächlich erforderlichen Personendaten überhaupt erhoben werden, dass Randdaten, die bei der Nutzung von IT-Systemen anfallen, nicht gespeichert, möglichst rasch anonymisiert oder mindestens pseudonymisiert werden oder dass die Zweckänderung der Datenbearbeitung verhindert wird. Beispielsweise muss der Download von Informationen von einer staatlichen Website anonym möglich sein; bei Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen muss es möglich sein, die Angabe des Standortes manuell vorzunehmen (und nicht einfach durch eine automatische Ortung durch das Handy). Wenn solche grundrechtsschonenden Möglichkeiten nicht bestehen, werden die Grundrechte der betroffenen Personen unnötigerweise verletzt – und wenn diese Möglichkeiten nicht von Anfang an in den Systemen und Anwendungen eingebaut sind, ist es oft nicht mehr möglich oder sehr viel aufwändiger, dies nachträglich zu tun.

Datenschutzfreundliche Voreinstellungen Das Prinzip *«Privacy by default»* (§ 14 Abs. 2 revIDG) verlangt, dass bei Datenbearbeitungen die Voreinstellungen datenschutzfreundlich gewählt werden.[21] Die betroffene Person soll sich nicht durch Einstellungen kämpfen müssen, um ihr Grundrecht auf informationelle Selbstbestimmung zu schützen. Die Voreinstellungen sollen ihre Selbstbestimmung schützen und nur die Erfassung der absolut notwendigen Daten zulassen. Die betroffene Person soll selber bestimmen, wenn sie eine weiter gehende Einschränkung ihres Grundrechts zulassen will (Opt-in anstelle von Opt-out). Am Beispiel der Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen: In den Voreinstellungen darf der Standortdienst nicht aktiviert sein. Die Benutzerin oder der Benutzer muss diesen selber aktivieren, wenn sie oder er ihn nutzen will (z.B. mit einer Option «Ortung des Handys nutzen»).

Datenschutz-Folgenabschätzung als Vorbereitung der Vorabkonsultation

Nicht ganz neu Das revidierte IDG verpflichtet die öffentlichen Organe zu einer Datenschutz-Folgenabschätzung (DSFA, § 12a revIDG). Diese Bestimmung ist zwar neu – das, was zu tun ist, aber nicht. Denn die DSFA ist im Grunde genommen nichts anderes als das, was die öffentlichen Organe schon bisher zur Vorbereitung der Vorabkontrolle (§ 13 IDG) tun mussten. Weiteres dazu sogleich auf der nächsten Seite und vor allem im letzten Tätigkeitsbericht[22].

Weitere neue Regelungen

Gesamtverantwortung Wenn mehrere öffentliche Organe einen gemeinsamen Informationsbestand bearbeiten, muss neu festgelegt werden, welches öffentliche Organ die Gesamtverantwortung trägt (§ 6 Abs. 2 revIDG). Das gesamtverantwortliche öffentliche Organ muss nicht für alles die Verantwortung übernehmen, aber dafür sorgen, dass alle Teile der Verantwortung einer Stelle zugewiesen sind, und sich vergewissern, dass diese teilverantwortlichen Stellen ihre Verantwortung wahrnehmen. Als Beispiel: Die KOI trägt nach der Datenmarktverordnung (DMV)[23] die Gesamtverantwortung für den kantonalen Datenmarkt. Sie koordiniert die Nutzung des Gesamtsystems und erlässt Vorgaben für die Nutzung.[24] Die DMV weist ihr bestimmte Aufgaben zu, in den folgenden Bestimmungen aber auch anderen öffentlichen Organen, z.B. den dateneinliefernden Stellen.

Subcontracting Auftragsdatenbearbeiter:innen dürfen ohne vorgängige schriftliche Zustimmung der auftraggebenden öffentlichen Organe für die Auftragsdatenbearbeitung keine Unterauftragnehmer:innen beiziehen (§ 7 Abs. 3 revIDG). Ein Verstoss gegen diese Bestimmung wird mit Busse bestraft (§ 51 Abs. 1 lit. b revIDG).

Vorabkonsultation Nach § 13 Abs. 2 revIDG erstellt (und veröffentlicht) die/der DSB eine Liste der Bearbeitungsvorgänge, die zur Vorabkonsultation zu unterbreiten sind. Sie ergänzt die Umschreibung in § 13 Abs. 1 lit. b revIDG («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») und die Konkretisierung in § 2 Abs. 1 IDV.[25] Damit kann spezifischer festgelegt werden, wann eine Vorabkonsultation in jedem Fall erforderlich ist, indem z.B. neue Technologien erfasst werden: bei automatisierten Einzelentscheidungen ohne Mitwirkung von Menschen, bei Robotic Process Automation, bei systematischer Überwachung (etwa bei der Verwendung von Überwachungstools [wie Google Analytics], bei denen die Personendaten nicht vor der Übermittlung anonymisiert werden, bei denen nicht vor der Übermittlung eine informierte Einwilligung der Betroffenen eingeholt wird und bei denen die Erteilung der Einwilligung ohne Einschränkung der Funktionalität nicht verweigert werden kann).

Inhalt des Zugangs zu den eigenen Personendaten Jede Person hat Anspruch darauf zu erfahren, ob bei einem öffentlichen Organ Personendaten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten (§ 26 IDG). Die europarechtlichen Rechtsgrundlagen[26] legen präziser fest, welche Informationen einer gesuchstellenden Person bei einem Gesuch um Zugang zu den eigenen Personendaten zugänglich zu machen sind. Offenzulegen sind der gesuchstellenden Person insbesondere die verfügbaren Angaben darüber, woher die Daten stammen. Auf diesem Weg kann diese, wenn die Daten unrichtig sind, sich mit dem Berichtigungsanspruch an die Quelle der Unrichtigkeit wenden. Ausserdem sind – quasi als «Metadaten» zu den erwähnten Personendaten über die gesuchstellende Person – die Angaben mitzuliefern, über die nach der Transparenzbestimmung (der Pflicht zur aktiven Information die betroffene Person bei der Datenerhebung nach dem neuen § 15 Abs. 2 revIDG) ohnehin schon zu informieren ist.[27]

Regelungen neu auf Gesetzesstufe

Hinweise Zuletzt soll noch auf ein paar weitere Regelungen hingewiesen werden, die früher auf Verordnungsstufe geregelt waren, jetzt auf Gesetzesstufe gehoben werden oder nun auf Gesetzesstufe konkretisiert werden.

Vergewisserungspflicht bezüglich der Richtigkeit Aus dem bisher geltenden Gesetzestext ging nicht hervor, was die Anforderung der Richtigkeit bedeutet.[28] In Übereinstimmung mit der Regelung im Bundes-DSG werden nun die Handlungspflichten klar benannt:[29] Das öffentliche Organ, das zur Aufgabenerfüllung Personendaten bearbeitet, muss sich vergewissern, ob die Daten richtig sind. Der Umfang dieser Vergewisserungspflicht ist im Einzelfall zu bestimmen. Stammen die Daten von der betroffenen Person selber, dann darf das öffentliche Organ – aus datenschutzrechtlicher Sicht – auf die Richtigkeit vertrauen, muss also keine zusätzlichen Prüfschritte unternehmen. In einem solchen Fall kann aber aus anderen Gründen eine vertiefte Prüfung angezeigt sein, etwa wenn mit den Daten das Bestehen eines Anspruchs auf eine staatliche Leistung behauptet wird. Die betroffene Person kann dabei eine Mitwirkungspflicht treffen, etwa wenn sich ursprünglich richtig erfasste Daten nachträglich aufgrund von Umständen, die die Behörde nicht kennen kann, als unrichtig erweisen. >

Zeitpunkt der Vergewisserung Die Vergewisserungspflicht greift nicht permanent, sondern nur, wenn die Personendaten aktiv bearbeitet werden. Wenn ein öffentliches Organ Personendaten zur Aufgabenerfüllung erhebt, muss es die Daten allenfalls noch über die Phase der eigentlichen Aufgabenerfüllung hinaus weiter aufbewahren, weil eine solche Aufbewahrungsfrist gesetzlich vorgesehen ist oder weil die Aufbewahrung zu Beweis- und Sicherungszwecken erforderlich ist. In dieser «inaktiven» Phase muss sich das öffentliche Organ nicht permanent vergewissern, ob die Daten noch richtig sind oder allenfalls unrichtig geworden sind. Die Vergewisserungspflicht lebt erst wieder auf, wenn die Daten wieder aktiv bearbeitet werden, wenn sie also beispielweise erneut für die Prüfung gebraucht werden, ob ein Leistungsanspruch besteht, oder wenn bei einer andauernden Leistung geprüft werden soll, ob der Anspruch noch zu Recht besteht.[30]

Massnahmen bezüglich Berichtigung bzw. Vernichtung Nach dem ebenfalls neu eingefügten § 11 Abs. 3 revIDG muss das verantwortliche öffentliche Organ alle angemessenen Massnahmen treffen, damit Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.[31] Wenn sich Personendaten als unrichtig herausstellen, dann ist dafür zu sorgen, dass die Korrektur – die Berichtigung oder die Löschung nach § 27 IDG – auch umgesetzt werden kann.[32] Bei Papierdossiers ist dies einfacher zu bewerkstelligen, bei IT-Systemen muss das mit angemessenen Massnahmen sichergestellt werden. Wenn beispielsweise bei einem IT-System wegen der Revisionstauglichkeit (unrichtige) Einträge nicht einfach durch die richtigen Einträge ersetzt werden können, ist auf andere Weise sicherzustellen, dass die Berichtigung umgesetzt wird, etwa durch spätere Ergänzungen, die mit dem ursprünglichen Eintrag verknüpft werden, wie das etwa beim Rapportsystem der Kantonspolizei der Fall ist. Gleichzeitig wird mit dem neuen Gesetzestext auch festgehalten, dass es nicht um eine «absolute» Richtigkeit und Vollständigkeit geht, sondern um Richtigkeit und Vollständigkeit im Hinblick auf dem Zweck der Beschaffung bzw. Bearbeitung der Personendaten.

Veröffentlichung der Videoüberwachungsreglemente Ergänzt wurden auch die §§ 17 und 18 IDG betreffend die Videoüberwachung. Durch § 17 Abs. 1 IDG wird Videoüberwachung zum Schutz von Personen oder Sachen vor strafbaren Handlungen bzw. zur Verfolgung solcher strafbarer Handlungen generell erlaubt. Die einzelnen Videoüberwachungsanlagen sind jedoch nicht auf Gesetzes- oder Verordnungsstufe geregelt, die Betroffenen können sich also nicht über die Gesetzessammlung informieren, wo solche Anlagen bestehen. Deshalb ist es unerlässlich, dass die Reglemente für die einzelnen Videoüberwachungsanlagen öffentlich zugänglich sind. Die Pflicht zur Veröffentlichung (im Internet) war bisher nur in der IDV geregelt (§ 6 Abs. 1 IDV). Sie wird nun auf Gesetzesstufe gehoben (§ 18 Abs. 4bis revIDG). Gleichzeitig sollen – aufgrund der Erfahrungen mit der Umsetzung der Verordnungsbestimmung (§ 6 Abs. 2 IDV) – die Ausnahmen von der Veröffentlichungspflicht etwas erweitert werden. Da mit diesen Ausnahmen die zum Schutz der Grundrechte notwendige Transparenz für die betroffenen Personen eingeschränkt wird, werden auch diese Ausnahmen neu auf Gesetzesstufe verankert (§ 18 Abs. 4ter revIDG).

Das revidierte IDG kann hoffentlich noch in diesem Herbst in Kraft gesetzt werden! Immerhin geht es ja darum, den Grundrechten der Menschen in unserem Kanton besser zum Durchbruch zu verhelfen.

Eingeschränkte Veröffentlichungspflicht § 6 Abs. 2 IDV sah, als Ausnahme von der Veröffentlichungspflicht nach § 6 Abs. 1 IDV, schon bisher vor, dass auf die Veröffentlichung der Kamerastandorte verzichtet werden kann, soweit durch deren Bekanntgabe die *Zweckerreichung verunmöglicht* wird. In der Praxis hat sich gezeigt, dass nicht nur die Veröffentlichung der Kamerastandorte, sondern auch weiterer Einsatzdetails die Zweckerreichung vereiteln kann. Wenn etwa der Zugang zu einem zu schützenden Objekt nur von 22 bis 5 Uhr überwacht wird, kann das dazu führen, dass jemand knapp vor 22 Uhr oder just nach 5 Uhr einzudringen versucht. Aus diesem Grund soll auch auf die Veröffentlichung weiterer Einsatzdetails verzichtet werden können, wenn deren Bekanntgabe die Zweckerreichung verunmöglicht. Im Rahmen der Vorabkonsultation vor Erlass oder Verlängerung eines Videoüberwachungsreglements kann die/der DSB prüfen, ob eine solche Ausnahme gerechtfertigt ist.

Inhalt des Zugangs zu den eigenen Personendaten Jede Person hat Anspruch darauf zu erfahren, ob bei einem öffentlichen Organ Personendaten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten (§ 26 IDG). Die europarechtlichen Rechtsgrundlagen[33] legen präziser fest, welche Informationen einer gesuchstellenden Person bei einem Gesuch um Zugang zu den eigenen Personendaten zugänglich zu machen sind. Offenzulegen sind der gesuchstellenden Person insbesondere die verfügbaren Angaben darüber, woher die Daten stammen. Auf diesem Weg kann diese, wenn die Daten unrichtig sind, sich mit dem Berichtigungsanspruch an die Quelle der Unrichtigkeit wenden. Ausserdem sind – quasi als «Metadaten» zu den erwähnten Personendaten über die gesuchstellende Person – die Angaben mitzuliefern, über die nach der Transparenzbestimmung (der Pflicht zur aktiven Information die betroffene Person bei der Datenerhebung nach dem neuen § 15 Abs. 2 revIDG) ohnehin schon zu informieren ist.[34]

Fazit

Wieder aktuell Mit dieser Revision wird das baselstädtische IDG wieder die Anforderungen der modernisierten europarechtlichen Anforderungen erfüllen. Als nächstes ist die IDV dem revidierten IDG anzupassen. Zurzeit laufen die entsprechenden Vorbereitungsarbeiten.

Inkrafttreten Nach den neuesten Informationen soll die Vernehmlassung zur IDV-Revision noch vor den Sommerferien durchgeführt werden. Es ist zu hoffen, dass die diese Revision zügig abgeschlossen wird. Sobald dies der Fall ist, kann das IDG in Kraft gesetzt werden – hoffentlich noch in diesem Herbst.[35] Immerhin geht es darum, den Grundrechten der Menschen in unserem Kanton besser zum Durchbruch zu verhelfen.

1 Das gilt auch umgekehrt: Nach dem revidierten Bundesdatenschutzgesetz dürfen Personendaten ohne Weiteres nur «ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet» (Art. 16 Abs. 1 revDSG).
2 Art. 3 Ziff. 12 und 13 und Art. 10 der Richtlinie (EU) 2016/680; Art. 6 Abs. 1 der Europarats-Konvention 108+.
3 Nun: Art. 13 der Richtlinie (EU) 2016/680; Art. 7bis der Europarats-Konvention 108+.
4 Wie bisher schon bei systematischen Erhebungen nach § 15 Abs. 2 IDG.
5 PK-IDG/BS-Rudin, § 29 N 18 ff., insb. N 19.
6 Art. 30 f. der Richtlinie (EU) 2016/680; Art. 7 Ziff. 2 der Europarats-Konvention 108+.
7 PK-IDG/BS-Rudin, § 9 N 50.
8 Art. 30 Abs. 1 der Richtlinie (EU) 2016/680.
9 Vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 ff.
10 Nach § 3 Abs. 4 lit. a revIDV werden die «Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht» neu als «sensitive Personendaten» bezeichnet.
11 Vgl. TB 2015 des DSB/BS, 33.
12 Art. 5 der Richtlinie (EU) 2016/680; Art. 5 Ziff. 4 lit. e der Europarats-Konvention 108+.
13 Ratschlag 21.1239.01, S. 17 f.
14 Ratschlag 21.1239.01, S. 31 f.
15 § 7 Archivgesetz; §§ 21 ff. RAV.
16 Ratschlag 21.1239.01, S. 31 f.
17 Art. 4 Abs. 4 der Richtlinie (EU) 2016/680; Art. 10 Abs. 1 der Europarats-Konvention 108+.
18 Art. 20 der Richtlinie (EU) 2016/680.
19 Ratschlag 21.1239.01, S. 27.
20 Siehe Fn. 10.
21 Ratschlag 21.1239.01, S. 28.
22 TB 2020/2021 des DSB/BS, S. 14 ff.
23 § 3 Abs. 1 DMV.
24 § 3 Abs. 2 DMV; detaillierter sind ihre Aufgaben in § 3 Abs. 3 DMV aufgeführt.
25 Aktuell: Bei Abrufverfahren, bei der Bearbeitung besonderer Personendaten, beim Einsatz neuer Technologie, bei einer grossen Anzahl betroffener Personen, bei Datenpools im Sinn von § 1a IDV bzw. wenn ein Gesetz oder eine Verordnung es vorsieht. Die IDV muss aber noch dem revIDG angepasst werden.
26 Art. 14 der Richtlinie (EU) 2016/680 (ebenso wie Art. 15 Abs. 2 der Verordnung [EU] 2016/679); Art. 9 Abs. 1 lit. b der Europarats-Konvention 108+.
27 Ratschlag 21.1239.01, S. 40.
28 Vgl. aber Ratschlag 08.0637.01, S. 26; PK-IDG/BS-Rudin, § 11 N 11 ff.
29 Ratschlag 21.1239.01, S. 21.
30 PK-IDG/BS-Rudin, § 11 N 12.
31 Ratschlag 21.1239.01, S. 21.
32 PK-IDG/BS-Rudin, § 11 N 13.
33 Art. 14 der Richtlinie (EU) 2016/680 (ebenso wie Art. 15 Abs. 2 der Verordnung [EU] 2016/679); Art. 9 Abs. 1 lit. b der Europarats-Konvention 108+.
34 Ratschlag 21.1239.01, S. 40.
35 Die schengen-relevante Richtlinie (EU) 2016/680 wurde der Schweiz am 1. August 2016 notifiziert. Die zweijährige Frist zur Umsetzung, also zur Anpassung der (Informations- und) Datenschutzgesetze von Bund und Kantonen lief demnach am 1. August 2018 ab – also vor bald fünf Jahren.

Trend 2 Revidiertes IDG: Unterstützung durch die Datenschutzberater:innen

Der Grosse Rat hat beschlossen, dass nicht nur im engen «Schengen-Bereich» Datenschutzberater:innen bezeichnet werden müssen. Sie sollen insbesondere bei der Datenschutz-Folgenabschätzung (DSFA), also bei der Vorbereitung der (seit 2008 vorgeschriebenen) Vorabkonsultation (bisher: Vorabkontrolle) unterstützen. Es gilt, die Chance zu packen, welche die Datenschutzberater:innen bieten – auf dem Weg zur digitalen Verwaltung, damit nicht die betroffenen Einwohner:innen in unserem Kanton den Preis dafür mit einer Gefährdung ihrer Grundrechte bezahlen.

IDG-Revision

Ausgangslage Wie erwähnt (vorne S. 9) hat der Grosse Rat auf Antrag der JSSK beschlossen, dass – zur Erfüllung der europarechtlichen Vorgaben – nicht bloss die Kantonspolizei, die Staatsanwaltschaft und der Justizvollzug Datenschutzberater:innen bezeichnen müssen.

Datenschutzberater:innen

Europarechtliche Vorgaben Die *Richtlinie* (EU) 2016/680 schreibt vor, dass die öffentlichen Organe, die im Schengen-Bereich Personendaten bearbeiten, «einen Datenschutzbeauftragten» benennen (Art. 32 Abs. 1 RL (EU) 2016/680). Ausführlich gibt die Richtlinie auch die Stellung und die Aufgaben dieser Organe vor (Art. 33 und 34 RL (EU) 2016/680). Eine ähnliche Regelung enthält die *Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO)* in ihren Art. 37–39. Hier trifft diese Pflicht alle datenbearbeitenden öffentlichen Stellen (nur bei ihrer justiziellen Tätigkeit sind die Gerichte ausgenommen).

«Datenschutzbeauftragte» Dieser Begriff bezeichnet in der EU-Terminologie nicht dasselbe wie in der schweizerischen Gesetzgebung: Die Datenschutzbeauftragten nach dem schweizerischen Recht heissen im EU-Recht «unabhängige Aufsichtsbehörden». Die «Datenschutzbeauftragten» nach EU-Recht sind in der Schweiz die Datenschutzberater:innen; der Bund nennt sie in seiner Verordnung zum Datenschutzgesetz (VDSG) seit der Revision von 2007 «Berater für den Datenschutz» (Art. 23 VDSG).

Ratschlag

Beschränkte Einrichtung Im Ratschlag 21.1239.01 wurde die Frage gestellt, ob die Funktion der Datenschutzberater:innen (DSBer) generell für alle öffentlichen Organe oder mindestens für alle Departemente und die Gemeinden vorgeschrieben werden soll. Der DSB, der den Ratschlagsentwurf dem Präsidialdepartement im Januar 2019 abgeliefert hatte, schlug damals vor: «Angesichts der Tatsache, dass die Dienststellen mit den umfangreichsten Datenbearbeitungen schon heute interne Ansprechpersonen bezeichnet haben, erscheint die Pflicht, für jedes öffentliche Organ oder mindestens für jedes Departement und jede Gemeinde eine Datenschutzberaterin oder einen Datenschutzberater einzusetzen, als unverhältnismässig. Deshalb wird darauf verzichtet»[1].

Interne Vernehmlassung Von einem öffentlichen Organ, das seit mehreren Jahren über eine:n DSBer verfügt, wurde betont, wie hilfreich es sei, über eine Person mit datenschutzrechtlichem Spezialwissen zu verfügen. Für die anderen Vernehmlassungsteilnehmer:innen war dies kein Thema. Darum wurde mit dem regierungsrätlichen Entwurf nur beantragt, die Pflicht im Zusammenhang mit der justiziellen und polizeilichen Zusammenarbeit umzusetzen, also für die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde.[2]

Behandlung im Grossen Rat

Minimalvariante hinterfragt Während der Beratung des Ratschlags in der JSSK wurde die vorgeschlagene Minimalvariante in Frage gestellt. Und da ist der DSB aufgrund der Erfahrungen aus den vier Jahren seit der Ablieferung des Ratschlagsentwurfs zu einer anderen Erkenntnis gelangt. Es gibt nur in einzelnen wenigen Organisationseinheiten für den Datenschutz zuständig erklärte Mitarbeiter:innen. So ist es leider in keiner Weise garantiert, dass bei den datenschutzrelevanten Projekten in einem Departement jemand mit

fundiertem Know-how involviert ist.[3] Deshalb hat der DSB den Antrag, die «Einführung» von DSBer über den engen «Schengen-Bereich» hinaus zu prüfen, unterstützt und im Auftrag der JSSK und in Abstimmung mit dem Präsidialdepartement eine «Auslegeordnung» mit Alternativvarianten zur Ratschlags-Minimalvariante vorgenommen.

Maximalvariante: generelle Pflicht Eine erste Alternativvariante könnte darin bestehen, dass alle Departemente der kantonalen Verwaltung, die Bereiche, Abteilungen und Stabsstellen[4], die Gerichte, die Gemeinden und die weiteren juristischen Personen des kantonalen und kommunalen öffentlichen Rechts – unabhängig von der Grösse der Organisationseinheit, von der Sensitivität oder Menge der bearbeiteten Personendaten – eigene DSBer zu bezeichnen hätten. Diese Maximalvariante hat der DSB (übereinstimmend mit dem Präsidialdepartement) auch weiterhin als unverhältnismässig beurteilt und deshalb nicht empfohlen.

Einige Dienststellen haben aus der Einsicht, dass das interne Bündeln des Datenschutz-Knowhows notwendig ist, auch schon von sich aus betriebliche Datenschutzbeauftragte, eben Datenschutzberater:innen, bezeichnet.

Mittlere Variante: differenzierte Pflicht Weniger weit geht es, die Pflicht zur Benennung von DSBer an bestimmte Kriterien zu knüpfen. Denkbar sind verschiedene Anknüpfungskriterien, aber nicht alle sind praktikabel: Die Grösse der Organisationseinheit, die Datenart (besondere Personendaten i.S.v. § 3 Abs. 4 revIDG), die Datenbearbeitungsart (Profiling i.S.v. § 3 Abs. 7 revIDG) oder die Zahl der betroffenen Personen berücksichtigen entweder die Sensitivität der Datenbearbeitung nicht, sind per se keine stabilen Kriterien oder häufig vorweg nicht zuverlässig eruierbar. Umsetzbar ist hingegen das Anknüpfen an der Organisation. Wenn mindestens bei allen kantonalen Departementen, bei den Gerichten und bei den Gemeinden ein:e DSBer bezeichnet wird, wäre sichergestellt, dass für jede Datenbearbeitung ein:e DSBer zuständig ist. Allerdings wäre es viel zweckmässiger, diese Beratung und Unterstützung «näher» an die datenschutzrelevanten Datenbearbeitungen zu bringen. Aus diesem Grund sollten auch die Bereiche, Abteilungen und Stabsstellen, bei denen tendenziell ein höherer Beratungs- und Unterstützungsbedarf anfällt, verpflichtet werden, eigene DSBer zu bezeichnen – und einige davon haben aus der Einsicht, dass das interne Bündeln des Datenschutz-Knowhows notwendig ist, auch schon von sich aus betriebliche Datenschutzbeauftragte, eben DSBer, bezeichnet.

Antrag der JSSK Das Präsidialdepartement hat weiterhin am Antrag des Regierungsrates festgehalten und sah – anders als der DSB – keinen Handlungsbedarf für die Bezeichnung von zusätzlichen DSBer.[5] Die JSSK hat jedoch nach ausführlicher Diskussion beschlossen, dem Grossen Rat zu beantragen, dass

— die *Departemente* der kantonalen Verwaltung, die *Gerichte* und die *Einwohner- und Bürgergemeinden* je mindestens eine:n DSBer bezeichnen müssen und

— der Regierungsrat darüber hinaus verpflichtet wird, zusätzlich die *Bereiche, Abteilungen und Stabsstellen* der kantonalen Verwaltung sowie die *öffentlich-rechtlichen Anstalten des kantonalen Rechts* zu bestimmen, die eigene DSBer zu bezeichnen haben.[6]

Beschluss des Grossen Rates Der Grosse Rat ist am 20. Oktober 2022 vollumfänglich dem Antrag seiner Kommission gefolgt.

Verpflichtete Organisationseinheiten

Von Gesetzes wegen Direkt von § 16b Abs. 1 revIDG verpflichtet, für ihren Zuständigkeitsbereich DSBer zu bezeichnen, werden:

— die *Departemente* der kantonalen Verwaltung,

— die *Gerichte* (aber nicht jedes einzelne Gericht) und

— die *Einwohner- und Bürgergemeinden*.

Vom Regierungsrat zu verpflichten Bei der Bestimmung der zusätzlichen *Bereiche, Abteilungen und Stabsstellen* der kantonalen Verwaltung sowie die *öffentlich-rechtlichen Anstalten des kantonalen Rechts*, die selber DSBer zu bezeichnen haben, muss der Regierungsrat nach § 16b Abs. 2 revIDG die Art und Menge der von diesen Organisationseinheiten bearbeiteten Personendaten berücksichtigen. Darunter fallen sicher schon mal die Dienststellen, die schon nach dem Ratschlag DSBer hätten bezeichnen müssen, also die Staatsanwaltschaft, die Kantonspolizei und der Justizvollzug. Die weiteren Dienststellen sollen auf der Basis von *Risikoüberlegungen* bestimmt werden: Welche Dienststellen bearbeiten *regelmässig sensitive Personendaten*[7], also insbesondere Angaben über (im weitesten Sinne) die Gesundheit (inkl. genetische Daten), die soziale Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen oder biometrische Daten? >

Aufgaben der Datenschutzberater:innen

Gesetzliche Aufgaben Die DSBer beraten und unterstützen die öffentlichen Organe in ihrem Zuständigkeitsbereich bei der Bearbeitung von Personendaten, unterstützen sie bei der Vornahme der Datenschutz-Folgenabschätzung und arbeiten mit der/dem DSB zusammen (nach § 16b Abs. 3 revIDG).

Neue Aufgaben?

Nein Dem Argument, aufgrund dieser Bestimmung müssten neue Stellen geschaffen werden, kann nicht gefolgt werden. Vielleicht müssen neue Stellen geschaffen werden – aber *nicht aufgrund dieser Bestimmung*. Es werden keine neuen Aufgaben statuiert. Alle Aufgaben, die in § 16b Abs. 3 revIDG beschrieben werden, mussten schon bisher erfüllt werden bzw. hätten schon bisher erfüllt werden müssen:

— *Beratung und Unterstützung beim Bearbeiten von Personendaten:* «First level support» mussten die öffentlichen Organe schon bisher beim zuständigen Rechtsdienst und bei der/dem Informationssicherheitsbeauftragten Departement (ISBD) holen. Es ist – wie im letzten Tätigkeitsbericht[8] erwähnt – z.B. nicht Aufgabe des DSB, Rechtsgrundlagenanalysen, Schutzbedarfsanalysen oder Informationssicherheits- und Datenschutzkonzepte (ISDS-Konzepte) zu erstellen.

— *Unterstützung bei der Vornahme der Datenschutz-Folgenabschätzung:* Die DSFA ist zwar neu in § 12a revIDG verankert, sie ist aber, wie der Regierungsrat im Ratschlag 21.1239.01 selber festhält, keine neue Aufgabe. Die DSFA ist nichts anderes als die Vorbereitung der Vorabkonsultation (§ 13 revIDG, bisher § 13 IDG unter dem Namen «Vorabkontrolle»). Seit anderthalb Jahrzehnten, nämlich seit dem 1. Juni 2008 sind öffentliche Organe verpflichtet, Bearbeitungen von Personendaten vorab der oder dem DSB zur Kontrolle vorzulegen, wenn sie aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet sind, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen.[9]

— *Zusammenarbeit mit der/dem DSB:* Auch das ist keine neue Aufgabe.

Aufgaben bisher nicht überall erfüllt All dies war also schon vorher zu tun. Wenn es jetzt neue Ressourcen braucht, dann offensichtlich deshalb, weil diese Aufgaben – zur Wahrung der Grundrechte der Menschen in unserem Kanton – bis heute nicht oder nicht in genügendem Umfang wahrgenommen worden sind.

Dringender Bedarf der Dienststellen Was der Datenschutzbeauftragte festgestellt und in den letzten Tätigkeitsberichten dargelegt hat: Es besteht ein dringender Bedarf bei Bereichen, Abteilungen und Stabsstellen der kantonalen Verwaltung sowie bei den öffentlich-rechtlichen Anstalten des kantonalen Rechts, dass Datenbearbeitungen – laufende und erst recht künftige, geplante! – datenschutzkonform erfolgen. Moderne Projektmanagement-Systeme (wie z.B. Hermes) haben das erkannt und aufgenommen. Die Digitalisierung soll zu mehr digitalen Lösungen führen – mit allen Risiken, die digitale Lösungen mit sich bringen. Und mit diesen Risiken sind nicht die «üblichen» Projektrisiken gemeint: dass die Kosten explodieren, dass das beauftragte Unternehmen in Konkurs fällt, dass die Projektleiterin ausfällt oder dass sich ein Erdbeben ereignet. Hier geht es um die Risiken für die Menschen, über die (digital) Daten bearbeitet werden: wenn beispielsweise ihre Daten unwiederbringlich vernichtet werden oder verloren gehen, wenn ihre Daten unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder wenn Unbefugte Zugang zu ihren Daten erhalten. Um diese Risiken zu vermeiden oder auf ein tragbares Mass zu verringern, brauchen die öffentlichen Organe Knowhow – technisches, aber eben auch rechtliches. Wenn der DSB Projektdokumentationen zurückweisen muss, weil sie unvollständig oder nicht richtig ausgefüllt sind, dauern Projekte länger und werden sicher nicht günstiger, wenn nachträglich Änderungen vorgenommen werden müssen.

Alle Aufgaben, die den Datenschutzberater:innen aufgetragen werden, mussten schon bisher erfüllt werden bzw. hätten schon bisher erfüllt werden müssen.

Die Idee hinter den Datenschutzberater:innen

Was ist das Ziel? Mit der Funktion der DSBer soll das Knowhow gebündelt werden, das (schon bisher) zur Erfüllung der Pflichten und Aufgaben nach IDG notwendig war. Statt dass in einer Dienststelle einzelne Mitarbeiter:innen ab und zu mal mit Datenschutzfragen konfrontiert werden (und, wenn sie selten damit zu tun haben, bei spezifischen Fragen recht schnell überfordert sind), soll das Knowhow zusammengefasst werden. Das soll sicher auf Departementsebene geschehen, bei den Dienststellen, die regelmässig sensitive oder sehr viele Personendaten bearbeiten, auf Dienststellenebene.

Ausbildung und Erfahrung Die europarechtlichen Vorgaben[11] nennen als Voraussetzungen für die Benennung als DSBer die berufliche Qualifikation und das Fachwissen, das sie auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzen. Durch die Knowhow-Bündelung lohnt es sich auch, in die Aus- und Weiterbildung dieser DSBer zu investieren, und sie können auch besser Erfahrungen sammeln, wenn sie nicht nur ab und zu mal mit Datenschutzfragen konfrontiert werden. Der DSB wird sich für ihre Ausbildung und den Erfahrungsaustausch mit und unter ihnen engagieren.

Die Digitalisierung wird scheitern, wenn die betroffenen Menschen auch nur schon das Gefühl bekommen, dass sie den Preis für die erhoffte Effizienzsteigerung der Verwaltung mit ihren Grundrechten bezahlen.

Eine Chance auf dem Weg in die digitale Verwaltung

Ein Erfolgsfaktor Die Digitalisierung wird scheitern, wenn die betroffenen Menschen den Preis für die erhoffte Effizienzsteigerung der Verwaltung mit ihren Grundrechten bezahlen oder auch nur schon das Gefühl haben, sie mit ihren Grundrechten zu bezahlen. Um dem entgegenzuwirken und der Digitalisierung Akzeptanz zu verschaffen, hat das modernisierte Datenschutzrecht – europaweit – neue Instrumente geschaffen. Die effiziente und effektive Arbeit mit diesen Instrumenten (u.a. Datenschutz-Folgenabschätzung, Vorabkonsultation, Meldepflicht bei Datenschutzverletzungen) braucht Knowhow. Der besseren Nutzung dieses Knowhows dient die Bündelung – die Bezeichnung von Datenschutzberater:innen.

Chance packen! Es gilt, die Chance zu packen und den DSBer die notwendigen Befugnisse zu geben, damit die Digitalisierung der Verwaltung bei den Betroffenen Akzeptanz findet. Die DSBer sollen bei Projekten rechtzeitig – z.B. schon beim Projektinitialisierungsauftrag (PIA) – einbezogen werden, damit sichergestellt ist, dass die Weichen bezüglich des Datenschutzes rechtzeitig richtig gestellt werden. Sie sollen in der Initialisierungs- und in der Konzeptphase ihr Fachwissen und ihre Erfahrung einbringen können. Und sie können mit der Behandlung von Datenschutz-Anliegen von Betroffenen beauftragt werden. Kurz: Im Interesse eines besseren Grundrechtsschutzes lohnt es sich auf jeden Fall, das Datenschutz-Knowhow in der Verwaltung zu bündeln.

1 Ratschlag 21.1239.01, S. 35.
2 Ratschlag 21.1239.01, S. 50 (neuer § 98a GOG), S. 52 (neuer § 28a JVG), S. 53 (neuer § 57a PolG).
3 Siehe z.B. TB 2020/2021 des DSB/BS, S. 17 ff.; JSSK-Bericht 21.1239.02, S. 12.
4 Die Terminologie der kantonalen Organisationseinheiten richtet sich nach § 26 Abs. 2 OG.
5 JSSK-Bericht 21.1239.02, S. 12.
6 JSSK-Bericht 21.1239.02, S. 11 ff.
7 § 3 Abs. 4 lit. a revIDG.
8 TB 2020/2021 des DSB/BS, S. 18 f.
9 § 18a DSG/BS in der Fassung des Grossratsbeschlusses vom 16.04.2008, <https://www.gesetzessammlung.bs.ch/app/de/texts_of_law/153.260/versions/889> (per 01.01.2012 abgelöst durch das IDG).
10 Ausdrücklich z.B. nach § 45 Abs. 2 IDG.
11 Art. 32 Abs. 2 der Richtlinie (EU) 2016/680; Art. 37 Abs. 5 DSGVO (EU) 2016/679.

Trend 3 Die grössten «Baustellen» und Herausforderungen bei der Digitalisierung

Viele Mitarbeiter:innen, auch auf den Leitungsebenen, der öffentlichen Organe sind ernsthaft bemüht, datenschutzkonform zu arbeiten. Doch teilweise fehlt der konzeptionelle Rahmen. In einzelnen Bereichen sogar ganz. In anderen Bereichen wäre es sinnvoll, die Herausforderungen, die sich quer durch die ganze Verwaltung stellen, koordiniert anzugehen und mit Vorgaben zentral zu steuern. Wo sieht der Datenschutzbeauftragte diesbezüglich die grössten «Baustellen» und Herausforderungen?

Einleitung

Erfreulich Der Datenschutzbeauftragte sieht im Rahmen seiner Beratungs- und Kontrolltätigkeit tief in die Verwaltung hinein. Erfreulich: Er trifft an sehr vielen Stellen, auf allen Ebenen, Mitarbeiter:innen, die ernsthaft bemüht sind, dafür zu sorgen, dass die Daten über die Einwohner:innen im Kanton datenschutzkonform bearbeitet werden.

Weniger erfreulich Er sieht im Laufe seiner Tätigkeit aber auch, wo sich diese Mitarbeiter:innen vergeblich bemühen, weil Aufgaben, Kompetenzen und Verantwortlichkeiten nicht geklärt sind, weil Vorgaben fehlen oder weil Vorgaben nicht eingehalten werden. Solche «grösseren» Problembereiche sollen hier angesprochen werden. Es sind Bereiche, die der Datenschutzbeauftragte allein nicht ändern kann. Sie anzusprechen soll dazu beitragen, Lösungsfindung zu beschleunigen.

Der DSB hofft, dass das Vakuum bald mit einer wirkungsvollen IT-Governance beendet wird.

Sehr dringend und absolut erforderlich: IT-Governance

Konzeptioneller Rahmen Mit einer IT-Governance wird der konzeptionelle Rahmen geschaffen für die Führung und Organisation der kantonalen Informatik und für ihre Aufgaben, Kompetenzen und Verantwortlichkeiten. Ohne Governance wird die Digitalisierung kaum gelingen.

Ersatzlos aufgehoben Vor etwas mehr als drei Jahren wurde die bis anhin geltende IT-Governance aufgehoben. Zwar enthält die Verordnung vom 13. Dezember 2016 über die Informationssicherheit (ISV, SG 153.320) immer noch Regeln für einzelne Funktionen (wie die/der ISB, die ISBD). Aber es fehlt seither der oben erwähnte konzeptionelle Rahmen. Mit der Aufhebung der IT-Governance wurde auch die Abteilung Informatik-Steuerung und -Organisation (ISO) aufgehoben bzw. wurden ihre Funktionen teilweise in IT BS integriert. Seither existiert die vormalige Funktionstrennung zwischen der Formulierung der Anforderungen an die IT (und an die kantonsinterne Leistungserbringerin IT BS) und die Erfüllung der Anforderungen (durch IT BS) nicht mehr im gleichen Masse.

Vakuum Der Datenschutzbeauftragte stellt fest, dass dieses Vakuum für die verantwortungsvolle Steuerung der IT nicht dienlich ist. Die Leitung von IT BS ist sich dessen bewusst und hat den DSB informiert, dass an einer neuen IT-Governance gearbeitet wird. Der DSB hofft – wie schon in seinem Tätigkeitsbericht 2017/2018/2019[1] –, dass das Vakuum sehr bald mit einer wirkungsorientierten IT-Governance beendet wird.

Zentrale Entscheidungen und Vorgaben

Herausforderungen Neue Entwicklungen fordern die Verwaltung heraus. Es wird erwartet, dass sie mit der Zeit geht und neue Technologien nutzt. Und die versprechen viel:

Chatbots Chatbots – auch weniger «intelligente» als ChatGPT[2] – sollen es den Einwohner:innen erleichtern, beim Kontakt mit der Verwaltung rasch(er) zur richtigen Information, zum richtigen Formular oder zur richtigen Ansprechperson zu kommen. Macht ja Sinn, oder? Doch welche (u.U. besonderen?) Personendaten werden dabei erhoben? Wer hat Zugriff darauf? Wann werden sie wieder gelöscht? Ist es bloss die Verwaltung, die diese Daten erhebt, oder liest der Anbieter auch noch mit?

Soziale Medien Über soziale Medien sollen bestimmte Informationen gezielt an spezifische Zielgruppen ausgeliefert werden. Ist ja sinnvoll, oder? Darf der Kanton aber dafür Informationen nutzen, die er selber gar nicht hat, aber von den Betreiber:innen der sozialen Medien – teilweise mit sehr fraglichen Rechtfertigungen – erhoben worden sind? Wie weit darf der Kanton sich unterstützen lassen? Mit Methoden, die ihm selber gar nicht zur Verfügung stehen würden?

Überwachungstools Öffentliche Organe wollen mehr wissen über die Reichweite ihrer digitalen Angebote. Tönt interessant, oder? Wenn sie Web-Applikationen einkaufen, sind häufig standardmässig Überwachungstools (wie z.B. Google Analytics) mitenthalten. Doch hat das öffentliche Organ die erforderliche gesetzliche Grundlage, um Daten über die Nutzer:innen an die Anbieterin des Überwachungstools (z.B. an Google) bekannt zu geben? Wie bringt man die Organe dazu, nur datenschutzkonforme Auswertungstools einzusetzen bei denen die Personendaten *vor* der Übermittlung anonymisiert werden, bei denen eine informierte Einwilligung der Betroffenen *vor* der Übermittlung eingeholt wird oder bei denen die Erteilung der Einwilligung (ohne Einschränkung der Funktionalität) möglich ist?

Stellungnahmen nur im Einzelfall Der DSB kann nur in Einzelvorhaben Stellung nehmen und z.B. den Verzicht auf die Nutzung von Google Analytics empfehlen – bei allen Vorhaben, die (richtigerweise und fälschlicherweise) nicht zur Vorabkonsultation eingereicht werden, erhält er nicht einmal Kenntnis davon. Chatbots sind bisher bei mindestens zwei Stellen eingerichtet, ohne dass der DSB vorgängig involviert worden oder mit eher kurzen Vorläufen angefragt worden wäre. Das mag im «harmlosen» Umfeld und mit «einfachen» Chatbots, die nur zum richtigen Formular leiten, zu keinem Schaden führen – aber soll diese Entscheidung und Risikoübernahme einfach jeder Dienststellenleitung überlassen sein? Oder wäre es nicht sinnvoller, solche Nutzen- und Risikoüberlegungen für alle gemeinsam anzustellen und mit zentralen Vorgaben zu steuern? Der Bericht der GPK zum Jahresbericht 2021 des Regierungsrates hat die schwache organisatorische Einbindung der Querschnittsfunktionen (wie der IT) moniert und empfohlen, dass die rechtlichen und organisatorischen Voraussetzungen geschaffen werden, dass die Querschnittsfunktionen zumindest in gewissen Bereichen ein durchsetzbares Weisungsrecht erhalten.[3]

IT-Governance als Grundlage Eine neue IT-Governance könnte den Boden dafür legen, indem sie die nötigen Steuerungs-Organisationen schafft und deren Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) festlegt – und damit auch die Weichen dafür stellen, was zentral zu entscheiden und zu verantworten ist. Wenn dann diese Organisationen auch noch mit den erforderlichen Ressourcen und Befugnissen ausgestattet sind, könnte dies auch aus Datenschutzsicht zu einer deutlichen Verbesserung führen.

Soll die Entscheidung, ob ein Chatbot eingesetzt wird, und die Übernahme der entsprechenden Risiken einfach jeder Dienststellenleitung überlassen sein. oder wären kantonsweite Nutzen- und Risikoüberlegungen und evtl zentrale Vorgaben nicht sinnvoller?

Projektmanagement

Defizite beim Projektmanagement Im Tätigkeitsbericht 2020/2021[4] hat der DSB über die Defizite beim Projektmanagement berichtet. In der Zwischenzeit arbeitet IT BS an der Umsetzung des HERMES Projektmanagement 2022[5]. So wird etwa der Projektleitfaden überarbeitet. Dazu wurde auch der DSB beigezogen, um gerade auch die mit dem revIDG beschlossenen Instrumente (insb. die Datenschutz-Folgenabschätzung und die Vorabkonsultation) einzubauen.

Erfolgsfaktoren Wichtig ist, dass schliesslich eine *umsetzungstaugliche* Lösung herauskommt, dass diese vom Regierungsrat als *verbindlich* erklärt und dann auch *durchgesetzt* wird. Es ist zu hoffen, dass die IT-Leitungen der anderen Departemente auch einen Gewinn darin sehen, dass das Projektmanagement in strukturierteren Bahnen abläuft als bisher. Ein Projekt, bei dem nach jahrelanger Vorarbeit ein neu eingesetzter Projektleiter feststellen muss, dass schon ein Projektauftrag fehlt, der diesen Namen verdient, und im Gespräch mit dem DSB auch herauskommt, dass die weiteren, für eine Vorabkonsultation erforderlichen Dokumentationen nicht vorhanden sind, dann hat die frühere Projektleitung offensichtlich nicht brilliert. Dass für die nicht nutzbaren Softwarelizenzen auch schon lange Lizenzgebühren entrichtet werden, macht es – wenn auch nicht primär aus Datenschutzsicht – auch nicht besser. >

Sicherheit von Datentransfers

Pendenz seit Jahren Schon seit Jahren ist die Sicherheit der Datenübermittlung eine Herausforderung, die der Lösung harrt.[6] Vor mehreren Jahren hat der Regierungsrat beschlossen, dass das Problem nicht zentral, sondern durch die Departemente zu lösen sei – und die haben es oft einfach an die Dienststellen weitergereicht. Das hat dazu geführt, dass etliche Dienststellen unterschiedlichste Lösungen implementiert haben. Dadurch entstand ein eigentlicher «Wildwuchs». Noch immer erreichen den DSB fast monatlich Anfragen von Dienststellen, die für den Transfer von Daten, insbesondere von besonderen Personendaten, eine sichere Lösung suchen. Gesucht ist eine Lösung, die den Datenaustausch unter öffentlichen Organen sicher macht, aber es auch Einwohner:innen erlaubt, sensitive Daten sicher an öffentliche Organe zu senden als auch solche Daten von öffentlichen Organen zu erhalten.

Nicht so Eine kantonale Dienststelle, die regelmässig besondere Personendaten bearbeitet, hat im Berichtsjahr unter dem Titel «Wir werden digital» die Kund:innen eingeladen, ihr Unterlagen per E-Mail zuzustellen. Der DSB hat umgehend interveniert und verlangt, dass für die Übermittlung von besonderen Personendaten nicht der unsichere Weg über unverschlüsselte E-Mails verwendet sondern eine sichere Lösung zur Verfügung gestellt wird.

In Arbeit Der Bedarf nach einer Möglichkeit, Daten sicher zu übermitteln, ist unübersehbar. Eine Lösung wird nicht nur seit Jahren vom DSB gefordert, sondern zunehmend auch von Dienststellen. Dass sich jedes öffentliche Organ eine andere Lösung beschafft macht keinen Sinn – erst recht nicht für den Kontakt mit Einwohner:innen, die sich dann mit den verschiedenen Systemen herumschlagen müssen. IT BS hat das Thema aufgenommen und ist daran, eine sichere Lösung zur Verfügung zu stellen. Es ist zu hoffen, dass eine solche Lösung zeitnah implementiert, für verbindlich erklärt und durchgesetzt werden kann.

Connect 365

Cloud Im Tätigkeitsbericht 2020/2021[7] hat der DSB über die Herausforderungen beim Gang in die Cloud und speziell über die Rolle des Regierungsrates[8] berichtet.

Das Programm Connect 365 Da aber die entsprechenden Lizenzen schon zu Beginn der Covid-19-Pandemie gelöst wurden, damit MS Teams (als Teil von M365) schon genutzt werden kann, ist es öffentlichen Organen heute bereits möglich, einzelne Microsoft-Onlinedienste zu aktivieren, ohne den noch zu entwickelnden, kontrollierten Weg zu beschreiten. Der DSB hat den Verdacht, dass dies von einzelnen Verwaltungsstellen auch schon genutzt wird.

Der DSB hat den Verdacht, dass einzelne Verwaltungsstellen schon jetzt Microsoft-Onlinedienste aktivieren, ohne den noch zu entwickelnden, kontrollierten Weg zu beschreiten.

Unterlaufen des Programms? Dieser «Wildwuchs» schafft Risiken, die wahrscheinlich nicht im Risikokataster des Kantons erscheinen, weil die verantwortlichen Stellen möglicherweise gar nichts davon wissen. Der DSB wird darauf hinwirken, dass dieses «Unterlaufen» eines kontrollierten Wegs in die Cloud, wie ihn der Regierungsrat gestartet hat, geprüft wird. Der Regierungsrat oder die Konferenz für Organisation und Informatik (KOI) sollten sich dringend einen Überblick über die ohne ihr Wissen eingegangenen Risiken verschaffen und dem unkontrollierten Eingehen von Risiken Einhalt gebieten, dies umso eher, je mehr besondere Personendaten betroffen sein könnten.

M365 im Bund Im Übrigen lohnt sich auch hier ein Blick über die Kantonsgrenzen hinaus. Der Bundesrat hat am 15. Februar 2023 einen Verpflichtungskredit zur Einführung von M365 als neue Office-Version genehmigt.

Nicht für besonders schützenswerte Personendaten In seiner Medienmitteilung hält der Bundesrat die zu beachtenden Einschränkungen fest: «Mit der Einführung sind technische und organisatorische Schutzmassnahmen zu treffen, damit die Software beim Bund geschützt vor dem Zugriff Dritter zum Einsatz kommen kann. Nutzerinnen und Nutzer dürfen in der Cloud von Microsoft *keine besonders schützenswerten Daten* und *keine vertraulichen Dokumente* speichern. Die *E-Mails und Kalender* der Mitarbeitenden der Bundesverwaltung werden weiter *vom Bund selber und vor Ort in den Rechenzentren des Bundes* («On-Premises») verarbeitet und gespeichert.»[9]

Alternativen zur Reduktion der Abhängigkeit Ausserdem spricht er die Abhängigkeit von Microsoft an und will mit der *Prüfung* von *Alternativen* diese Abhängigkeit reduzieren: «Faktisch ist die Bundesverwaltung heute abhängig von Office-Produkten des Herstellers Microsoft. Ein Anbieter- und Produktewechsel wird zurzeit als zu risikoreich und aufgrund der zahlreichen Abhängigkeiten zu Fachanwendungen als zu aufwendig beurteilt. Zur mittel- bis langfristigen Reduktion der Abhängigkeit wird die Prüfung von Alternativen zu Microsoft 365 weitergeführt. Im Rahmen einer *Exit-Strategie* prüft der Bereich DTI der Bundeskanzlei auch Open-Source-Alternativen.»[10]

Bedeutung für die Kantone Selbstverständlich hat der Bund den Kantonen bezüglich der Cloud-Nutzung nichts zu sagen. Dass er aber nach einer gründlichen Prüfung und einer länger andauernden Testphase zur Überzeugung kommt, dass die Cloud von Microsoft nicht für die Speicherung von (in der IDG-Terminologie) besonderen Personendaten und vertraulichen Dokumenten geeignet ist, ist äusserst bemerkenswert – ebenso, dass er E-Mail und Kalender seiner Mitarbeiter:innen «on-prem» bearbeitet werden. Es ist schwer davon auszugehen, dass die Kantone mit vergleichbaren Datenbeständen nicht zu einer anderen, «lockereren» Beurteilung kommen können.

Videokonferenz-Tools

MS Teams Seit dem Beginn der Covid-19-Pandemie wird in der Verwaltung MS Teams genutzt. IT BS hat allerdings von Anfang an darauf hingewiesen, dass dieses Tool nicht für die Bearbeitung von besonderen Personendaten geeignet ist. Der Datenschutzbeauftragte hat im Tätigkeitsbericht 2020/2021[11] bestätigt, dass, solange Covid-19 keinen «Normalbetrieb» erlaubt, die Risikoabwägung anders ausfallen kann. Nachher, wenn wieder ein «normaler» Betrieb möglich ist und/oder die Online-Tools im Regelbetrieb genutzt werden sollen, gelten auch Covid-19-spezifische Risikoabwägungen nicht mehr.

Nutzung im Regelbetrieb Regelmässig wenden sich öffentliche Organ an den DSB, um zu erfahren, welches Videokonferenz-Tool für den Einsatz in sensitiven Bereichen genutzt werden kann. Offensichtlich besteht ein grosser Bedarf nach einer Lösung für diesen Bereich.

Webex von Cisco Bereits während der Covid-19-Pandemie haben die Gerichte nicht MS Teams, sondern Webex eingesetzt. Dieses Tool wird z.B. auch im Kanton Zürich oder in Dienststellen in sensitiven Bereichen in unserem Nachbarkanton genutzt.

Laufende Prüfung Der DSB hat eine Prüfung von Webex gestartet, um herauszufinden, ob und in welchen Konfigurationen dieses Videokonferenz-Tool die Anforderung für das Bearbeiten von besonderen Personendaten zu erfüllen vermag. An den gleichen Anforderungen kann im Anschluss daran MS Teams gemessen werden.

Strategien

Zukunftsgerichtet Der Regierungsrat verabschiedet Strategien, um das Handeln des Kantons in bestimmten Bereichen zukunftsgerichtet zu steuern. Der DSB wird meistens in den Erstellungsprozess einbezogen und nimmt zu den Entwürfen Stellung.

Es ist schwer davon auszugehen, dass die Kantone nicht zu einer «lockereren» Beurteilung kommen können als der Bundesrat, der die MS Cloud für die Speicherung von sensitiven Personendaten und vertraulichen Dokumenten als ungeeignet beurteilt.

Ziele vs. Normen Solche Strategien – wie beispielsweise die Digitalisierungs- oder die Datenstrategie – geben Ziele und Entwicklungsrichtungen vor. Dem DSB obliegt es dabei nicht selten, darauf hinzuweisen, dass solche politische Aussagen in einem rechtlichen Umfeld stattfinden, das zu beachten ist. So erscheint manchmal das Verhältnis zwischen verbindlichen, normativen Vorgaben (insbesondere Vorschriften in Gesetzen und Verordnungen) und Zielen verkannt. Normative Vorgaben gelten. Sollen solche Vorgaben mit Prinzipien einer Strategie «aufeinander abgestimmt» werden, dann halten entweder die Prinzipien die normativen Vorgaben ein oder die Gesetze oder Verordnungen werden im dafür vorgesehenen Verfahren geändert. >

Datenschutzrecht Zu den normativen Vorgaben gehört auch das Datenschutzrecht, das einem öffentlichen Organ die Bearbeitung von Personendaten nur gestützt auf eine gesetzliche Grundlage erlaubt. Auch das Bekanntgeben von Personendaten an ein anderes öffentliches Organ bedarf einer gesetzlichen Grundlage. Damit sind der gemeinsamen Nutzung von Personendaten, wie sie beispielsweise in der Datenstrategie dargestellt wird, Grenzen gesetzt, die – wie erwähnt – nur durch eine Gesetzes- oder Verordnungsänderung (im entsprechenden Fachrecht, also in den Fachgesetzen und nicht im IDG) aufgehoben oder verschoben werden können. Dabei müssen auch die (bundes-)verfassungsrechtlichen oder internationalrechtlichen Vorgaben eingehalten werden.

Die Effizienzsteigerung und Kostenminderung bei der Verwaltung sind berechtigte Ziele. Strategien sollten aber vor allem bringen: einen Nutzen für die Einwohner:innen und die Unternehmen in unserem Kanton.

«Datenschutz ist gewährleistet» Auf Strategieebene werden deshalb Sätze – häufig im Indikativ (z.B. «Daten stehen … zur Verfügung») – auf hohem Abstraktionsgrad verwendet, und auch Aussagen zum Datenschutz sind entsprechend generell: «Datenschutz und Datensicherheit sind jederzeit gewährleistet.»[12] Die Hauptarbeit wird zu leisten sein, wenn nach der Genehmigung der Strategie die Massnahmenpläne auszuarbeiten sind. Dann müssen Aussagen wie «Daten stehen … zur Verfügung» an den bestehenden gesetzlichen Vorgaben gemessen oder Änderungen der gesetzlichen Vorgaben beschlossen werden.

«Einwohner:innen-Nutzen»

Nicht primär Verwaltungssicht Wesentlich ist, dass Strategien nicht primär und schon gar nicht ausschliesslich aus Sicht der Verwaltung formuliert werden. Die Effizienzsteigerung und Kostenminderung bei der Verwaltung sind berechtigte Ziele. Strategien sollten aber vor allem bringen: einen Nutzen für die Einwohner:innen und die Unternehmen in unserem Kanton. Jurist:innen verweisen auf die gleichlautenden Bestimmungen in § 5 Abs. 2 der Kantonsverfassung und Art. 5 Abs. 2 der Bundesverfassung: «Staatliches Handeln muss *im öffentlichen Interesse* liegen und verhältnismässig sein.» Also selbst wenn ein staatliches Handeln auf einer gesetzlichen Grundlage basiert (§ 5 Abs. 1 KV und Art. 5 Abs. 1 BV), muss es auch noch im öffentlichen Interesse liegen. Und das meint nicht einfach im Interesse der Verwaltung, sondern (vor allem auch!) im Interesse der Öffentlichkeit, der vom Handeln betroffenen Personen.

Politisch zu diskutieren Das gilt generell für alle Digitalisierungs- und eGovernment-Projekte – und nicht nur aus Datenschutzsicht. Beim eVoting beispielsweise haben sich die Hoffnungen, dass die Stimmbeteiligung erhöht werden kann, kaum erfüllt – elektronisch abstimmen ist ja (ausser für Menschen mit Behinderungen und Auslandschweizer:innen) auch nicht einfacher als brieflich abstimmen. Jetzt erlaubt der Bund den Einsatz wieder. Ob ein solches System über die erwähnten Anspruchsgruppen hinaus für alle Stimmberechtigten angeboten werden soll, muss politisch diskutiert werden. Entscheidend dafür ist, ob mit eVoting das Vertrauen der Öffentlichkeit in die Korrektheit des Abstimmungsresultats erhalten werden kann.

Künstliche Intelligenz (KI)

Neue Herausforderungen Künstliche Intelligenz wird in jüngster Zeit extrem gehypt. Vieles, was zurzeit bei Verwaltungen unter «künstlicher Intelligenz» behandelt wird, hat noch wenig damit zu tun, sondern es handelt sich um Automatisierungen, allenfalls unter Einbezug «intelligenter» Algorithmen, oder bessere Statistik. Nicht, dass die alle harmlos sind – aber mit echter KI kommen noch neue Herausforderungen auf uns zu.

Motion Thomas Gander Das Thema wurde bereits aufgenommen mit der Motion 21.5704.01 von Grossrat Thomas Gander und Konsorten[13]. Dabei ging es um die Schaffung von rechtlichen Grundlagen für die Anwendung algorithmus-basierter Instrumente in der Polizeiarbeit. Der Regierungsrat hat dazu recht sorgfältig Stellung genommen und die Überweisung an ihn als Anzug beantragt (Stellungnahme 21. 5704.02). Der Grosse Rat hat das Geschäft jedoch an seine Justiz-, Sicherheits- und Sportkommission (JSSK) überwiesen zur Behandlung im Kontext der mit dem IDG-Revisions-Ratschlag beantragten Ergänzung von § 57 PolG um einen neuen Abs. 5.

Beratung in der JSSK Die JSSK stellte in der Folge fest, «dass die Thematik weit über den Anzug, welcher sich «lediglich» auf den Bereich Predictive Policing/ Polizeiarbeit beschränkt, hinausgeht und damit letztlich zu kurz greift, sowie eine Ergänzung im IDG nicht notwendig resp. noch zu früh zu sein scheint. Sie gelangte deshalb nach eingehender Diskussion einstimmig zum Entscheid, dem Grossen Rat die Abschreibung des Anzugs Thomas Gander und Konsorten zu beantragen, um möglichst zeitnahe dazu, nach Durchführung eines Hearings mit Expertinnen und Experten aus Wissenschaft und Technik im September dieses Jahres, einen neuen parlamentarischen Vorstoss mit einer weitergehenden Ausformulierung der Thematik zu den wesentlichen Grundfragen wie Definition der Begrifflichkeiten (Künstliche Intelligenz, algorithmus-basiert etc.), Risiken und Chancen der Technologie, Anwendungsbereiche, Regelungsmöglichkeiten etc. einzureichen, mit welcher der Regierungsrat zur vertieften Anhandnahme der Problematik aufgefordert werden soll.»[14] Der Grosse Rat hat den Anzug dementsprechend am 20. Oktober 2022 abgeschrieben.

Leider hat der Regierungsrat die Schriftliche Anfrage betreffend KI-Systeme nicht ganz so fundiert beantwortet wie vorher die Motion zur Anwendung algorithmus-basierter Instrumente in der Polizeiarbeit.

Schriftliche Anfrage Danielle Kaufmann Am gleichen Tag hat die damalige Präsidentin der JSSK den angesprochenen neuen Vorstoss, die Schriftliche Anfrage 22.5461.01[15] von Danielle Kaufmann betreffend KI-Systemen im Kanton Basel-Stadt eingereicht. Sie wollte damit nach einem Hearing mit Prof. Dr. Nadja Braun Binder (Universität Basel), stellvertretend für die Kommission, zunächst weitere Informationen erhalten zu den im Kanton betriebenen, zur Entwicklung oder Anschaffung geplanten KI-Systemen. Sie stützte sich für den Begriff «KI-System» auf die folgende technikneutrale Definition: «Aus technischer Perspektive handelt es sich um einen etablierten Sammelbegriff, der eine Reihe von Technologien umfasst, die automatisierte Entscheidungen fällen, Empfehlungen machen, Schlussfolgerungen ziehen oder Vorhersagen treffen. Dazu gehören wissensbasierte Systeme und statistische Methoden ebenso wie Ansätze des maschinellen Lernens (z.B. unter Einsatz neuronaler Netze). Die grosse Leistungsfähigkeit dieser Technologien basiert meist auf der Aneinanderreihung einer Vielzahl von mathematischen Optimierungen, die unter Nutzung grosser Rechnerkapazitäten Strukturen aus grossen Datenmengen extrahieren»[16]. Gewünscht wurden Angaben zu:

— den heute schon verwendeten KI-Systemen (inkl. dazu, ob diese Systeme Grundlagen für Entscheidungen liefern, die sich auf natürliche oder juristische Personen auswirken, oder selber solche Entscheidungen treffen [sog. automatisierte Einzelentscheidungen]);

— zu solchen Systemen deren Anschaffung oder Entwicklung geplant ist;

— zum allfälligen kantonalen Regulierungsbedarf insbesondere bezüglich Sicherstellung des Daten- und Persönlichkeitsschutzes, der Einhaltung von Verfahrensgarantien (z.B. Begründungspflicht) sowie der Verhinderung von Diskriminierung für die Anwendung solcher Systeme;

— zu konkreten Anforderungen, insbesondere mit Blick auf die Beschaffungskriterien, Qualitätserfordernisse (hinsichtlich der eingesetzten Algorithmen und Daten), Schulung der Mitarbeitenden (digital literacy), Transparenz (z.B. Transparenzregister für solche Systeme) und Aufsicht.

Antwort des Regierungsrates Leider hat der Regierungsrat nicht ganz so fundiert wie zur Motion Thomas Gander geantwortet, sondern – ganz kurz zusammengefasst – festgehalten,

— dass es zuerst gelte, das Fundament für die Digitalisierung und KI-Systeme bereitzustellen und dass er dazu die Digitalstrategie und die Datenstrategie in Auftrag gegeben habe;

— dass es in der Verwaltung hauptsächlich im Bereich der Effizienzsteigerung (z.B. Text-, Sprach- oder Bilderkennung, Betrugserkennung, Plausibilitätskontrolle, Chatbot / Konversationsagent) und in geringerem Masse auch im Bereich der Entscheidungsgrundlagen (z.B. bessere Prognosen) KI-Systeme, aber keine Übersicht nach Departementen bzw. öffentlich-rechtlichen Anstalten gebe;

— dass die regulatorischen Rahmenbedingungen differenziert betrachtet und dort, wo nötig, aktualisiert werden müssen, wobei er noch auf einen Bericht einer Arbeitsgruppe des Bundes verweist, wonach der allgemeine Rechtsrahmen in der Schweiz zum gegenwärtigen Zeitpunkt grundsätzlich geeignet und ausreichend ist, um mit den Herausforderungen von KI umzugehen.[17] >

Blick über die Kantonsgrenzen Andere Kantone sind da weniger sicher, dass alles in bester Ordnung ist. Im Kanton Zürich soll ein KI-Transparenzregister geschaffen werden. Am 25. April 2022 hat der Kantonsrat diskussionslos ein Postulat[18] von SP, GLP, Grünen, FDP und SVP an den Regierungsrat überwiesen[19], mit dem dieser gebeten wird, zur Herstellung der Transparenz über den Einsatz von künstlicher Intelligenz (KI) in der kantonalen Verwaltung ein Register zur Erfassung der eingesetzten automatisierten Entscheidungssysteme zu erstellen. Die Regierung hatte sich bereit erklärt, den Vorstoss entgegenzunehmen.

Andere Kantone sind da weniger sicher, dass alles in bester Ordnung ist. Im Kanton Zürich soll ein KI-Transparenzregister geschaffen werden.

Nicht erledigt Das Thema hat sich mit der Antwort des Regierungsrates nicht erledigt. Mit § 13 Abs. 2 revIDG hat der DSB die Aufgabe erhalten, eine Liste der Bearbeitungsvorgänge zu erstellen, die zur Vorabkonsultation zu unterbreiten sind. Er wird automatisierte Entscheidungssysteme auf diese Liste setzen. Trotzdem sollte auch dieser Bereich nicht nur vom DSB unter die Lupe genommen sondern vom Kanton gesamtheitlich angegangen werden. Erfreulich ist, dass der Zentrale Rechtsdienst die Basler Gesetzgebungstagung im Herbst 2023 den rechtlichen Herausforderungen beim Einsatz von künstlicher Intelligenz und algorithmusbasierten Systemen in der Verwaltung unter besonderer Berücksichtigung von rechtsstaatlichen Verfahrensgarantien widmet.

1 TB 2017/2018/2019 des DSB/BS, S. 32, linke Spalte.
2 Vgl. dazu das Themenpapier zu ChatGPT von der Stiftung für Technikfolgen-Abschätzung TA SWISS: <https://www.ta-swiss.ch/app/uploads/2023/04/ThemenpapierChatGPT-DE.pdf>.
3 Rechenschaftsbericht und Bericht der Geschäftsprüfungskommission des Grossen Rats des Kantons Basel-Stadt vom 21. Juni 2021 zum Jahresbericht 2021 des Regierungsrats, <https://grosserrat.bs.ch/dokumente/100397/000000397638.pdf>, S. 39-41.
4 TB 2020/2021 des DSB/BS, S. 17–20.
5 <https://www.hermes.admin.ch/de/pjm-2022/verstehen/hermes-projektmanagement-methodenelemente.html>.
6 Vgl. nur etwa TB 2017/2018/2019 des DSB/BS, S. 32, rechte Spalte.
7 TB 2020/2021 des DSB/BS, S. 21–31.
8 TB 2020/2021 des DSB/BS, S. 32–35.
9 Medienmitteilung des Bundesrates vom 15.02.2023, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-93076.html> (Hervorhebungen nicht im Original).
10 Medienmitteilung des Bundesrates vom 15.02.2023, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-93076.html> (Hervorhebungen nicht im Original). Vgl. dazu auch die Kurzmitteilung des EDÖB vom 07.03.2023: <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#207406292>.
11 TB 2020/2021 des DSB/BS, S. 21–31.
12 Das erinnert den Datenschutzbeauftragten an eine Ausschreibung für ein Personalinformationssystem in den 1990er Jahren. Einzige Anforderung zum Datenschutz in der Ausschreibung: «Der Datenschutz und die Datensicherheit sind zu gewährleisten». Einzige Aussage zum Datenschutz in der Offerte: «Der Datenschutz und die Datensicherheit sind gewährleistet.»
13 Motion 21.5704.01 (<https://grosserrat.bs.ch/dokumente/100395/000000395705.pdf>).
14 Bericht 21.1239.02 der JSSK (<https://grosserrat.bs.ch/dokumente/100402/000000402994.pdf>), S. 19.
15 Schriftliche Anfrage 22.5461.01 (<https://grosserrat.bs.ch/dokumente/100403/000000403060.pdf>).
16 Positionspapier «Ein Rechtsrahmen für KI», Florent Thouvenin et al., 2021.
17 Antwort 22.5461.02 (<https://grosserrat.bs.ch/dokumente/100403/000000403870.pdf>).
18 Postulat KR-Nr. 9/2022 Nicola Yuste / Gabriel Mäder / Wilma Willi / Arianne Moser / Erika Zahler betreffend Transparenz über den Einsatz von künstlicher Intelligenz in der Verwaltung, <https://parlzhcdws.cmicloud.ch/parlzh5/cdws/Files/b8bd4cdb86dd446cb9aca73586a9bf23-332/2/pdf>.
19 Kantonsratsprotokoll: <https://parlzhcdws.cmicloud.ch/parlzh5/cdws/Files/4a82dc26d2b34a4e9a3a7ea99b37a3f7-332/6/pdf>.

Trend 4 Anwendbares Datenschutzrecht beim Vollzug von Bundesrecht

Von Berater:innen ist ab und zu zu lesen, dass die Pensionskassen (PK) datenschutzrechtlich betrachtet Bundesorgane seien und dass für ihr Bearbeiten von Personendaten deshalb die entsprechenden Bestimmungen des Bundes-Datenschutzgesetzes (DSG) Anwendung finden. Das stimmt für die privaten PK und die des Bundes, nicht aber für die kantonalen und städtischen PK des öffentlichen Rechts.

Rechtsetzungskompetenz

Kompetenz zur Rechtsetzung im Datenschutz Der Bund ist nur zuständig, in einem Sachgebiet Recht zu setzen, wenn ihm die Bundesverfassung (BV) die entsprechende Kompetenz zuweist.[1] Da es in der BV zum Datenschutz keine solche Bestimmung gibt, kommt dem Bund keine umfassende Datenschutz-Rechtsetzungskompetenz zu. Eine Teilkompetenz kann er ableiten aus seiner Zuständigkeit, das Zivil- und Zivilprozessrecht zu regeln[2]. Deshalb darf er in seinem DSG das Datenbearbeiten durch Private regeln. Zudem darf er, abgeleitet aus seinen Aufgabenkompetenzen in der BV, im DSG Regeln für das Datenbearbeiten durch Bundesorgane aufstellen. Die Kompetenz (und Pflicht) zur Regelung des Datenbearbeitens durch kantonale und kommunale öffentliche Organe liegt aber bei den Kantonen. Die Antwort auf die Frage, welches Datenschutzgesetz für ein Datenbearbeiten gilt, hängt somit primär davon ab, *wer die Personendaten bearbeitet*: Für das Datenbearbeiten durch Bundesorgane und Private gilt das Bundes-DSG, für dasjenige von kantonalen und kommunalen öffentlichen Organe das jeweilige kantonale (Informations- und) Datenschutzgesetz.

Datenbearbeiter:innen

Bundesorgane Als Bundesorgane gelten – nach dem alten und nach dem neuen DSG – Behörden oder Dienststellen des Bundes sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind. Mit einer solchen Aufgabe des Bundes betraut sind zum Beispiel die privaten Krankenkassen, die das Krankenversicherungsgesetz (KVG) vollziehen, im Bereich der obligatorischen Krankenpflegeversicherung (OKP), die Branchenausgleichskassen, die das AHV-Gesetz vollziehen, oder eben auch die privaten Vorsorgestiftungen, die das BVG vollziehen. Wenn sie in diesem Rahmen Personendaten bearbeiten, gelten dafür deshalb die DSG-Bestimmungen für Bundesorgane. Ausserhalb des Vollzugs dieser übertragenen Bundesaufgabe unterstehen sie den DSG-Bestimmungen für private Datenbearbeiterinnen, zum Beispiel beim Bearbeiten von Personendaten zur Abwicklung des Arbeitsvertrages mit ihren Angestellten oder beispielsweise bei der Vergabe von Hypotheken an ihre Versicherten.

Anders als die Privaten, denen vom Bund öffentliche Aufgaben übertragen werden, werden kantonale (oder kommunale) öffentliche Organe, die Bundesrecht vollziehen, nicht zu Bundesorganen.

Kantonale öffentliche Organe Kantonale (bzw. kommunale) öffentliche Organe sind die Organisationseinheiten des Kantons und der Gemeinden; die Organisationseinheiten der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, die eine öffentliche Aufgabe erfüllen, und Private, soweit ihnen vom Kanton oder von den Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist.[3]

Kantonale öffentliche Organe beim Vollzug von Bundesrecht

Keine Bundesorgane Auch kantonalen (bzw. kommunalen) öffentlichen Organen überträgt der Bund den Vollzug von Bundesrecht. Aber anders als die Privaten, denen vom Bund öffentliche Aufgaben übertragen werden, werden sie *nicht zu Bundesorganen*. Sie bleiben kantonale (bzw. kommunale) öffentliche Organe. Das hat das Bundesgericht auch für die kantonalen IV-Stellen, die vom Kanton gestützt auf das Invalidenversicherungsgesetzes (IVG) geschaffen werden müssen[4] und das IVG vollziehen, so bestätigt.[5] Wäre dem nicht so, wären ja grosse Teile der Kantons- und Gemeindeverwaltungen Bundesorgane.

>

Öffentliche Pensionskassen Die öffentlichen PK von Kantonen oder Städten sind nach Art. 48 Abs. 2 BVG Vorsorgeeinrichtungen des öffentlichen Rechts mit eigener Rechtspersönlichkeit. Auch sie vollziehen das BVG, werden damit aber wie erwähnt nicht zu Bundesorganen. Sie *bleiben kantonale (bzw. kommunale) öffentliche Organe*. Damit gilt für ihr Datenbearbeiten das jeweilige kantonale (Informations- und) Datenschutzgesetz – im BVG-Bereich! Darüber hinaus, wenn sie also im wirtschaftlichen Wettbewerb stehen und dabei privatrechtlich handeln und beispielsweise ihren Versicherten Hypotheken gewähren, sind auf ihr Datenbearbeiten die Bundes-DSG-Bestimmungen für das Datenbearbeiten durch Private anwendbar.

Unterscheidung zwischen «allgemeinem» und «besonderem Datenschutzrecht»

«Allgemeines Datenschutzrecht» Droht nicht ein föderalistisches Durcheinander, wenn für die kantonalen oder städtischen PK das jeweilige kantonale Datenschutzgesetz gilt? Nein. Die kantonalen Datenschutzgesetze enthalten, wie das Bundes-DSG für die Bundesorgane, nur die *Datenschutzgrundsätze* – und die sind spätestens seit der Assoziierung der Schweiz an Schengen harmonisiert: Datenbearbeitungen müssen auf einer gesetzlichen Grundlage basieren (Legalitätsprinzip); sie müssen verhältnismässig und für die Betroffenen transparent sein; Zweckänderungen müssen gerechtfertigt werden; die Daten müssen richtig und durch technische und organisatorische Massnahmen vor unbefugter Bearbeitung geschützt sein. Die Datenschutzgesetze sind eben nur das «allgemeine Datenschutzrecht».

«Besonderes Datenschutzrecht» Wird für das Datenbearbeiten einer privaten oder Bundes-PK durch das Bundes-DSG oder für eine kantonale oder städtische PK durch das anwendbare kantonale (Informations- und) Datenschutzgesetz eine gesetzliche Grundlage verlangt, dann findet sich eben diese gesetzliche Grundlage nicht im DSG oder IDG, sondern in den Fachgesetzen – für die PK im BVG. Diese *Fachgesetze* enthalten die *bereichsspezifischen Datenschutzvorschriften* – sie bilden das sog. «besondere Datenschutzrecht». Die BVG-Bestimmungen gelten für alle PK, für die PK des Bundes, für die privaten PK, aber auch für alle kantonalen und städtischen PK. Damit wird sichergestellt, dass in diesem Bereich einheitliche Regeln gelten.

Aufsicht

Datenschutzaufsicht Grundsätzlich folgt die *Datenschutzaufsicht* dem anwendbaren DSG bzw. IDG. Wer dem Bundes-DSG untersteht, untersteht grundsätzlich der Datenschutzaufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) – wer einem kantonalen IDG oder DSG untersteht, wird durch die kantonalen (oder kommunalen) Datenschutzbeauftragten (DSB) beaufsichtigt.

Modernere kantonale Datenschutzgesetze halten ausdrücklich fest, dass für öffentliche Organe im wirtschaftlichen Wettbewerb die privatrechtlichen Bestimmungen des Bundes-DSG gelten, dass aber die Aufsicht bei den kantonalen DSB bleibt.

Fachaufsicht Daneben besteht aber auch die *Fachaufsicht*, im Falle der PK durch die kantonalen BVG-Aufsichtsbehörden und durch die vom Bundesrat bestellte Oberaufsichtskommission. Auch damit wird eine Einheitlichkeit der Auslegung der Bestimmungen des anwendbaren besonderen Datenschutzrechts (im Falle der Pensionskassen also des BVG und des dazugehörenden Verordnungsrechts) gefördert.

Tätigkeiten der öffentlichen Pensionskasse über den BVG-Bereich hinaus

Wirtschaftlicher Wettbewerb Oft nehmen die öffentlichen Organe am wirtschaftlichen Wettbewerb teil und handeln dabei privatrechtlich. Das ist z.B. der Fall, wenn die PK ihren Versicherten Hypotheken anbieten. In diesem Kontext handeln sie wie Private, und auf ihre entsprechenden Datenbearbeitungen sind die Bestimmungen des Bundes-DSG für Private anwendbar. Sie sind aber nicht Private, sind z.B. weiterhin an die Grundrechte gebunden und geniessen nicht wie «echte» Private Privatautonomie. Modernere kantonale Datenschutzgesetze, z.B. das IDG/ZH[6] und unser revidiertes IDG[7], halten ausdrücklich fest, dass die privatrechtlichen Bestimmungen des Bundes-DSG gelten, aber auch, dass die Aufsicht bei den kantonalen DSB bleibt (Prinzip der Einheitlichkeit der Datenschutzaufsicht) (siehe dazu vorne S. 8).

Zusammenfassung

In fünf Sätzen Die Erkenntnisse bezüglich des anwendbaren Rechts bei Privaten bzw. öffentlichen Organen des Kantons, die Bundesrecht vollziehen, können wie folgt zusammengefasst werden:

— Betraut der Bund Private mit öffentlichen Aufgaben, werden diese Privaten datenschutzrechtlich zu Bundesorganen.

— Betraut der Bund kantonale öffentliche Organe mit dem Vollzug des Bundesrechts, bleiben diese datenschutzrechtlich kantonale öffentliche Organe.

— Private Pensionskassen (wie auch die Branchenausgleichskassen) werden im obligatorischen Bereich Bundesorgane, für deren Datenbearbeiten das Bundes-DSG gilt.

Öffentliche Organe, die am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln, sind nicht Private, sind z.B. weiterhin an die Grundrechte gebunden und geniessen nicht wie «echte» Private Privatautonomie.

— Kantonale oder städtische öffentliche Pensionskassen (und die kantonalen Ausgleichskassen und IV-Stellen) bleiben im Bereich des Vollzugs des Bundesrechts kantonale oder kommunale öffentliche Organe, für deren Datenbearbeiten das entsprechende kantonale (Informations- und) Datenschutzgesetz gilt.

— Bei Datenbearbeitungen über den BVG-Bereich hinaus (z.B. bei der Gewährung von Hypotheken an ihre Versicherten) gelten für alle Pensionskassen die Bundes-DSG-Bestimmungen für das Datenbearbeiten durch Private.

1 Art. 3 und 42 BV.
2 Art. 122 BV.
3 § 3 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 4 ff.
4 Art. 54 Abs. 2 IVG.
5 Urteil 1C_125/2015 der I. öffentlich-rechtlichen Abteilung des Bundesgerichts vom 17.07.2015.
6 § 2c Abs. 2 IDG/ZH.
7 § 2 Abs. 2 revIDG; vgl. dazu Bericht 21.1239.02, S. 7 f.


HOTEL

Jahresrückblick

2022:
Kurzer Blick auf die wichtigsten Geschäfte

34 Aufgaben des Datenschutzbeauftragten
Beratungstätigkeit
36 Kantonaler Datenmarkt
Weitere «Baustellen»
Pilotversuche
Kontrolltätigkeit
37 Informationszugangsgesuche
38 Statistik zu den Geschäften des Datenschutzbeauftragten
Personelle Ressourcen des Datenschutzbeauftragten

Statistik

40 Geschäfte
Indikatoren gemäss Budget
Öffentlichkeitsprinzip
41 Initianten (Veranlasser der Geschäfte)
In die Geschäfte involvierte Stellen

Jahresrückblick

2022: Kurzer Blick auf die wichtigsten Geschäfte

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

Aufgaben des Datenschutzbeauftragten

Beratung und Kontrolle Das Informations- und Datenschutzgesetz (IDG) bezweckt, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern und die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.[1] Das IDG beauftragt die/den DSB schwergewichtig mit der Beratung und Kontrolle[2] – das bleibt auch nach dem revidierten IDG so. Beraten werden einerseits die öffentlichen Organe beim Umgang mit Informationen und andererseits die von einer Datenbearbeitung betroffenen Personen über ihre Rechte.

Beratungstätigkeit

Querschnittsthema Die Beratungstätigkeit bindet gegen drei Viertel der Ressourcen des DSB. Thematisch wurde auch im Jahr 2022 die gesamte Breite der Staatstätigkeit erfasst. Ausgewählte Bereiche sind vorne im Kapitel «Trends» (S. 8 ff.) dargestellt. Nur exemplarisch seien hier ein paar weitere Themen kurz erwähnt.

Übermitteln Überwachungstools Daten der Nutzer:innen an die Anbieter:innen, so stellt dies eine Datenbekanntgabe durch das öffentliche Organ dar, wofür keine gesetzliche Grundlage besteht.

Belege mit nicht relevanten Inhalten Oft müssen Einwohner:innen Belege liefern, um bestimmte Tatsachen zu beweisen. Nicht immer sind alle Teile (z.B. eines Vertrages) relevant. Dann darf die einliefernde Person die nicht-relevanten Informationen abdecken oder einschwärzen. Nicht korrekt ist es, wenn dann von Mitarbeiter:innen des öffentlichen Organs die Abdeckung entfernt und das Dokument mit allen Informationen eingescannt und zu den Akten genommen wird.

Bewerbungsunterlagen Die Unterlagen von bei einer Stellenbesetzung nicht berücksichtigten Bewerber:innen sind zurückzugeben oder zu vernichten. Wenn die Bewerbung vielleicht bei der nächsten entsprechenden Stellenausschreibung berücksichtigt werden kann, darf sie mit der ausdrücklichen Einwilligung der betroffenen Person weiter aufbewahrt werden. Auch wieder nur mit einer ausdrücklichen Einwilligung der betroffenen Person darf die Bewerbung an eine andere Dienststelle oder Abteilung weitergegeben werden.

Überwachungstools Etliche Amtsstellen möchten gerne die Daten über die Reichweite eines Newsletters oder die Nutzung ihrer Website erheben. Oft werden dafür von externen Anbieter:innen Überwachungstools (wie z.B. Google Analytics) empfohlen. Übermitteln solche Tools Daten der Nutzer:innen an die Anbieter:innen, so stellt dies eine Datenbekanntgabe durch das öffentliche Organ dar, wofür keine gesetzliche Grundlage besteht. Der Einsatz von Überwachungstools, bei denen die Personendaten nicht *vor* der Übermittlung anonymisiert werden, bei denen nicht eine informierte Einwilligung der Betroffenen *vor* der Übermittlung eingeholt wird und bei denen die Erteilung der Einwilligung (ohne Einschränkung der Funktionalität) nicht verweigert werden kann, ist deshalb unzulässig. Der DSB empfiehlt immer den Einsatz von Tools, die das nicht tun. Die Pensionskasse Basel-Stadt ist bei ihrer neuen Website dieser Empfehlung umgehend gefolgt und setzt ein Tool ein, das die Website-Nutzung datenschutzkonform erfasst. Für andere Fälle wäre eine verbindliche zentrale Vorgabe hilfreich (siehe dazu vorne S. 23).

«Absprung» auf andere Websites Bei einer staatlichen App können die Nutzer:innen, statt selber die aktuelle Adresse einzugeben, freiwillig einen Kartendienst (wie z.B. Google Maps) nutzen und so den Standort eingeben lassen. Damit nutzen die Betroffenen den Internetdienst eines Dritten und verlassen den Verantwortungsbereich des Kantons (und Geltungsbereich des IDG). Dieser «Absprung» braucht die Einwilligung der betroffenen Person. Dazu ist mindestens ein Klick auf ein «Ja» nötig – im Sinne von: Ich weiss, dass ich jetzt den «kantonalen Bereich» verlasse, und begebe mich bewusst und freiwillig in ein Verhältnis mit der (in der Regel privaten, häufig ausländischen) Anbieterin. Das Klicken allein auf den im Logo der Kartendienstanbieterin hinterlegten Link stellt keine bewusste Einwilligung dar.

Automatische Fahrzeugfahndung und Verkehrsüberwachung Die Kantonspolizei möchte automatisch den Verkehr überwachen (AFV: automatische Fahrzeugfahndung und Verkehrsüberwachung). Der DSB nimmt dazu Stellung und verlangt insbesondere eine Differenzierung nach dem Zweck: Die Fahndung nach gestohlenen Fahrzeuge ist nicht dasselbe wie die Suche nach Fahrzeugen, deren Halter:innen eine Ordnungsbusse nicht bezahlt haben. Nicht für alle Fahndungs- und Überwachungszwecke besteht schon eine hinreichende gesetzliche Grundlage. Ein inzwischen ergangenes Bundesgerichtsurteil zu einer ähnlichen Vorlage im Kanton Solothurn[3] erhöht die Anforderungen an die Rechtsgrundlage. Dies wird auch in Basel-Stadt zu beachten sein.

Werbung auf Social Media Der Kanton will Werbung auf Social Media schalten – zielgruppenspezifisch. Darf der Kanton das überhaupt? Darf er dafür Informationen nutzen, die er selber gar nicht hat, aber von den Betreiber:innen der sozialen Medien – teilweise mit sehr fraglichen Rechtfertigungen – erhoben worden sind (siehe dazu vorne S. 23)?

Bekanntgabe von Personendaten für ein Forschungsprojekt Ein öffentliches Organ soll Personendaten für ein Versorgungsforschungsprojekt zur Verfügung stellen (i.S.v. § 22 Abs. 1 IDG[4]). Die Daten sollen mit Daten aus anderen Quellen zusammengeführt werden und können deshalb nicht vor der Bekanntgabe anonymisiert oder pseudonymisiert werden, wie es § 22 Abs. 2 lit. a IDG verlangen würde. Der DSB empfiehlt, eine unabhängige Datentreuhandstelle mit der Zusammenführung der Daten und der anschliessenden Anonymisierung oder Pseudonymisierung zu beauftragen.

Überwachungs-/Assistenzsystem in einem Spital Eine Gesundheitseinrichtung will ein Überwachungs- bzw. Assistenzsystem einsetzen, das bei Demenz- und/oder Delirpatient:innen eingesetzt werden soll, die aufgrund ihrer Verwirrung stark sturz- und weglaufgefährdet sind. Das System zeichnet nicht Videoaufnahmen auf, sondern detektiert Bewegungen mittels Radar. Es dient bei akuten Verwirrungszuständen ergänzend zum Pflegekonzept mit seinen Funktionen Sturzalarm, Sturzprophylaxe, Aufsteh- und Entfernungs-Warnung und Aktivitätsanalyse der Erhöhung der Patient:innensicherheit. Der DSB hat Empfehlungen in Bezug auf die Rechtsgrundlagenanalyse (inkl. der Information und Einholung einer Einwilligung bei urteilsfähigen Patient:innen und/oder Angehörigen), die Unterscheidung von Behandlungs- und Forschungszwecken, die Risikoanalyse und die Sicherheitsmassnahmen abgegeben und die Erstellung eines Datenschutzkonzepts verlangt.

Der «Absprung» auf eine andere (private) Website braucht die Einwilligung der betroffenen Person. Dazu ist mindestens ein Klick auf ein «Ja» nötig.

Anwendbares Datenschutzrecht bei öffentlichen Organen des Kantons, die Bundesrecht vollziehen Von Berater:innen ist ab und zu zu lesen, dass die Pensionskassen (PK) datenschutzrechtlich betrachtet Bundesorgane seien und dass für ihr Bearbeiten von Personendaten deshalb die entsprechenden Bestimmungen des Bundes-Datenschutzgesetzes (DSG) Anwendung finden. Das stimmt für die privaten PK und die des Bundes, nicht aber für die kantonalen und städtischen PK des öffentlichen Rechts (siehe ausführlich dazu vorne S. 29 ff.). Die Erkenntnisse bezüglich des anwendbaren Rechts bei Privaten bzw. öffentlichen Organen des Kantons, die Bundesrecht vollziehen, können wie folgt zusammengefasst werden:

— Betraut der Bund Private mit öffentlichen Aufgaben, werden diese Privaten datenschutzrechtlich zu Bundesorganen.

— Betraut der Bund kantonale öffentliche Organe mit dem Vollzug des Bundesrechts, bleiben diese datenschutzrechtlich kantonale öffentliche Organe.

— Private Pensionskassen (wie auch die Branchenausgleichskassen) werden im obligatorischen Bereich Bundesorgane, für deren Datenbearbeiten das Bundes-DSG gilt. >

— Kantonale oder städtische öffentliche Pensionskassen (und die kantonalen Ausgleichskassen und IV-Stellen) bleiben im Bereich des Vollzugs des Bundesrechts kantonale oder kommunale öffentliche Organe, für deren Datenbearbeiten das entsprechende kantonale (Informations- und) Datenschutzgesetz gilt.

— Bei Datenbearbeitungen über den BVG-Bereich hinaus (z.B. bei der Gewährung von Hypotheken an ihre Versicherten) gelten für alle Pensionskassen die Bundes-DSG-Bestimmungen für das Datenbearbeiten durch Private.

Bevor – wie in etlichen Strategien vorgesehen – das «Once only»-Prinzip umgesetzt werden kann, muss dringend Ordnung in den Datenmarkt gebracht werden.

Kantonaler Datenmarkt

Abgelaufene Autorisierungen Im Tätigkeitsbericht 2020/2021[5] hat der DSB über die abgelaufenen Autorisierungen für Onlinezugriffe im Datenmarkt berichtet. Gegen Ende des Jahres 2022 hat der DSB den Druck erhöht und der Konferenz für Organisation und Informatik (KOI), der Gesamtverantwortlichen für den Datenmarkt[6], nahegelegt, die Erneuerung der 12 Gesuche, die den Zugriff auf besondere Personendaten betreffen, prioritär behandeln zu lassen und für die Einreichung der Gesuche eine Frist bis Ende des ersten Quartals 2023 zu setzen. Nach Ablauf dieser Frist könne sich der DSB gezwungen sehen, den betroffenen Dateneigner:innen als Verantwortliche für die Bekanntgabe «ihrer» Personendaten zu empfehlen, den Datenbezug umgehend zu unterbinden.

Priorisierung Der Druck hat bewirkt, dass sich bis Ende März 2023 mehr bewegt hat. Entweder waren die Gesuche eingereicht (und zum Teil bereits für den «Round Table»[7] traktandiert) oder es wurden (begründete) Fristerstreckungsgesuche eingereicht (z.B. weil Gesuche zusammengelegt werden können) oder die Onlinezugriffe wurden hinfällig. Ausserdem legt IT BS der KOI im April 2023 einen «Sanierungsplan» für die anderen Onlinezugriffsberechtigungen mit abgelaufenen oder nicht dokumentierten Autorisierungen vor (nach Schätzung der Finanzkontrolle: 300 Gesuche).

Ausblick Bevor – wie in etlichen Strategien vorgesehen – das *«Once only»-Prinzip*[8] umgesetzt werden kann, muss dringend *Ordnung in den Datenmarkt* gebracht werden. Die Gesamtverantwortung liegt wie erwähnt bei der KOI.

Weitere «Baustellen»

Verweis Für die weiteren «Baustellen» und Herausforderungen bei der Digitalisierung siehe ausführlich vorne S.22 ff.

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.[9] Bei der Beratung des § 9a IDG in der Justiz-, Sicherheits- und Sportkommission des Grossen Rates wurde grossen Wert darauf gelegt, dass die Umsetzung der Bestimmung durch den DSB eng begleitet wird.[10] Er soll jährlich darüber berichten, welche Pilotversuche laufen und insbesondere auch kontrollieren, ob Pilotversuche nach Ablauf der fünfjährigen Versuchsphase, falls die notwendige formellgesetzliche Grundlage nicht geschaffen wurde, tatsächlich definitiv eingestellt worden sind.

Laufende Pilotversuche Zurzeit läuft kein auf § 9a IDG gestützter Pilotversuch. Der Datenschutzbeauftragte hat aber schon zu drei Vorhaben der Verwaltung Stellung genommen, bei denen allenfalls in Zukunft Pilotversuche erforderlich sein könnten, bevor die erforderliche formellgesetzliche Grundlage geschaffen werden kann.

Kontrolltätigkeit

Datenschutzprüfungen (Audits) Im Jahr 2022 konnten sechs Datenschutzprüfungen abgeschlossen werden. Als Abschluss gilt die Zustellung des finalen Schlussberichts nach der Schlussbesprechung.

Abgeschlossener Audit bei der Steuerverwaltung 2022 wurde eine erste von mehreren Datenschutzprüfungen bei der Steuerverwaltung abgeschlossen. Der Audit fokussierte sich auf die Prozesse und die Organisation. Er führte zu vier Feststellungen und Empfehlungen (Priorität mittel) in den Bereichen Aufbewahrung/Vernichtung von Steuererklärungsakten, Zutrittsmanagement und Löschung von temporären Foldern.

Abgeschlossener Audit zum Smartmetering bei den IWB Der Fokus der 2022 abgeschlossenen Datenschutzprüfung bei den Industriellen Werken Basel (IWB) lag auf den Datenschutzrisiken in Bezug auf die Erfassung von Daten durch digitale Stromzähler und auf der Gewährleistung der Datentrennung. Verbesserungen wurden verlangt in den Bereichen Informationssicherheit und Datenschutzrisikomanagement bei den verschiedenen Netzwerkelementen sowie beim Zugriffskonzept. Die Datentrennungsfrage konnte in dieser Datenschutzprüfung noch nicht beantwortet werden.

Drei abgeschlossene Follow-up-Audits bei der Einwohnergemeinde Riehen Im Nachgang zu den im Jahr 2020 abgeschlossenen Datenschutzprüfungen fanden zu den drei Bereichen Personal, Sozialhilfe und Verstärkte Massnahmen Schulen in der Einwohnergemeinde Riehen Follow-up-Audits statt. Sie führten zu folgenden Feststellungen und Empfehlungen:

— Personal: eine Empfehlung (Priorität hoch) zu den vertraglichen Vereinbarungen bei Auftragsdatenbearbeitungen, drei Empfehlungen (Priorität mittel) zum Benutzer:innenadministrationsprozess, zum Berechtigungsadministrationsprozess und zur Überwachung von durch Dritte erbrachten externen Dienstleistungen;

— Sozialhilfe: eine Empfehlung (Priorität hoch) zu den vertraglichen Vereinbarungen bei Auftragsdatenbearbeitungen, vier Empfehlungen (Priorität mittel) zur Aufbewahrung und Löschung, zur Verwaltung der Onlinezugriffs-Gesuche, zum Benutzer:innenadministrationsprozess sowie zu Datensicherung und Notfallplanung;

— Verstärkte Massnahmen Schulen: drei Empfehlungen (Priorität mittel) zum Dokumentenversand per E-Mail, zur Umsetzung des Aufbewahrungs- und Löschkonzeptes und zum Schutz von Dokumenten auf den Geräten von Lehrpersonen.

Abgeschlossene SIS-Kontrolle beim Migrationsamt Regelmässig führt der DSB sog. «SIS-Kontrollen» durch. Dabei geht es um stichprobenbasierte Audits, bei denen Interviews mit Mitarbeiter:innen derjenigen Verwaltungsstellen durchgeführt werden, die auf das Schengener Informationssystem (SIS) zugreifen. Im Berichtsjahr 2022 konnte die SIS-Kontrolle beim Migrationsamt (Abteilung Einreisen) abgeschlossen werden. Die Prüfung fokussierte 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. Die Feststellungen und Empfehlungen betrafen die Passwortkomplexität, die Identifikation von telefonisch Anfragenden, die Verschlüsselung besonders sensitiver Kommunikation und die regelmässige Schulung der Mitarbeiter:innen.

Laufende Audits Ende 2022 waren darüber hinaus weitere Datenschutzprüfungen am Laufen, die Schlussberichte aber noch nicht abgeschlossen:

— Datenschutzprüfung ISMS.BS bei IT BS;

— Datenschutzprüfung beim Universitären Zentrum für Zahnmedizin Basel (UZB);

— Follow-up-Audit beim Universitätsspital Basel (USB);

— SIS-Kontrolle bei der Kantonspolizei, Abteilung Sicherheitspolizei;

— SIS-Kontrolle bei der Kriminalpolizei.

Informationszugangsgesuche

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

Regelmässig führt der DSB sog. «SIS-Kontrollen» durch, bei denen Interviews mit Mitarbeiter:innen derjenigen Verwaltungsstellen durchgeführt werden, die auf das Schengener Informationssystem (SIS) zugreifen.

Statistik Die Informationszugangsgesuchs-Zahlen für das Jahr 2022 finden sich – über die gesamte Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (S. 40). Nach Departementen aufgeschlüsselt hat sie der Regierungsrat jeweils in seinem Jahresbericht veröffentlicht.[11]

Erledigung Die Zahl der eingegangenen Gesuche war gegenüber der Vorperiode praktisch gleich (30 / Vorjahr 2021: 31). Der Anteil der ganz oder teilweise gutgeheissenen Gesuche war gegenüber dem Vorjahr markant höher (73% / Vorjahr 2021: 52%). Der Anteil der ganz abgewiesenen Gesuche, der in der Vorperiode gestiegen war, fiel auf rund die Hälfte (23% / Vorjahr 2021: 45%). Die Zahl der am Jahresende noch

>

nicht erledigten Gesuche blieb unverändert (3% / Vorjahr 2021: 3%). Ob die höhere Gutheissungs- und tiefere Abweisungsquote an der besseren Qualität der Gesuche lag oder an der höheren Bereitschaft der Verwaltung, allfällige Geheimhaltungsinteressen als weniger gewichtig zu bewerten, kann ohne Kenntnis der Ablehnungsgründe nicht beurteilt werden.

Statistik zu den Geschäften des Datenschutzbeauftragten

Kennzahlen Die Kennzahlen für das Jahr 2022 finden sich im Statistikteil dieses Tätigkeitsberichts (S. 40).

Neu eröffnete Geschäfte Neu eröffnet wurden im Jahr 2022 zwölf Geschäfte weniger als im Vorjahr (571; 2021: 583). Damit weist die Geschäftskontrolle des Datenschutzbeauftragten erstmals seit sieben Jahren keinen Zuwachs (2015: +3%; 2016: +9%; 2017: +1%; 2018: +5%; 2019: +10%; 2020: +5%; 2021: +7%), sondern einen minimalen Rückgang (-2%) aus. Zu diesem Rückgang beigetragen hat unter anderem die Tatsache, dass ein Drittel weniger Schengen-Weiterentwicklungen zu beurteilen waren (24 / Vorjahr 2021: 36), was mit der hohen Zahl von Corona-bedingten Weiterentwicklungen im Vorjahr zu tun hat. Aufgrund der Belastung, die auch mit dem höheren Anteil komplexer Geschäfte zusammenhängt, hat der DSB selber etwas weniger Geschäfte selber initiiert (7% aller Geschäfte; 2021: 8%), was sich natürlich auch auf die Geschäftszahl auswirkt.

Wie schon im letzten Tätigkeitsbericht vermerkt, stösst das Team des DSB aufgrund der starken Zunahme von Digitalisierungsprojekten an seine Belastungsgrenzen.

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 2022 deutlich gestiegen, nämlich um fast einen Fünftel (19% / 2021: 16%).

Erledigung innert 14 Tagen Von den nicht-komplexen Beratungsgeschäften, also mit höchstens neun Bearbeitungsschritten, wurden im letzten Jahr ein ähnlich grosser Anteil innert 14 Tagen abgeschlossen (43% / 2021: 44%).

Schulungen Der DSB hat im Jahr 2022 acht Schulungen (Vorjahr: 9) durchgeführt, unter anderem zweimal das ganztägige Seminar «Datenschutz und Öffentlichkeitsprinzip – kurz erklärt» und Schulungen für die Mitarbeiter:innen des Arbeitsinspektorats sowie des Empfangs eines Listenspitals.

Initiant:innen und involvierte Stellen Bei den Stellen, die sich an den DSB gewandt haben[12], sind leichte Verschiebungen von den kantonalen öffentlichen Organen (60% / Vorjahr 2021: 67%) hin zu ausserkantonalen Stellen (11% / Vorjahr 2021: 6%) und zu den Privatpersonen (18% / Vorjahr 2021: 14%) festzustellen. Recht stabil blieben aber auch in diesem Jahr die Zahlen bei den Stellen, die in die vom DSB bearbeiteten Geschäften involviert waren.[13]

Personelle Ressourcen des Datenschutzbeauftragten

Team Das Team des Datenschutzbeauftragten setzt sich auch Ende 2022 aus sieben Personen[14] zusammen, die sich 590 Stellenprozente teilen (100% Leitung, 230% Jurist:innen, 180% Informatiker, 80% Assistenz). 10% einer Jurist:innenstelle waren zum Jahreswechsel vakant. Ausserdem bietet der DSB zweimal im Jahr eine sechsmonatige juristische Volontariatsstelle an. Die Besetzung dieser Ausbildungsstelle ist aber deutlich schwieriger geworden; zweimal haben im Berichtsjahr Volontär:innen abgesagt, weil sie inzwischen eine feste Stelle angeboten erhalten haben. Deshalb konnte trotz verstärkter Werbung mindestens die Stelle für das erste Halbjahr 2023 nicht besetzt werden. Da die Volontär:innen, die häufig bereits an der Universität die Vorlesung zum Datenschutzrecht besucht haben und sich beim DSB in einem Bewerbungsverfahren gegen andere Bewerber:innen durchsetzen müssen, spätestens ab dem vierten Monat fast vollwertige Team-Mitglieder sind, fehlt dadurch praktisch ein:e 50%-Mitarbeiter:in.

Belastung Wie schon im letzten Tätigkeitsbericht vermerkt,[15] stösst das Team des DSB aufgrund der starken Zunahme von Digitalisierungsprojekten an seine Belastungsgrenzen. Solche Geschäfte sind regelmässig auch (sehr) komplexe Geschäfte, verlangen eine intensive interdisziplinäre Zusammenarbeit und

stehen häufig auch noch unter Zeitdruck. Mit der Verbesserung des Projektmanagements (siehe dazu vorne S. 23) ist davon auszugehen, dass die Zahl der Vorabkonsultationen (bisher: Vorabkontrollen) zunehmen wird – nicht weil die Vorabkonsultationspflicht ausgeweitet würde, sondern weil die schon seit 2008 bestehende Pflicht endlich besser eingehalten werden dürfte. Zudem bringt die Digitalisierung der Verwaltung, wie sie vom Regierungsrat mit der Digitalisierungsstrategie beabsichtigt ist und deren Wichtigkeit von der Geschäftsprüfungskommission in ihrem letztjährigen Bericht zum Jahresbericht 2021 des Regierungsrates unterstrichen wurde,[16] mehr vorabkonsultationspflichtige Projekte. Der Datenschutzbeauftragte wird Kriterien ausarbeiten, um festzulegen, welche vorabkonsultationspflichtigen Projekte ohne vertiefte Prüfung erledigt werden können. Ausserdem wird heute schon versucht, durch die interkantonale Zusammenarbeit von bereits durch andere Datenschutzaufsichtsbehörden durchgeführten Vorabkonsultationen zu profitieren.

Die Digitalisierung der Verwaltung bringt mehr vorabkonsultationspflichtige Projekte.

Budget 2024 Trotz dieser Bemühungen wird es ohne zusätzliche Ressourcen beim Datenschutzbeauftragten nicht gehen. Er wird deshalb, wie auch schon gegenüber der Datenschutz-Delegation des Büros des Grossen Rates angekündigt, mit seinem Entwurf für das Budget 2024 eine Erhöhung der personellen Ressourcen beantragen.

1 § 1 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 1 N 5 ff.
2 § 44 IDG; vgl. dazu PK-IDG/BS-Schilling, § 44 N 1 ff.
3 Urteil 1C_39/2021 der I. öffentlich-rechtlichen Abteilung des Bundesgerichts vom 29.11.2022 (Änderung des Gesetzes über die Kantonspolizei).
4 Vgl. dazu PK-IDG/BS-Husi, § 22 N 22 und PK-IDG/BS-Baeriswyl, § 14 N 10 ff.
5 TB 2020-2021 des DSB/BS, S. 46 f.
6 § 3 Abs. 1 DMV.
7 TB 2020-2021 des DSB/BS, S. 46, linke Spalte.
8 Vgl. dazu das von privatim in Auftrag gegebene Rechtsgutachten von Astrid Epiney / Sophia Rovelli.
9 Vgl. dazu die Ausführungen im TB 2016 des DSB/BS, S. 41, sowie PK-IDG/BS-Husi, § 9a N 6 ff.
10 Bericht 13.0739.02, S. 5 f.
11 Jahresbericht 2022 (des Regierungsrates), S. 75.
12 Grafik D im Statistikteil (S. 41).
13 Grafik E im Statistikteil (S. 41).
14 Zu den einzelnen Personen siehe Impressum (Umschlagsseite 3).
15 TB 2020-2021 des DSB/BS, S. 48 f.
16 GPK-Bericht 22.5316.01, S. 38 f.

Statistische Auswertungen 2022 (mit Vorjahresvergleich)

A Geschäfte

	2022		2021		2020		2019	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	571		583		543		517	
prozentuale Veränderung gegenüber Vorjahr		-2		7		5		10

B Indikatoren gemäss Budget

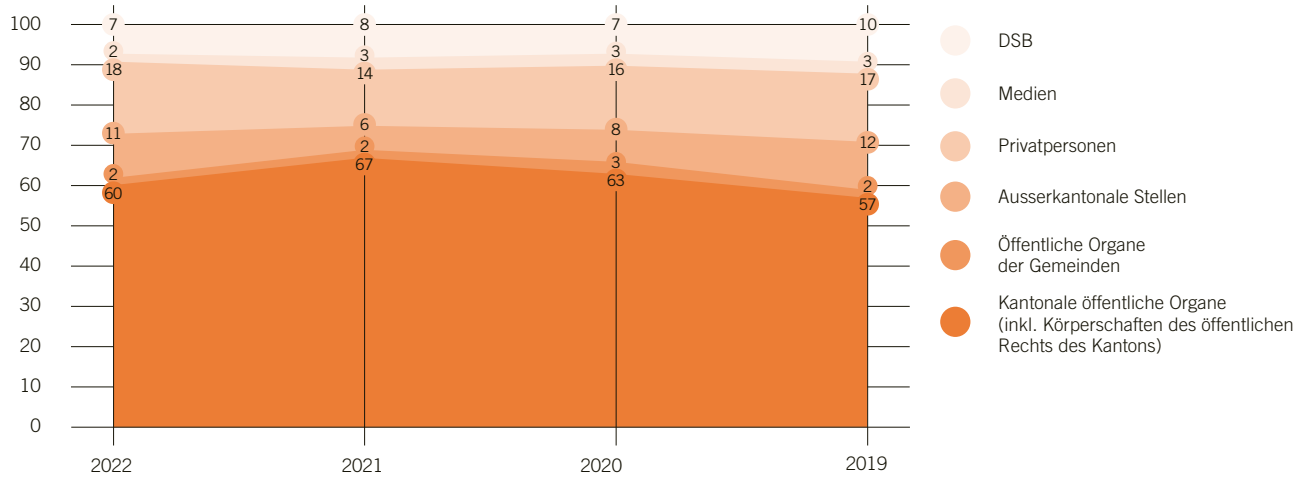
	2022		2021		2020		2019	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		19		16		14		13
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		43		44		48		40
Durchgeführte Audits								
Anzahl durchgeführte Audits	6		1		0		4	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	8		9		6		5	

C Öffentlichkeitsprinzip

	2022		2021		2020		2019	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	30		31		36		24	
prozentuale Veränderung gegenüber Vorjahr		-3		-14		50		4
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche	19	63	13	42	18	50	16	67
Anzahl teilweise gutgeheissener Gesuche	3	10	3	10	2	6	0	0
Anzahl ganz abgewiesener Gesuche	7	23	14	45	11	31	4	17
Anzahl noch nicht rechtskräftig entschiedener Gesuche	1	3	1	3	4	11	4	17
zurückgezogen	0	0	0	0	1	3	0	0

Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen (nicht enthalten sind jeweils die Zahlen zur Staatsanwaltschaft):
Jahresbericht 2022 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2022, S. 75

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %

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

* Rundungsfehler: +1

Anhang

Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

Kanton Basel-Stadt:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

ArchivG Gesetz vom 11. September 1996 über das Archivwesen (Archivgesetz), SG 153.600.

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

DSG/BS Gesetz vom 9. Juni 1993 über den Schutz von Personendaten (Datenschutzgesetz), SG 153.260, in der Version des GRB von GRB vom 16.04.2008 (aufgehoben am 31.12.2011).

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

GOG Gesetz vom 3. Juni 2015 über die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG), SG 154.100.

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).

JVG Gesetz vom 13. November 2019 über den Justizvollzug (Justizvollzugsgesetz, JVG), SG 258.200.

OG Gesetz vom 22. April 1976 betreffend die Organisation des Regierungsrates und der Verwaltung des Kantons Basel-Stadt (Organisationsgesetz, OG), SG 153.100.

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

RAV Verordnung vom 13. Oktober 1998 über die Registraturen und das Archivieren (Registratur- und Archivierungsverordnung), SG 153.610.

revIDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) in der Fassung gemäss dem Grossratsbeschluss vom 20. Oktober 2022.

Materialien (sortiert nach Geschäftsnummer)

Antwort 22.5461.02 Antwort 22.5461.02 des Regierungsrates vom 18.01.2023 auf die Schriftliche Anfrage Danielle Kaufmann betreffend KI-Systemen im Kanton Basel-Stadt (<https://grosserrat.bs.ch/dokumente/100403/000000403870.pdf>).

Schriftliche Anfrage 22.5461.01 Schriftliche Anfrage Danielle Kaufmann vom 20.10.2022 betreffend KI-Systemen im Kanton Basel-Stadt (<https://grosserrat.bs.ch/dokumente/100403/000000403060.pdf>).

Stellungnahme 21.5704.02 Stellungnahme 21.5704.02 des Regierungsrates vom 23.02.2022 zur Motion Thomas Gander und Konsorten zur Schaffung von rechtlichen Grundlagen für die Anwendung von algorithmus-basierter Instrumente in der Polizeiarbeit (<https://grosserrat.bs.ch/dokumente/100396/000000396742.pdf>).

Motion 21.5704.01 Motion 21.5704.01 Thomas Gander und Konsorten vom 27.10.2021 zur Schaffung von rechtlichen Grundlagen für die Anwendung von algorithmus-basierter Instrumente in der Polizeiarbeit, <https://grosserrat.bs.ch/dokumente/100395/000000395705.pdf>.

JSSK-Bericht 21.1239.02 Bericht 21.1239.02 (und 21.5704.03) der Justiz-, Sicherheits- und Sportkommission vom 15. September 2022 zum Ratschlag 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 Thomas Gander und Konsorten zur Schaffung von rechtlichen Grundlagen für die Anwendung von algorithmus-basierter Instrumente in der Polizeiarbeit, <https://grosserrat.bs.ch/dokumente/100402/000000402898.pdf>.

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), <https://grosserrat.bs.ch/dokumente/100395/000000395550.pdf>.

Andere Kantone
Rechtsgrundlagen

Rechtsgrundlagen

IDG/ZH Gesetz (des Kantons Zürich) vom 12. Februar 2007 über die Information und den Datenschutz (IDG), LS 170.4.

Bund:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

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

BVG Bundesgesetz vom 25. Juni 1982 über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG), SR 831.40.

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

DSV Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV) (ersetzt die VDSG per 01.09.2023).

IVG Bundesgesetz vom 19. Juni 1959 über die Invalidenversicherung (IVG), SR 831.20.

KVG Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG), SR 832.10.

revDSG Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG), Referendumsvorlage: BBl 2020 7639.

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

VDSG Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11 (wird per 01.09.2023 abgelöst durch die DSV).

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.

Tätigkeitsberichte

GPK-Bericht 22.5316.01 Rechenschaftsbericht und Bericht 22.5316.01 der Geschäftsprüfungskommission des Grossen Rats des Kantons Basel-Stadt vom 21. Juni 2022 zum Jahresbericht 2021 des Regierungsrats, <https://grosserrat.bs.ch/dokumente/100397/000000397638.pdf>.

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

Astrid Epiney / Sophia Rovelli Astrid Epiney / Sophia Rovelli, Once only und das Rechtsstaatsprinzip, Rechtsgutachten im Auftrag von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten / Once-only et le principe de l'État de droit, Avis de droit sur mandat de privatiom, la Conférence des préposé(e)s suisses à la protection des données, digma-Schriften zum Datenrecht, Band 11, Zürich / Genf 2022.

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.

Positionspapier «Rechtsrahmen für KI» Florent Thouvenin / Markus Christen / Abraham Bernstein / Nadja Braun Binder / Thomas Burri / Karsten Donnay / Lena Jäger / Mariela Jaffe / Michael Krauthammer / Melinda Lohmann / Anna Mätzener / Sophie Mützel / Liliane Obrecht / Nicole Ritter / Matthias Spielkamp / Stephanie Volz, Ein Rechtsrahmen für Künstliche Intelligenz, Positionspapier, 2021, abrufbar unter: https://www.zora.uzh.ch/id/eprint/211386/.

Abkürzungen

AKV Aufgaben, Kompetenzen und Verantwortlichkeiten
BBl Bundesblatt
BFS Bundesamt für Statistik
DSB Datenschutzbeauftragte:r
DSBer Datenschutzberater:in
DSFA Datenschutz-Folgenabschätzung
DTI Bereich Digitale Transformation und IKT-Lenkung (der Bundeskanzlei)
GPK Geschäftsprüfungskommission (des Grossen Rates des Kantons Basel-Stadt)
ISB Kantonale:r Beauftragte:r für Informationssicherheit
ISBD Departementale:r Beauftragte:r für Informationssicherheit
ISMS Informationssicherheits-Managementsystem
IWB Industrielle Werke Basel
JSSK Justiz-, Sicherheits- und Sportkommission (des Grossen Rates des Kantons Basel-Stadt)
KBM Kantonales Bedrohungsmanagement
KI Künstliche Intelligenz
KOI Konferenz für Organisation und Informatik
MS Microsoft
M365 Microsoft 365
OKP Obligatorische Krankenpflegeversicherung
PIA Projektinitialisierungsauftrag
PK (BS) Pensionskasse (Basel-Stadt)
SG Systematische Gesetzessammlung (des Kantons Basel-Stadt)
LS Loseblattsammlung (des Kantons Zürich)
SIK Schweizerische Informatikkonferenz
SIS Schengener Informationssystem
SR Systematische Rechtssammlung (des Bundes)
USB Universitätsspital Basel
UZB Universitäres Zentrum für Zahnmedizin Basel

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

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

Team
Eva Maria Bader (Sekretariat)
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

Volontärinnen/Volontäre:
Colin Carter, MLaw
(1.1.2022 - 30.6.2022)
Sama Bolog, MLaw
(1.7.2022 - 31.12.2022)

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