



Datenschutzbeauftragte des Kantons Basel-Stadt



# 2025

Tätigkeitsbericht

#### Datenschutzbeauftragte

Danielle Kaufmann

#### Stellvertretender Datenschutzbeauftragter

Julian Powell (seit Februar 2025)

#### Juristisches Team

Pascal Lachenmeier

Ines Weihrauch

Barbara Widmer

#### IT-Team

Dimitrios Kallivroussis

Sukhwant Singh

Thomas Sterchi

#### Juristischer Volontär

Kevin Ohler

(seit Februar 2025; ab Oktober 2025 befristet,  
angestellt als juristischer Mitarbeiter)

#### Sekretariat

Eva Maria Bader

Marco Husi (Februar bis Juni 2025)

#### Kontaktinformationen

Henric Petri-Strasse 15

4051 Basel

Telefon: +41 61 267 16 40

E-Mail: datenschutz@dsb.bs.ch

Web: www.dsb.bs.ch

#### Gestaltung

Jenny Hartmann und Team, Basel

Die Datenschutzbeauftragte erstattet dem Grossen Rat und der Öffentlichkeit gestützt auf § 50 Abs. 1 des Informations- und Datenschutzgesetzes (IDG) den folgenden Bericht über Umfang und Schwerpunkte ihrer Tätigkeit, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des IDG.

Der vorliegende Bericht ist als barrierefreies Dokument auf der Webseite der Datenschutzbeauftragten abrufbar. Bis auf die Bilder sind sämtliche Inhalte, insbesondere der Text, ohne die Nutzung von KI-Systemen erstellt worden.

## Inhalt

<b>Die Datenschutzbeauftragte</b>	<b>5</b>
<b>Auslastung und Ressourcen</b>	<b>6</b>
<b>Rückblick: ein Jahr revidiertes IDG</b>	<b>7</b>
<b>Fokusthema: Künstliche Intelligenz (KI)</b>	<b>8</b>

<b>1</b>	<b>Beratungen</b>	<b>12</b>
1.1	Zugriff der Arbeitgeberin auf E-Mails und Daten von verstorbenen Mitarbeitenden	
1.2	Welchen Schutzbedarf haben Personendaten?	
1.3	Einreichung von Steuererklärungen mit Online-Software	
1.4	Schwärzung der Namen von Meldepersonen und Verwaltungsmitarbeitenden bei der Einsichtnahme in Akten	
1.5	Veröffentlichung von Kontaktdaten im Quartier	
1.6	Wesentliche Elemente eines Vernichtungs- und Archivierungskonzepts	
1.7	Hitzemonitoring bei Schulfassaden	
1.8	Publikation von Namen im Rahmen der Provenienzforschung der staatlichen Museen im Kanton Basel-Stadt	
1.9	Organisation eines LGBTQ+ Vernetzungstreffens	
1.10	Berechnung räumlicher Distanz zwischen Menschen mit Behinderung und medizinischen Leistungserbringern	
<b>2</b>	<b>Vorabkonsultationen</b>	<b>17</b>
2.1	Microsoft 365 in der Kantonsverwaltung	
2.2	Microsoft Copilot im Schulbereich	
2.3	Digitalisierung Personalrekrutierung	
2.4	Digitalisierung Mitarbeitendengespräche	
2.5	Ablösung HR-Software bei den Basler Verkehrs-Betrieben (BVB)	
2.6	Digitalisierung der schulärztlichen Dossiers	
2.7	Eurovision Song Contest (ESC) und Fussball-Europameisterschaft der Frauen	
2.8	Videoüberwachung beim Eurovision Song Contest (ESC)	
2.9	Revision der Bau- und Planungsverordnung	
<b>3</b>	<b>Kontrollen</b>	<b>22</b>
3.1	Klinikinformationssystem im Universitäts-Kinderspital beider Basel (UKBB)	
3.2	Nachkontrolle zum Cyberangriff im Erziehungsdepartement	
3.3	Nachkontrolle im Care Management von HR BS	
3.4	Baustellenfortschrittkameras	
3.5	Mobile Überwachungsroboter an der Herbstmesse	
3.6	Kantonales Bedrohungsmanagement	
<b>4</b>	<b>Meldungen von Datenschutzverletzungen</b>	<b>24</b>
4.1	Hintergrund und Zweck	
4.2	Hilfestellungen der DSB	
4.3	Erfolgte Meldungen und Beschreibung ausgewählter Fälle	
<b>5</b>	<b>Schulungen und Sensibilisierung</b>	<b>25</b>
5.1	Neue Merkblätter	
5.2	Fallkonferenzen	
5.3	Bedürfnis-Umfrage bei den Datenschutzberater:innen	
5.4	Mitarbeitendenveranstaltung beim Amt für Wirtschaft und Arbeit	
5.5	Partizipative Arbeitstagung des Bundesamts für Justiz zur Umsetzung der KI-Konvention des Europarats	
<b>6</b>	<b>Zusammenarbeit mit anderen Datenschutzbehörden</b>	<b>27</b>
6.1	Privatim	
6.2	Schengen-Koordinationsgruppe	
<b>7</b>	<b>Personalbestand und Rechnung</b>	<b>29</b>
<b>8</b>	<b>Zahlen zum Berichtsjahr</b>	<b>29</b>
	<b>Dank</b>	<b>35</b>



# Die Datenschutzbeauftragte

Die Datenschutzbeauftragte des Kantons Basel-Stadt (DSB) ist eine unabhängige Aufsichtsbehörde. Sie nimmt Aufgaben im Bereich des Datenschutzrechts und des Öffentlichkeitsprinzips wahr, mit dem Ziel die Grundrechte der Menschen im Kanton Basel-Stadt zu schützen. Insbesondere berät sie öffentliche Organe zum rechtmässigen Umgang mit Informationen sowie Private zu ihren Rechten, nimmt Stellung zu relevanten Datenbearbeitungen und Rechtsetzungsprojekten und kontrolliert die Einhaltung der massgeblichen Gesetzesbestimmungen.

Der vorliegende Tätigkeitsbericht vermittelt anhand einer Auswahl von Fällen einen Einblick in die Praxis der DSB während des Berichtsjahres.

Soweit in diesem Tätigkeitsbericht Aussagen über die Datenschutzbeauftragte als Aufsichtsbehörde gemacht werden, wird jeweils generisch von der «DSB» gesprochen. An den Stellen, an denen sich Aussagen spezifisch auf die Leitung beziehen, wird von der «Beauftragten» (Danielle Kaufmann) gesprochen.

Am vorliegenden Tätigkeitsbericht haben mitgewirkt, neben der Beauftragten Danielle Kaufmann selbst, ihr Stellvertreter Julian Powell, aus dem juristischen Team Pascal Lachenmeier, Ines Wehrauch und Barbara Widmer, aus dem IT-Team Dimitrios Kallivroussis, Sukhwant Singh und Thomas Sterchi, des Weiteren der juristische Volontär und Mitarbeiter Kevin Ohler und aus dem Sekretariat Eva Maria Bader.

# Auslastung und Ressourcen

**Die Geschäftslast der DSB war im Berichtsjahr sehr hoch. Die verfügbaren Ressourcen reichten nur knapp aus, um den gesetzlichen Auftrag zu erfüllen. Ohne zusätzliche Ressourcen besteht das Risiko, dass es zu Engpässen in der Aufgabenerfüllung kommt und der Datenschutz zum Flaschenhals in der Verwaltung wird.**

Mit der zu Beginn des Berichtsjahres in Kraft getretenen Revision des Informations- und Datenschutzgesetzes (IDG) wurden insbesondere der präventive Datenschutz im Projektmanagement ausgebaut, sowie neue Transparenzvorgaben und eine Meldepflicht bei Datenschutzverletzungen eingeführt. Der DSB kommt in all diesen Bereichen eine wichtige Rolle zu. Sei es in der datenschutzrechtlichen Prüfung neuer Vorhaben, in der Beratung der öffentlichen Organe bei der Umsetzung der neuen Pflichten oder in der Beurteilung von erhaltenen Meldungen über Datenschutzverletzungen.

Entsprechend gestaltete sich die Arbeitslast der DSB mit insgesamt 711 bearbeiteten produktiven Geschäften (d. h. exklusive der administrativen Geschäfte) im Berichtsjahr als sehr hoch. Der erweiterte Aufgabenkatalog kann gegenwärtig nur knapp und mit viel Mühe erfüllt werden. Namentlich aufgrund der immer zahlreicheren Digitalisierungsprojekte im Kanton ist absehbar, dass die vorhandenen Ressourcen zur angemessenen Erfüllung des gesetzlichen Auftrages künftig nicht mehr ausreichen werden.

# Rückblick: ein Jahr revidiertes IDG

**Das Berichtsjahr war geprägt von der Umsetzung des revidierten Informations- und Datenschutzgesetzes (IDG), welches am 1. Januar 2025 in Kraft trat.**

Dieses hat insbesondere den präventiven Datenschutz in den Vordergrund gerückt. Mittels einer Schwellwertanalyse müssen öffentliche Organe bei allen geplanten Vorhaben, bei denen Personendaten bearbeitet werden, prüfen, ob ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Liegt ein solches Risiko vor, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. In der DSFA werden die für den Datenschutz relevanten Aspekte des Vorhabens beschrieben. Ebenfalls werden darin die Risiken für die betroffenen Personen bewertet und Massnahmen festgelegt, um diese Risiken zu minimieren. Die öffentlichen Organe legen die DSFA sodann der DSB zur Prüfung im Rahmen einer Vorabkonsultation vor.

Die DSB stellte bereits früh im Berichtsjahr fest, dass in den öffentlichen Organen Unklarheiten zum Inhalt der einzureichenden Unterlagen im Rahmen der DSFA bestanden. Ausserdem erhielt die DSB die Unterlagen in vielen Fällen erst zu einem Zeitpunkt vorgelegt, in dem ihre Empfehlungen, wenn überhaupt, nur mit erheblichem Aufwand umgesetzt werden konnten. Um diesen Prozess für die öffentlichen Organe zu vereinfachen und effizienter zu gestalten, hat die DSB dazu Hilfsmittel auf ihrer neu gestalteten Webseite veröffentlicht. Insbesondere hat sie ein handliches DSFA-Formular ausgearbeitet, welches die Datenschutzerfordernisse transparent macht und die öffentlichen Organe durch den Prozess führt. Die ersten Erfahrungen damit haben gezeigt, dass dadurch der Prozess der Vorabkonsultation für alle involvierten Parteien deutlich verbessert werden konnte.

Die fortschreitende Digitalisierung, namentlich in Bezug auf Cloud-Projekte oder auf die Einführung von Anwendungen der künstlichen Intelligenz (KI), halten die Geschäftslast der DSB hoch. Gleichzeitig geht die DSB davon aus, dass weiterhin eine nicht unwesentliche Anzahl vorabkonsultationspflichtiger Vorhaben aus verschiedenen Gründen nicht (oder nicht rechtzeitig) an sie gelangt. Die DSB erhofft sich, dass die beschriebenen Vereinfachungen im

Vorabkonsultationsprozess und ihre kontinuierliche Sensibilisierungsarbeit künftig zu einer Schliessung dieser Lücke beitragen.

Zu den Vorabkonsultationen, die besonders hervorzuheben sind, weil sie die DSB im Berichtsjahr intensiv beschäftigt haben, zählen die umfassende Umstellung der kantonalen Verwaltung auf die Arbeitsumgebung der Microsoft 365-Cloud, verschiedene Digitalisierungsprojekte bei Human Resources Basel-Stadt (HR BS) sowie diverse Datenbearbeitungen im Zusammenhang mit der Austragung des Eurovision Song Contest (ESC).

Mit dem revidierten IDG wurden neu die Datenschutzberater:innen (DSBer) in den kantonalen Departementen, den Gerichten, den Gemeinden und in bestimmten öffentlich-rechtlichen Anstalten verpflichtend eingeführt. Diese beraten und unterstützen die jeweiligen Organe bei der Einhaltung der Datenschutzbestimmungen, insbesondere bei der Erstellung der DSFA, und arbeiten mit der DSB zusammen. Aus Sicht der DSB haben sich die DSBer mehrheitlich bereits gut etabliert, auch wenn sie leider teilweise immer noch nicht so in die Projekte eingebunden werden, wie es für den Datenschutz am zielführendsten wäre. Gemeinsam mit dem kantonalen Informationssicherheitsbeauftragten hat die DSB im Berichtsjahr, insbesondere für die DSBer, eine Reihe von Schulungsveranstaltungen durchgeführt, um die Vernetzung und die Weitergabe von Datenschutzwissen zu fördern.

Eine zentrale Neuerung im revidierten IDG ist die Präzisierung der Informationspflicht, wonach öffentliche Organe betroffene Personen proaktiv über die Beschaffung von Personendaten informieren müssen – auch wenn diese bei Dritten erhoben werden. Die öffentlichen Organe müssen insbesondere transparent darlegen, welche Daten sie zu welchen Zwecken bearbeiten, gestützt auf welcher rechtlichen Grundlage sie dies tun und wem sie die Daten allenfalls bekannt geben. Ausnahmen von dieser Pflicht bestehen, wenn die Informationen bereits bekannt sind, die Datenbearbeitung ausdrücklich gesetzlich geregelt ist oder ein unverhältnismässiger Aufwand entstehen würde.

Es ist vermutlich zumindest teilweise den Neuerungen im IDG geschuldet, dass die Beratungen weiterhin den grössten Anteil an Geschäften der DSB ausmachen. Gerade aufgrund der Gesetzesrevision – aber nicht nur – bestehen in den öffentlichen Organen und in der Bevölkerung nach wie vor viele Fragen zum Datenschutz. In diesem Kontext bleibt die Unterstützung durch die DSB unabdingbar.

# Fokusthema: Künstliche Intelligenz (KI)

**Mit der voranschreitenden Digitalisierung und der Verbreitung von Anwendungen der künstlichen Intelligenz (KI), sind auch öffentliche Organe im Kanton Basel-Stadt zunehmend am Einsatz von KI-Lösungen interessiert. Die DSB wurde im Berichtsjahr mehrmals um Beratung im Zusammenhang mit KI-Fragen ersucht und ihr wurden diverse KI-Projekte zur Vorabkonsultation vorgelegt. Die allgemeinen Datenschutzvorgaben gelten ohne Weiteres auch für KI-Anwendungen. Allerdings muss auch den besonderen Risiken von KI-Anwendungen angemessene Rechnung getragen werden.**

Ausschlaggebend ist zunächst das Legalitätsprinzip. Demnach sind öffentliche Organe – im Gegensatz zu Privaten – insbesondere an die Grundrechte gebunden und benötigen für ihre Handlungen jeweils eine gesetzliche Grundlage. Bei der Initialisierung eines KI-Projekts – gleich wie bei anderen Projekten, bei denen Personendaten bearbeitet werden – muss das verantwortliche öffentliche Organ zunächst prüfen, ob das Vorhaben auf den bestehenden Rechtsrahmen abgestützt werden kann oder ob dafür neue Gesetzesbestimmungen erlassen werden müssen. Diese Prüfung erfolgt im Rahmen einer Rechtsgrundlagenanalyse. Sie setzt juristisches Fachwissen voraus, weshalb in der Regel entweder der Rechtsdienst oder eine externe Expertise dafür beizuziehen sind. Wie bestimmt und auf welcher Normstufe (Gesetz oder Verordnung) die betreffende Rechtsgrundlage sein muss, um für den Einsatz einer KI-Anwendung zu genügen, hängt von der Ausgestaltung des Vorhabens und den konkreten Risiken für die betroffenen Personen ab.

Der Einsatz von KI-Anwendungen kann eine Reihe von Risiken für betroffene Personen bergen. Viele KI-Systeme basieren auf maschinellem Lernen. Solche Systeme generieren Inhalte, treffen Vorhersagen oder Entscheidungen aufgrund von statistischen Algorithmen, d. h. aufgrund von Wahrscheinlichkeitsberechnungen. Dadurch bleiben die Ergebnisse solcher KI-Systeme intransparent («Black Box»), unvorhersehbar und fehleranfällig. Unter anderem sind Entscheide, die auf maschinellem Lernen beruhen, oftmals nicht vollständig nachvollziehbar und können gegenüber den betroffenen Personen deshalb auch nicht abschliessend begründet werden. Insbesondere je nach Qualität der Daten, mit denen ein KI-Modell trainiert wurde, können die generierten Ergebnisse durch Vorurteile («Biases») beeinflusst sein. Dies kann zu Diskriminierungen und Fehlern führen. Bei bestimmten KI-Anwendungen werden die von den Nutzenden eingegebenen Daten nicht nur für die unmittelbare Aufgabe (z. B. Textverbesserung), sondern von der KI-Anbieterin für das Training eigener KI-Modelle weiterverwendet. Dies widerspricht dem datenschutzrechtlichen Grundsatz der Zweckbindung.

Die Einführung neuer KI-Anwendungen erfordert teilweise auch die Schaffung neuer Rechtsgrundlagen.

KI-Anwendungen werden oftmals von Drittanbietern in einer Cloud-Umgebung betrieben. Deshalb sind bei solchen KI-Anwendungen nicht nur die soeben beschriebenen Risiken von Bedeutung, sondern auch allgemeinere Risiken im Zusammenhang mit der Bearbeitung von Personendaten in der Cloud. Zu diesem Thema hat privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, im Berichtsjahr eine Resolution verabschiedet. Viele der Cloud-Risiken ergeben sich aus dem Kontrollverlust, welcher entstehen kann, wenn öffentliche Organe umfangreiche Datenbearbeitungen in eine Cloud auslagern. Dies gilt insbesondere für Software-as-a-Service-Lösungen (SaaS), bei welchen ein Zugriff der Cloud-Anbieterin nur vertraglich, aber nicht faktisch unterbunden werden kann.

Erfreulicherweise kann die DSB feststellen, dass das Bewusstsein für die mit KI-Anwendungen verbundenen Risiken in diversen öffentlichen Organen des Kantons Basel-Stadt bereits fest verankert ist. Entsprechend entwickelten das Statistische Amt und IT BS im Berichtsjahr eine Palette von KI-Anwendungen als Hilfsmittel in der täglichen Arbeit für Mitarbeitende der kantonalen Verwaltung. Die DSB prüfte das Projekt im Vorfeld und ihre Empfehlungen wurden umgesetzt. Diese KI-Anwendungen (zur Übersetzung, Textverbesserung und Transkription) werden in der kantonseigenen Infrastruktur («on-premise») betrieben. Die Eingaben der Nutzenden und die generierten Inhalte verlassen das kantonsinterne Netzwerk zu keiner Zeit und werden auch nicht gespeichert (ausser von den Nutzenden selbst).

Um Klarheit im Umgang mit online verfügbaren, kantonsexternen KI-Anwendungen (z. B. ChatGPT, Copilot, DeepL etc.) zu schaffen, verabschiedete der Regierungsrat im Berichtsjahr auch eine entsprechende KI-Richtlinie. Bei der Erarbeitung der Richtlinie ist die DSB in beratender Rolle massgeblich beteiligt gewesen. Die Richtlinie weist auf die wichtigsten Grundsätze und Risiken hin und stellt klar, dass Personendaten und Daten, die einer Geheimhaltungspflicht (insbesondere dem Amts- und Berufsgeheimnis) unterstehen, nicht in solche KI-Anwendungen eingegeben werden dürfen.

Gleichzeitig beobachtet die DSB, dass unter den Mitarbeitenden der öffentlichen Organe weiterhin viele offene Fragen im Zusammenhang mit KI bestehen. Auch der Umgang mit dem Thema variiert stark von Organ zu Organ. Soweit es ihre Ressourcen zulassen, wird die DSB weiterhin darauf hinwirken, die Sensibilisierung für den Datenschutz beim Einsatz von KI-Anwendungen zu fördern. Ferner wird sie sich für eine angemessene Regulierung einsetzen, welche die Grundrechte der betroffenen Personen vor KI-Risiken schützt.

# 1

## 1 Beratungen

- 1.1 Zugriff der Arbeitgeberin auf E-Mails und Daten von verstorbenen Mitarbeitenden
- 1.2 Welchen Schutzbedarf haben Personendaten?
- 1.3 Einreichung von Steuererklärungen mit Online-Software
- 1.4 Schwärzung der Namen von Meldepersonen und Verwaltungsmitarbeitenden bei der Einsichtnahme in Akten
- 1.5 Veröffentlichung von Kontaktdaten im Quartier
- 1.6 Wesentliche Elemente eines Vernichtungs- und Archivierungskonzepts
- 1.7 Hitzemonitoring bei Schulfassaden
- 1.8 Publikation von Namen im Rahmen der Provenienzforschung der staatlichen Museen im Kanton Basel-Stadt
- 1.9 Organisation eines LGBTIQ+ Vernetzungstreffens
- 1.10 Berechnung räumlicher Distanz zwischen Menschen mit Behinderung und medizinischen Leistungserbringern

# 2

## 2 Vorabkonsultationen

- 2.1 Microsoft 365 in der Kantonsverwaltung
- 2.2 Microsoft Copilot im Schulbereich
- 2.3 Digitalisierung Personalrekrutierung
- 2.4 Digitalisierung Mitarbeitendengespräche
- 2.5 Ablösung HR-Software bei den Basler Verkehrs-Betrieben (BVB)
- 2.6 Digitalisierung der schulärztlichen Dossiers
- 2.7 Eurovision Song Contest (ESC) und Fussball-Europameisterschaft der Frauen
- 2.8 Videoüberwachung beim Eurovision Song Contest (ESC)
- 2.9 Revision der Bau- und Planungsverordnung

# 3

## 3 Kontrollen

- 3.1 Klinikinformationssystem im Universitäts-Kinderspital beider Basel (UKBB)
- 3.2 Nachkontrolle zum Cyberangriff im Erziehungsdepartement
- 3.3 Nachkontrolle im Care Management von HR BS
- 3.4 Baustellenfortschrittkameras
- 3.5 Mobile Überwachungsroboter an der Herbstmesse
- 3.6 Kantonales Bedrohungsmanagement

# 4

## 4 Meldungen von Datenschutzverletzungen

- 4.1 Hintergrund und Zweck
- 4.2 Hilfestellungen der DSB
- 4.3 Erfolgte Meldungen und Beschreibung ausgewählter Fälle

# 5

## 5 Schulungen und Sensibilisierung

- 5.1 Neue Merkblätter
- 5.2 Fallkonferenzen
- 5.3 Bedürfnis-Umfrage bei den Datenschutzberater:innen
- 5.4 Mitarbeitendenveranstaltung beim Amt für Wirtschaft und Arbeit
- 5.5 Partizipative Arbeitstagung des Bundesamts für Justiz zur Umsetzung der KI-Konvention des Europarats

# 6

## 6 Zusammenarbeit mit anderen Datenschutzbehörden

- 6.1 Privatim
- 6.2 Schengen-Koordinationsgruppe

# 7

## 7 Personalbestand und Rechnung

# 8

## 8 Zahlen zum Berichtsjahr

# 1 Beratungen

## Die DSB berät die öffentlichen Organe im Kanton Basel-Stadt zur Einhaltung der Datenschutzvorgaben und zum Öffentlichkeitsprinzip. Auf diesem Gebiet berät die DSB auch Privatpersonen zu ihren Rechten.

### 1.1 Zugriff der Arbeitgeberin auf E-Mails und Daten von verstorbenen Mitarbeitenden

#### Ausgangslage

Eine Amtsstelle des Departements für Wirtschaft, Soziales und Umwelt (WSU) wandte sich an die DSB mit Fragen im Zusammenhang mit dem Zugriff auf Daten eines verstorbenen Mitarbeiters. Konkret hatten sich einerseits Angehörige bei der Behörde erkundigt, ob auf dem Geschäftslaptop des Verstorbenen eventuell noch Fotos zu finden seien (z. B. von Geschäftsanlässen) und gebeten, ihnen diese gegebenenfalls auszuhändigen. Andererseits wollte die Behörde wissen, wie vorzugehen sei, wenn Vorgesetzte auf geschäftsrelevante E-Mails des Verstorbenen zugreifen möchten.

#### Beratung

Im konkreten Fall riet die DSB bezüglich der Herausgabe von Fotos zunächst verschiedene Sachverhaltsfragen zu klären: unter anderem erschienen der «Suchauftrag» der Angehörigen und die Erforderlichkeit des Zugriffs auf den Geschäftslaptop für Bilder des Geschäftsanlasses noch zu vage. Weiter wies die DSB das öffentliche Organ darauf hin, dass auch weitere Personen von einer Herausgabe der Fotos betroffen sein könnten und deren Persönlichkeitsrechte zu berücksichtigen seien. So empfahl die DSB dem öffentliche Organ grundsätzlich, vor der Herausgabe von Fotos von Geschäftsanlässen die Einwilligung weiterer auf den Fotos erkennbarer Personen einzuholen. Bezüglich des Zugriffs auf geschäftsrelevante E-Mails empfahl die DSB in genereller Hinsicht vor allem zu beachten, dass

- der Zugriff von der Leitung bewilligt werde,
- der Zugriff gemäss dem Vier-Augen-Prinzip erfolge, oder dafür eine externe, neutrale Stelle beauftragt werde,
- der Zugriff zeitlich zu befristen sei,
- zu protokollieren sei, wer auf welche Daten zugreift, und
- auf als privat gekennzeichnete oder offensichtlich als privat erkennbare Daten und Ordner nicht zugegriffen werden dürfe.

Losgelöst vom konkreten Fall regte die DSB an, den Zugriff auf Informatikmittel bei unvorhergesehenen Abwesenheiten oder Todesfällen von Mitarbeitenden zu regeln. Die zuständigen Stellen haben sich zwischenzeitlich dem Thema angenommen und die Erarbeitung einer Regelung für die gesamte Kantonsverwaltung in Aussicht gestellt.

### 1.2 Welchen Schutzbedarf haben Personendaten?

#### Ausgangslage

Mehrere öffentliche Organe der kantonalen Zentralverwaltung erkundigten sich während des Berichtsjahres danach, welcher Schutzbedarf für «gewöhnliche» Personendaten bzw. für besondere Personendaten gelte. Teilweise beriefen sich die öffentlichen Organe auf die Weisung «Schutzmassnahmen – Informationssicherheit (Schutzkatalog)», welche am 18. Dezember 2024 von der kantonalen Konferenz für Organisation und Informatik (KOI) verabschiedet worden ist. Darin sind drei Schutzbedarfsstufen für Informationen vorgesehen: Grundschutz (GS), erhöhter Schutzbedarf (ES) und sehr hoher Schutzbedarf (SHS). Diese Schutzbedarfsstufen gelten jeweils für die verschiedenen Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität sowie Zurechenbarkeit und Nachvollziehbarkeit. Die Weisung listet im Rahmen des Schutzziels Vertraulichkeit pro Schutzbedarfsstufe diverse Kategorien von Informationen als Beispiele auf. Insbesondere werden die besonderen Personendaten der Schutzstufe ES zugeordnet, während die «gewöhnlichen» Personendaten keine Erwähnung finden.

#### Beratung

Die DSB wies darauf hin, dass sich die Weisung «Schutzmassnahmen – Informationssicherheit (Schutzkatalog)» primär mit der Informationssicherheit befasse. Diese verfolge teilweise ähnliche, aber nicht identische Ziele wie der Datenschutz. Der Datenschutz fokussiere auf den Schutz des Grundrechts der informationellen Selbstbestimmung der betroffenen Personen. Der Schutzbedarf von Personendaten könne nicht pauschal und abstrakt bestimmt werden.

Vielmehr müsse dieser im Einzelfall anhand einer Gesamtbetrachtung der konkreten Umstände und des Kontextes ermittelt werden. Vermutungsweise könne bei besonderen Personendaten mindestens von einem erhöhten Schutzbedarf ausgegangen werden. Die DSB betonte jedoch, dass der Umkehrschluss, wonach «gewöhnliche» Personendaten grundsätzlich nur im Grundsatzschutz liegen würden, nur teilweise zutrefte. Es gäbe «gewöhnliche» Personendaten, welche zwar grundsätzlich nicht als besondere Personendaten gelten, jedoch aufgrund des Kontextes einen erhöhten Schutzbedarf erfordern würden. Das könne etwa bei Wohnadressen der Fall sein, wenn durch deren Offenlegung die Betroffenen unter Umständen einer Gefährdung ausgesetzt werden könnten.

### 1.3 Einreichung von Steuererklärungen mit Online-Software

#### Ausgangslage

Mithilfe von BalTax Download war es früher möglich, Steuererklärungen komplett elektronisch auszufüllen und einzureichen. Seit dem 1. Februar 2025 wird BalTax Download nicht mehr angeboten. Ersetzt wurde dieses Programm, durch BalTax Online, welches weiterhin viele von BalTax Download bekannten Funktionen zum digitalen Ausfüllen und Einreichen von Steuererklärungen bietet. Für die Nutzung von BalTax Online müssen sich die Nutzenden im ePortal des Kantons Basel-Stadt registrieren. Die Authentifizierung der Nutzenden erfolgt mit dem Behörden-Login AGOV des Bundes.

Mehrere Privatpersonen äusserten gegenüber der DSB Bedenken bezüglich der Sicherheit und des Datenschutzes bei der Umstellung auf BalTax Online und der Nutzung der AGOV-App. Zudem bestanden Unsicherheiten bezüglich der Möglichkeit, Steuererklärungen künftig weiterhin auf Papier auszufüllen. Die DSB beriet die betroffenen Privatpersonen.

#### Beratung

Die Bedienung von BalTax Online entspricht weitgehend derjenigen von BalTax Download. Nutzende benötigen eine Internetverbindung, da die Steuererklärungen direkt auf den lokalen Servern der Steuerverwaltung gespeichert werden. Für die Verwendung von BalTax Online muss somit keine Software heruntergeladen oder installiert werden. Nach Angaben der Steuerverwaltung bietet die Online-Lösung grössere Sicherheit und eine medienbruchfreie Behandlung der Steuererklärung, da der separate Versand der Steuerunterlagen nicht mehr nötig ist und das Login-Verfahren mit AGOV über eine besonders starke Authentifizierung verfügt.

Aus Sicht der DSB war entscheidend, dass Steuererklärungen weiterhin in Papierform ausgefüllt und per Post eingereicht werden können. Es sind der DSB auch keine Absichten bekannt, die Papiersteuererklärungen abzuschaffen. Somit steht Nutzenden weiterhin eine Alternative zu BalTax Online zur Verfügung.

### 1.4 Schwärzung der Namen von Meldepersonen und Verwaltungsmitarbeitenden bei der Einsichtnahme in Akten

#### Ausgangslage

Eine Privatperson wandte sich an die DSB mit der Frage, ob bzw. unter welchen Voraussetzungen es zulässig sei, Namen von Mitarbeitenden der kantonalen Verwaltung in den Akten eines Tierschutzfalls aus Datenschutzgründen zu schwärzen. Weiter bat sie um Auskunft darüber, ob der Name der Person, die den Verdacht auf einen Verstoss gegen eine artgerechte Tierhaltung meldet, gegenüber der von den Vorwürfen betroffenen Person offengelegt werden müsse.

#### Beratung

Die DSB teilte mit, dass die Bekanntgabe oder der Zugang zu Informationen im Anwendungsbereich des Informations- und Datenschutzgesetzes (IDG) eingeschränkt werden könne, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegenstehe. Das heisst, unter dem Vorbehalt einer spezialgesetzlichen Regelung sei bei beiden Sachverhalten eine Abwägung der sich gegenüberstehenden Interessen vorzunehmen. So kämen z. B. bezüglich der Preisgabe der Identität der meldenden Person im Bereich des Tierschutzes die Abwägung des öffentlichen Interesses an einer hohen Meldebereitschaft gegenüber dem privaten Interesse der meldenden Person am Schutz vor einer ernsthaften Gefährdungssituation in Betracht. Auch bei der Prüfung der Schwärzung von Namen von Angestellten, die in Erfüllung ihrer öffentlichen Aufgabe gehandelt haben, könne eine Gefährdungssituation unter Umständen eine Anonymisierung rechtfertigen. Grundsätzlich müssten hierfür aber konkrete Anhaltspunkte vorliegen. Weiterhin könne die Funktion und Stellung von Verwaltungsmitarbeitenden Einfluss auf die Gewichtung ihrer privaten Interessen haben. So würde das Interesse am Persönlichkeitsschutz von Verwaltungsmitarbeitenden mit Entscheidungskompetenzen und in Führungsfunktionen grundsätzlich weniger stark gewichtet als dasjenige von hierarchisch nachgeordneten Verwaltungsmitarbeitenden.

## 1.5 Veröffentlichung von Kontaktdaten im Quartier

### Ausgangslage

Eine Anwohnerin aus dem Matthäusquartier in Basel beschwerte sich bei der DSB, dass ihre Kontaktdaten (Name, Wohnadresse, Telefonnummer und E-Mail-Adresse) ohne ihre Einwilligung von der Kantons- und Stadtentwicklung auf einem öffentlichen Anschlagsbrett publiziert worden seien. Die Veröffentlichung war offenbar mit dem Ziel erfolgt, die Vernetzung der Anwohnenden im Rahmen des sogenannten Superblocks, einem Testprojekt zur Verkehrsberuhigung von Quartiersstrassen, zu erleichtern.

### Beratung

Die DSB klärte den Sachverhalt ab und wies die Kantons- und Stadtentwicklung darauf hin, dass eine Veröffentlichung der Kontaktdaten, auch wenn diese zum nachvollziehbaren Zweck der nachbarschaftlichen Unterstützung und Vernetzung erfolgt war, dennoch die Einwilligung der betroffenen Anwohnenden benötige. Sie empfahl, die Einwilligung schriftlich mittels eines Informationsschreibens einzuholen und gleichzeitig auch der gesetzlichen Informationspflicht nachzukommen. Dadurch könne gewährleistet werden, dass die betroffenen Personen transparent über den Zweck der Datenbearbeitung und Veröffentlichung sowie ihre Rechte aufgeklärt würden.

## 1.6 Wesentliche Elemente eines Vernichtungs- und Archivierungskonzepts

### Ausgangslage

Die DSB wurde auch im Berichtsjahr wieder nach der zulässigen Aufbewahrungsdauer von Akten gefragt und was es in diesem Zusammenhang zu berücksichtigen gelte.

### Beratung

Die DSB informierte über die massgeblichen Bestimmungen im Informations- und Datenschutzgesetz (IDG). Danach seien nicht mehr benötigte Daten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, vom öffentlichen Organ zu vernichten. Zudem seien für Informationsbestände, die Personendaten enthalten, Fristen für die Vernichtung beziehungsweise für die Überprüfung, ob die Daten noch zur Aufgabenerfüllung erforderlich sind, festzulegen. Ab wann die Personendaten nicht mehr zur Erfüllung ihrer gesetzlichen Aufgaben benötigt werden, müsse unter Vorbehalt spezialgesetzlicher Aufbewahrungs- oder Vernichtungsfristen das verantwortliche öffentliche Organ festlegen. In

der Regel ergebe sich aus der Anwendung dieser Grundsätze die Notwendigkeit der Bildung von verschiedenen Kategorien von Personendaten wie z. B. Personaldaten, Klient:innendaten, Finanzdaten o.ä. Auch innerhalb dieser Kategorien sei eine differenzierte Klassifizierung zu prüfen, die sicherstelle, dass nicht mehr benötigte Daten tatsächlich vernichtet werden.

Die DSB riet dazu, sämtliche Erkenntnisse betreffend Datenkategorien, internen Aufbewahrungsfristen mit sachlicher Begründung, gesetzlichen Fristen und entsprechenden Rechtsgrundlagen sowie Prozesse und Verantwortlichkeiten in einem Vernichtungs- und Archivierungskonzept festzuhalten. Bei der Festlegung der Fristen gelte es insbesondere auch den Beginn der laufenden Frist abstrakt (d. h. z. B. «seit Erhebung» oder «seit Austritt») und konkret (Datum) sowie den vorgesehenen Termin der Vernichtung oder der allfälligen Abgabe an das Archiv im konkreten Fall zu bezeichnen. Bezüglich einer allfälligen Archivierung riet die DSB auch, frühzeitig mit der für die Archivierung zuständigen Stelle (im vorliegenden Fall mit dem kantonalen Staatsarchiv) Kontakt aufzunehmen. Schliesslich sensibilisierte die DSB in diesem Zusammenhang die Fragestellerin auch in Bezug auf die Datensparsamkeit bei der Erhebung von Personendaten.

## 1.7 Hitzemonitoring bei Schulfassaden

### Ausgangslage

Aufgrund der stetigen Hitzezunahme in den vergangenen Jahren wollte die Abteilung Städtebau & Architektur des Bau- und Verkehrsdepartements im Rahmen eines Pilotversuchs mittels Fassadenkameras das Lüftungs- und Beschattungsverhalten an den Schulstandorten aufzeichnen. Die Fachhochschule Nordwestschweiz (FHNW) sollte anschliessend mithilfe einer KI-Anwendung die Daten auswerten. Zur Umsetzung dieses Vorhabens war geplant, an einem gegenüberliegenden Gebäude eine Kamera zu installieren, die stündlich ein Bild der Schulfassaden erstellen und so aufzeigen sollte, wie sich das Lüftungs- und Beschattungsverhalten der Nutzenden gestaltet. Die Abteilung Städtebau & Architektur kontaktierte die DSB, um sich dazu beraten zu lassen, ob und wie sich ein solches Vorgehen datenschutzkonform ausgestalten lasse.

### Beratung

Die DSB wies darauf hin, dass die Kameraeinstellungen (Bildauflösung und Kamerawinkel) dergestalt zu wählen seien, dass Personen, die sich hinter

den Fenstern befinden oder Fenster öffnen, nicht identifizierbar seien. Die DSB riet weiter dazu, mit der FHNW für die KI-Auswertung der Aufnahmen eine vertragliche Vereinbarung zu treffen, die den Umgang der FHNW mit den Daten regle. Im Weiteren wies die DSB darauf hin, die Eltern- und Schülerschaft der betroffenen Klassenzimmer vor Installation der Kamera darüber zu informieren, dass keine Aufzeichnungen von identifizierbaren Personen gemacht würden.

## 1.8 Publikation von Namen im Rahmen der Provenienzforschung der staatlichen Museen im Kanton Basel-Stadt

### Ausgangslage

Im Rahmen der 2023 erfolgten Revision des Museumsgesetzes, hat der Grosse Rat die Museen zur Provenienzforschung verpflichtet. Gemäss § 5 Abs. 1<sup>quater</sup> des Museumsgesetzes müssen die Museen neu bei Erwerbungen und Sammlungsobjekten deren rechtmässige Herkunft erforschen und die Ergebnisse der Öffentlichkeit zur Verfügung stellen. Die Abteilung Kultur des Präsidialdepartements wandte sich in diesem Zusammenhang bereits Ende 2024, noch vor dem Inkrafttreten des revidierten Gesetzes, mit datenschutzrechtlichen Fragen an die DSB. Konkret stellte sich einerseits die Frage, ob die neue Bestimmung im Museumsgesetz eine ausreichende gesetzliche Grundlage für die Bearbeitung von gewöhnlichen und allenfalls auch von besonderen Personendaten darstelle und wie andererseits im Einzelfall vorzugehen sei, wenn noch lebende Personen die Veröffentlichung ihrer Namen nicht erlauben würden.

### Beratung

Im Zusammenhang mit der Provenienzforschung wies die DSB darauf hin, dass das Informations- und Datenschutzgesetz (IDG) grundsätzlich nur auf die Bearbeitung von Daten über lebenden Personen zur Anwendung komme. Daher stünde einer Publikation von Namen Verstorbener aus Datenschutzsicht grundsätzlich nichts entgegen, wobei der Einzelfall dennoch zu prüfen sei. Insbesondere sei allenfalls bei der Bearbeitung von Personendaten Verstorbener das Persönlichkeitsrecht derer Angehörigen zu beachten. Bezüglich der Veröffentlichung von Namen noch lebender Personen, beantwortete die DSB die Fragen nach der Zulässigkeit einerseits vor und andererseits nach Inkrafttreten des neuen Gesetzes, da dieses während der Beratung in Kraft gesetzt wurde.

Vor Inkrafttreten des neuen Museumsgesetzes per 1. Januar 2025 verfügten die Museen nach Auffassung der DSB über keine gesetzliche Grundlage, um im Rahmen der Provenienzforschung Namen zu veröffentlichen. Daher empfahl die DSB, Namen noch lebender Personen ausschliesslich mit deren Einwilligung zu publizieren. Mit dem revidierten Museumsgesetz wurde eine gesetzliche Grundlage im Sinne von § 9 Abs. 1 lit. a IDG geschaffen, welche die Museen verpflichtet, Provenienzforschung zu betreiben und die Ergebnisse, gegebenenfalls inklusive Namen von involvierten Personen, zu veröffentlichen. Mangels Bestimmtheit hinsichtlich der Nennung der konkret zu publizierenden Daten ist § 5 Abs. 1<sup>quater</sup> des Museumsgesetzes nach Auffassung der DSB dagegen keine ausreichende gesetzliche Grundlage im Sinne von § 9 Abs. 2 IDG für die Publikation von besonderen Personendaten (z. B. Daten über Strafverfahren).

## 1.9 Organisation eines LGBTIQ+ Vernetzungstreffens

### Ausgangslage

Eine Abteilung von Human Resources Basel-Stadt (HR BS) plante im Berichtsjahr ein freiwilliges Vernetzungstreffen für LGBTIQ+ Mitarbeitende und schaltete dafür ein Anmeldeformular mit Microsoft Forms auf. Die DSB wurde darauf aufmerksam und wandte sich proaktiv an HR BS.

### Beratung

Die DSB wies darauf hin, dass die Daten, welche im Kontext der Anmeldung für ein LGBTIQ+ Vernetzungstreffen gesammelt werden, als besonders sensitiv zu betrachten seien, da sie potenziell Rückschlüsse auf die sexuelle Orientierung und die Intimsphäre der Teilnehmenden zulassen würden. Neben Bedenken an der Erhebung dieser Angaben durch HR BS selbst, äusserte die DSB auch Zweifel gegenüber dem Datenschutz bei Microsoft Forms als Cloud-Lösung, da der Kanton dadurch die Kontrolle über die Daten verliere. Im Rahmen der Diskussion zeigte sich, dass die Daten primär für die Bestellung der ausreichenden Menge an Verpflegung am Treffen benötigt wurde. Die DSB vermittelte eine Zusammenarbeit mit dem Statistischen Amt des Kantons, welches die entsprechenden Angaben mithilfe einer Umfrage unter Beachtung des Statistikgesetzes erhob, ohne das HR BS Angaben zur Identität der Teilnehmenden erhielt.

### 1.10 Berechnung räumlicher Distanz zwischen Menschen mit Behinderung und medizinischen Leistungserbringern Ausgangslage

Die Abteilung Behindertenhilfe des Amtes für Sozialbeiträge wollte, im Rahmen der Bedarfsermittlung, die Distanz zwischen Leistungserbringern und unterstützten Personen bestimmen. In der ursprünglich angedachten Lösung sollten die Adressen, von Leistungserbringern und unterstützten Personen, an Google Maps (oder ähnlichen Diensten) übermittelt werden, um die Route (Distanz und Wegzeit) berechnen zu lassen.

#### Beratung

Die DSB gab zu bedenken, dass durch die Routenberechnung zwischen medizinischen Dienstleistern und unterstützten Personen, ein externer Anbieter, wie beispielsweise Google, Rückschlüsse auf die Gesundheit, der an der Adresse wohnhaften Person, ziehen könne. Es zeigte sich jedoch, dass für die Abteilung Behindertenhilfe nicht die präzise Distanz oder Wegzeit entscheidend waren, sondern allein eine Berechnung der Distanzen nach Zonen im Kanton. Die DSB riet daher, anstelle der Adressen, Koordinaten zu verwenden und deren Genauigkeit so weit zu reduzieren, dass die Ausgangs- und Zieladressen nicht mehr eindeutig bestimmbar seien, während eine ausreichend aussagekräftige Berechnung der Distanz bzw. Wegzeit möglich bleibe. Für die Umsetzung hat die DSB wiederum den Kontakt zum Statistischen Amt des Kantons vermittelt, welches sowohl über die erforderlichen Daten wie auch über die Fachkompetenz verfügt, um die Abteilung Behindertenhilfe bei der Umsetzung dieses Vorhabens zu unterstützen.

In diesem und dem vorangehenden Beratungsfall (LGBTIQ+ Treffen) machte die DSB darauf aufmerksam, dass die anvisierten Ziele auch ohne die Bekanntgabe von (sensitiven) Daten an externe Stellen erreicht werden konnten. Die Zusammenarbeit mit dem Statistischen Amt erwies sich als datenschutzrechtlich verhältnismässiger und sogar ressourceneffizienter.

## 2 Vorabkonsultationen Die Vorabkonsultation der DSB ist ein wichtiges Instrument zum präventiven Schutz der Grundrechte. Dabei prüft die DSB im Voraus neue risikoreiche Datenbearbeitungsvorhaben und relevante Rechtsetzungsprojekte. Bei Bedarf gibt sie Empfehlungen ab. Die Vorabkonsultationen tragen dazu bei, dass Risiken für die Grundrechte frühzeitig erkannt und durch geeignete Massnahmen minimiert werden.

### 2.1 Microsoft 365 in der Kantonsverwaltung Ausgangslage

Der Regierungsrat hat sich bereits im Jahr 2022 für die grundsätzliche Einführung der Cloud-Lösung Microsoft 365 (M365) in der kantonalen Verwaltung ausgesprochen. Daraufhin begann die DSB (noch unter anderer Leitung) einen iterativen Prüfungsprozess.

#### Beurteilung

Die DSB gab dem federführenden Finanzdepartement (FD) ihre Einschätzung zu den Projektunterlagen laufend und strukturiert in Form von mehreren Berichten ab. Sie stützte sich bei ihrer Beurteilung stets auf das Cloud-Merkblatt von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Unter Berufung darauf, wies sie das FD insbesondere wiederholt darauf hin, dass sich aus der Auslagerung besonderer Personendaten in die Microsoft-Cloud erhebliche Risiken für die betroffenen Personen ergeben würden.

Noch bevor der Vorabkonsultationsprozess abgeschlossen werden konnte, beschloss der Regierungsrat im April 2025 die definitive Einführung von M365 und übernahm die dabei anfallenden Risiken. Der Entscheid gilt für sämtliche Einheiten der Kantonsverwaltung und betrifft sowohl «gewöhnliche» Personendaten als auch besondere Personendaten und somit unter anderem auch Gesundheitsdaten, Daten der Sozialhilfe und Steuerdaten. Aufgrund der erheblichen Tragweite des Entscheides sowie des grossen öffentlichen und medialen Interesses daran, veröffentlichte die DSB eine Medienmitteilung, in der

sie den Entscheid aus datenschutzrechtlicher Sicht würdigte. Mit Blick auf den Umfang der Auslagerung und dem einhergehenden Kontrollverlust warnte sie vor einer Schwächung der digitalen Souveränität und einer Gefährdung für die Grundrechte der Menschen im Kanton Basel-Stadt. Die DSB zeigte sich insbesondere über den Zeitpunkt der Entscheidung überrascht, da sich doch in jüngster Zeit zahlreiche staatliche Akteure in der Schweiz und ganz Europa vom US-Tech-Sektor abwenden, um ihre Souveränität und Unabhängigkeit zu stärken. Gleichzeitig betonte sie, die Implementierung von M365 genau zu überprüfen. Wichtig sei vor allem auch, dass Fachanwendungen in der Kantonsverwaltung weiterhin lokal betrieben würden, wie es der Regierungsrat bei seinem Entscheid zugesichert habe.

Die DSB schloss ihre Vorabkonsultation im Mai 2025 mit einem Bericht ab, in dem sie dem FD eine Reihe von Empfehlungen abgab. Unter anderem empfahl sie die Ausarbeitung eines umfassenden und wirksamen Business Continuity Managements (BCM). Dabei handelt es sich um Massnahmen zur Aufrechterhaltung der Dienstleistungen der kantonalen Verwaltung im Ernstfall, etwa falls Anwendungen von Microsoft (kurzfristig) nicht mehr verfügbar sein sollten. Ferner empfahl die DSB die Einführung einer gesamtkantonalen Datenklassifizierung, um sicherzustellen, dass sensitive Daten nach den entsprechenden Sicherheitsvorgaben behandelt würden. Darüber hinaus machte sie namentlich auf die Risiken beim Versand von sensitiven Daten über E-Mail aufmerksam.

### 2.2 Microsoft Copilot im Schulbereich Ausgangslage

Das Erziehungsdepartement (ED) reichte der DSB ein Vorhaben zur Einführung von Microsoft Copilot an den Volks-, Mittel- und Berufsschulen des Kantons Basel-Stadt ab der 1. Sekundarstufe ein. Copilot ist ein auf künstlicher Intelligenz (KI), konkret auf maschinellem Lernen, aufbauendes Assistenztool, welches in die Microsoft-365-Umgebung integriert ist.

### Beurteilung

Die DSB gab zuhänden des ED eine Reihe von Empfehlungen zur Einführung von Copilot ab. Unter anderem empfahl sie dem ED, eine vollständige Rechtsgrundlagenanalyse zu erstellen. Über die Rechtsgrundlagenanalyse wird ermittelt, ob die vorhandenen Rechtsgrundlagen (Gesetze oder Verordnungen) ausreichen, um das geplante Vorhaben abzustützen und es demokratisch zu legitimieren. Weiter empfahl die DSB, Copilot nicht für Leistungsbeurteilungen von Schüler:innen einzusetzen. Darüber hinaus forderte die DSB das ED dazu auf, von einer Überwachung der Copilot-Nutzenden abzusehen. Die DSB empfahl ausserdem die Deaktivierung der sogenannten Web Search Queries. Es handelt sich dabei um Internet-Abfragen, welche von Copilot aus über die Microsoft-Suchmaschine Bing verlaufen. Für diese gelten separate, weniger vorteilhafte, vertragliche Bedingungen als für die sonstigen Microsoft-Anwendungen. Ferner empfahl die DSB, sicherzustellen, dass die betroffenen Personen (Schüler:innen sowie Lehrpersonen) über die Datenbearbeitung in Copilot angemessen aufgeklärt werden.

Das ED gab der DSB eine Stellungnahme zu den Empfehlungen ab. Darin erläuterte es die Umsetzung gewisser Empfehlungen bzw. stellte die Umsetzung anderer Empfehlungen innerhalb nützlicher Frist in Aussicht. Allerdings blieben die Empfehlungen zum Ausschluss der Nutzung von Copilot im Rahmen von Leistungsbeurteilungen sowie zur Deaktivierung der Web Search Queries strittig. Die DSB konnte, trotz mehrfachen Versuchen, keine einvernehmliche Lösung mit dem ED vor dem geplanten Einführungstermin zum Schulbeginn im August des Berichtsjahres finden.

Von der Einführung von Copilot sind, neben den Lehrpersonen, sämtliche Schüler:innen, Lernende und Studierende im Kanton Basel-Stadt in den Sekundarstufen I und II betroffen. Dabei handelt es sich um eine grosse Anzahl Kinder und Jugendlicher, mithin eine Personengruppe, die Anspruch auf besonderen Schutz geniesst. Angesichts dieses Umstandes beurteilte die DSB das Interesse an der Durchsetzung ihrer Empfehlungen als besonders gewichtig. Insofern erliess sie die beiden strittigen Empfehlungen als verbindliche Weisung gegenüber dem ED. Diese wurde sodann vom ED akzeptiert und umgesetzt.

## 2.3 Digitalisierung Personalrekrutierung Ausgangslage

Human Resources Basel-Stadt (HR BS) stellt gegenwärtig diverse ihrer bislang lokal betriebenen Prozesse auf die Cloud-Lösungen der Anbieterin SAP um. Davon betroffen war im Berichtsjahr unter anderem der Prozess der Personalrekrutierung. Das Projekt war schon längere Zeit hängig, wurde der DSB jedoch erst kurz vor der geplanten Einführung vorgelegt. Ausserdem fiel die Einführung, zeitlich und thematisch, mit der Grundsatzentscheidung des Regierungsrates zur Nutzung von Microsoft 365 (M365) zusammen.

### Beurteilung

Zum Zeitpunkt des Einbezugs der DSB waren bereits zahlreiche Fakten geschaffen worden, welche nur schwer oder mit sehr hohen Kostenfolgen geändert werden konnten: Lieferanten waren bestimmt, Lizenzen waren gekauft und Betriebsverträge waren abgeschlossen. Weil mit der gewählten Lösung Personendaten, potenziell auch besondere Personendaten, in einer Cloud-Lösung (als Software-as-a-Service, SaaS) bearbeitet werden sollten, empfahl die DSB zunächst den Grundsatzentscheid des Regierungsrates zu M365 abzuwarten (siehe dazu oben Ziff. 2.1). Dieser betraf ebenfalls die Bearbeitung von Personendaten in einer Cloud- bzw. SaaS-Lösung und war daher richtungsweisend. Nach dem Regierungsratsentscheid konzentrierte sich die DSB bei ihren Empfehlungen auf das, was innerhalb der geschaffenen Fakten noch realistisch war. Insbesondere standen die transparente Information der betroffenen Personen bezüglich der Datenbearbeitung in der Cloud und ein Verzicht auf die Bearbeitung besonderer Personendaten in der Cloud im Vordergrund.

## 2.4 Digitalisierung Mitarbeitendengespräche Ausgangslage

Nicht lange nach Abschluss der Vorabkonsultation zum neuen Personalrekrutierungsprozess, legte Human Resources Basel-Stadt (HR BS) der DSB bereits das nächste Digitalisierungs- bzw. Cloud-Projekt vor. Bei diesem Vorhaben ging es um den jährlich stattfindenden Prozess der Mitarbeitendengespräche bzw. -beurteilungen (MAG).

### Beurteilung

Die DSB gab in Ihrem Vorabkonsultationsbericht eine Reihe von Empfehlungen zuhänden von HR BS ab. Unter anderem empfahl sie, eine zuvor vom Projektteam präsentierte, besondere Verschlüsselungslösung einzusetzen, um die von der Cloud-Anwendung ausgehenden datenschutzrechtlichen Risiken möglichst zu minimieren. Um die Verhältnismässigkeit zu gewährleisten, empfahl sie weiter, sämtlichen Mitarbeitenden die Möglichkeit zu geben, auf einen MAG-Prozess ausserhalb der Cloud zu wechseln (Opt-out-Recht). Die DSB begrüsst zudem ausdrücklich, die geplante Schaffung spezifischer gesetzlicher Grundlagen für die Durchführung der MAG.

Die Umsetzung sämtlicher Empfehlungen wurde von HR BS bestätigt. Im Nachgang zu weiteren Gesprächen mit der DSB und um die Risiken für die betroffenen Personen weiter zu reduzieren, sicherte HR BS darüber hinaus zu, bestimmte sensitive Datenkategorien von der Bearbeitung in der Cloud-Anwendung auszuschliessen. MAG, in denen sich abzeichnet, dass Themen im Zusammenhang mit Gesundheitsdiagnosen, administrativen oder strafrechtlichen Verfolgungen und Sanktionen (inklusive Disziplinar massnahmen), gewerkschaftlichen Tätigkeiten sowie der Konfession angesprochen werden könnten, müssen demnach im klassischen Prozess ausserhalb der Cloud durchgeführt werden. HR BS erliess hierzu eine entsprechende Weisung gegenüber den Führungspersonen in der Kantonsverwaltung.

## 2.5 Ablösung HR-Software bei den Basler Verkehrs-Betrieben (BVB) Ausgangslage

Im Berichtsjahr stiegen die Basler Verkehrs-Betriebe (BVB) von ihrer bis anhin genutzten HR-Software der Anbieterin SAP auf eine neue Lösung der P&I Personal & Informatik AG (P&I) um. In diesem Rahmen führte die DSB eine Vorabkonsultation durch.

### Beurteilung

Grundsätzlich ist es von Vorteil die DSB bereits vor einer Ausschreibung einzubeziehen, da gewisse ihrer Empfehlungen für das Ausschreibungsverfahren relevant sein können. Im vorliegenden Fall wurde die DSB zwar erst nach der Zuschlagserteilung involviert, jedoch noch vor Abschluss der Vertragsverhandlungen mit der neuen Anbieterin. Die Leistungen von P&I werden aus der EU erbracht. Die BVB beziehen diese über dedizierte Infrastruktur (d. h. die Server werden nur durch die BVB genutzt) aus Rechenzentren und mit Software der P&I. Die Prüfung der DSB konzentrierte sich auf den Auftragsdatenbearbeitungsvertrag (ADV) zwischen den BVB und der P&I, welcher entsprechend den Empfehlungen der DSB überarbeitet werden konnte.

## 2.6 Digitalisierung der schulärztlichen Dossiers Ausgangslage

Der schulärztliche Dienst (SÄD) des Gesundheitsdepartements verwaltet ca. 35'000 – 40'000 schulärztliche Dossiers in Papierform. Der SÄD plante im Berichtsjahr die Dossiers zu digitalisieren. Er hoffte sich mit der Einführung von elektronischen schulärztlichen Dossiers, die Geschäftsbearbeitung zu optimieren, die Datenqualität zu erhöhen und letztendlich einen besseren Service anbieten zu können. Durch die Digitalisierung sollten alle teilnehmenden Schüler:innen ein digitales Dossier erhalten, ähnlich einem Patientendossier in der ärztlichen Versorgung. Die datenschutzrechtlichen Herausforderungen des Projekts lagen insbesondere in der grossen Menge an sensitiven Personendaten, die in den Dossiers enthalten sind und künftig in einer Private Cloud einer externen Anbieterin gehostet werden sollten.

### Beurteilung

Bei der Beurteilung der Dokumente stellte die DSB schnell fest, dass neben dem Umstand der Bearbeitung von besonderen Personendaten bei einem Drittanbieter in einer Schweizer Private Cloud, das Vorhaben bereits weit fortgeschritten war. Da in den eingereichten Unterlagen nicht alle technischen Fragen plausibel beantwortet waren, empfahl die DSB, vor der Auslagerung von besonderen Personendaten und vor der produktiven Einführung des Systems, einen Penetrationstest (Pentest) durchzuführen. Im Weiteren verlangte die DSB eine detaillierte Beschreibung der Risiken und der risikominimierenden Massnahmen, sowie die noch offenen rechtlichen Fragestellungen zu klären. Der weit fortgeschrittene Projektstand und die erhöhte Komplexität führten letztendlich dazu, dass das Projektteam die Planung überarbeitete und die Einführung des Systems etapierte. In der ersten Etappe wurden nur «gewöhnliche» Personendaten, die zur Terminvereinbarung verwendet werden, bearbeitet. Das Auslagern aller Daten sowie die vollumfängliche Einführung des Systems erfolgten später in einem zweiten Schritt. Dieser Fall zeigt auf, dass ein frühzeitiger Einbezug der DSB die gesetzten Ziele eines Vorhabens begünstigen kann.

## 2.7 Eurovision Song Contest (ESC) und Fussball-Europameisterschaft der Frauen

### Ausgangslage

Auch die DSB war in vielfältiger Weise in die Austragung des Eurovision Song Contest (ESC) in Basel involviert. Als «Gastgeber» verantwortete der Kanton Basel-Stadt unter anderem die Organisation der freiwilligen Helfer:innen, der sogenannten Volunteers. Dazu mussten Daten über zahlreiche Personen bearbeitet werden, weshalb die DSB eine Vorabkonsultation durchführte.

Mit der Fussball-Europameisterschaft der Frauen fand im Berichtsjahr ein weiteres internationales Grossereignis in Basel statt. Auch hier kamen zahlreiche freiwillige Helfer:innen aus der ganzen Welt zum Einsatz.

### Beurteilung

Durch den aussergewöhnlichen Charakter des ESC stellte sich zunächst die Frage des anwendbaren Datenschutzrechts: wo agierte der Kanton hoheitlich und wo privatrechtlich, sprich wo unterlagen die Datenbearbeitungen dem kantonalen Informations- und Datenschutzgesetz (IDG) und wo dem Bundesgesetz über den Datenschutz (DSG). Vor allem bezüglich

der Durchführung von Personensicherheitsprüfungen sowie der Ausstellung von Aufenthalts- und Arbeitsbewilligungen ging die DSB von hoheitlichem Staatshandeln aus. Aufgrund des knappen Zeitplans suchte die DSB, zusammen mit den Verantwortlichen des Präsidialdepartements, der Europäischen Rundfunkunion (EBU) sowie externen Dienstleistern und Anwaltskanzleien, nach pragmatischen Lösungen, um den Datenschutz für die Betroffenen zu verbessern. Dies schlug sich vor allem in transparenten Datenschutzerklärungen für die Volunteers und einer klaren Regelung der Verantwortlichkeiten zwischen den Beteiligten nieder.

Im Gegensatz zum ESC betrieb die UEFA ihr Volunteer-Programm selbst und auch nicht im Auftrag des Kantons. Deshalb gelangte die DSB nach einer Prüfung zum Schluss, dass das Volunteer-Programm nicht unter das IDG und somit auch nicht in ihren Zuständigkeitsbereich falle.

Zwei grosse Veranstaltungen mit ähnlich grosser internationaler Visibilität hatten somit, aufgrund unterschiedlicher vertraglicher Verpflichtungen des Kantons, sehr unterschiedliche Auswirkungen auf die Arbeit der DSB. Angesichts der fixen Austragungstermine und der für den ESC durch die Sicherheitskräfte antizipierten Bedrohungslage, wurden beide Themen mit hoher Priorität und einer gesunden Portion Pragmatismus behandelt

## 2.8 Videoüberwachung beim Eurovision Song Contest (ESC)

### Ausgangslage

Anlässlich der Austragung des Eurovision Song Contests (ESC) in Basel legte die Kantonspolizei der DSB ein Vorhaben zur Videoüberwachung verschiedener Teile der Innenstadt (Barfüsserplatz und Steinenvorstadt) sowie Teile der Kleinbasler Rheinuferpromenade vor.

### Beurteilung

Insbesondere aufgrund der breiten räumlichen Ausdehnung der geplanten Videoüberwachung und der damit grossen Anzahl potenziell davon betroffener Personen, stufte die DSB das ursprünglich angedachte Vorhaben als unverhältnismässig ein. Die Kantonspolizei passte daher aufgrund der Empfehlungen der DSB die Videoüberwachung an. Die von der DSB ausgesprochenen Empfehlungen umfassten im Wesentlichen eine reduzierte Speicherdauer sowie eine separate Information der betroffenen Anwohnerschaft.

Bei ihrer Beurteilung berücksichtigte die DSB die von der Kantonspolizei dargelegte, besonders akute Bedrohungslage für die öffentliche Sicherheit. Sie betonte gleichzeitig, dass diese Form der Videoüberwachung eine absolute Ausnahme bleiben müsse.

## 2.9 Revision der Bau- und Planungsverordnung

### Ausgangslage

Gestützt auf den Legislaturplan 2021 bis 2025 hatte das Bau- und Verkehrsdepartement (BVD) den Auftrag, das Baugesuchsverfahren zu digitalisieren. Deshalb sollten die bestehenden Bestimmungen in der Bau- und Planungsverordnung (BPV) angepasst werden. In diesem Zusammenhang hatte das BVD die DSB bereits vor mehreren Jahren kontaktiert und legte ihr im Berichtsjahr schliesslich die BPV zur Vorabkonsultation vor.

### Beurteilung

Die DSB stellte fest, dass bei der digitalen Planaufgabe dieselben Unterlagen und darin enthaltenen Personendaten veröffentlicht würden wie bei der herkömmlichen Auflage und Einsicht vor Ort. Allerdings bestanden aus datenschutzrechtlicher Sicht wesentliche Unterschiede zwischen den beiden Veröffentlichungsformen. Im Internet veröffentlichte Daten sind jederzeit und durch jedermann weltweit abrufbar und können beliebig kopiert werden. Dadurch ist eine bedeutend schnellere und grössere Verbreitung der Daten möglich.

Wenn die Daten einmal im Internet veröffentlicht sind, hat die publizierende Behörde zudem keine Möglichkeit mehr, die Verwendung und Verbreitung der Daten wirksam zu steuern. Die Daten lassen sich kaum vollständig aus dem Internet entfernen (d. h. löschen). Diese Sachlage führt dazu, dass sich bei einer Publikation im Internet auch für gewöhnliche Personendaten erhöhte Datenschutzanforderungen ergeben. Im öffentlich-rechtlichen Bereich bedeutet dies, dass an die inhaltliche Ausgestaltung der gesetzlichen Grundlagen erhöhte Anforderungen zu stellen sind und der Grundsatz der Verhältnismässigkeit verstärkt zu beachten ist (Einsicht in so viele Daten wie nötig, aber so wenig wie möglich). Die DSB empfahl gestützt auf diese Sachlage entsprechende Anpassungen an den gesetzlichen Grundlagen. Diese wurden vom BVD umgesetzt.

## 3 Kontrollen

**Die DSB führt bei den öffentlichen Organen im Kanton Basel-Stadt Kontrollen durch, um die Einhaltung der datenschutzrechtlichen Bestimmungen zu überprüfen. Dabei wählt sie die zu kontrollierenden öffentlichen Organe und Datenbearbeitungen nach risikobasierten Kriterien aus. Darüber hinaus hat die DSB diverse spezialgesetzliche Kontrollaufträge. Im Speziellen kontrolliert sie Datenbearbeitungen durch öffentliche Organe im Kanton Basel-Stadt in Anwendung des Schengen-Assoziierungsabkommens. Zudem kontrolliert die DSB das kantonale Bedrohungsmanagement jährlich.**

### 3.1 Klinikinformationssystem im Universitäts-Kinderspital beider Basel (UKBB)

Im Berichtsjahr führte die DSB eine datenschutzrechtliche Kontrolle im Universitäts-Kinderspital beider Basel (UKBB) durch. Dabei prüfte die DSB schwerpunktmässig die organisatorischen und technischen Massnahmen zur datenschutzkonformen Nutzung des Klinikinformationssystems (KIS) und die internen Regelungen und Schulungen des UKBB zum Umgang mit Personendaten, insbesondere mit besonderen Personendaten.

Das KIS wird im Rechenzentrum des UKBB von der externen Firma CISTEC eigenständig unterhalten, betrieben und hinsichtlich der Einhaltung der Datenschutzerfordernisse überwacht. Das KIS verfügt dabei über mehr als 100 Schnittstellen zu internen und externen IT-Systemen.

Im Rahmen der Kontrolle des KIS zeigte sich, dass Aufgaben und Verantwortlichkeiten teilweise unklar oder nicht ausreichend geregelt waren. Insbesondere stellte sich heraus, dass die datenschutzrechtlichen Pflichten zwischen dem UKBB und der Anbieterin nicht ausreichend vertraglich geregelt waren.

Bei der Prüfung der internen Regelungen und Schulungen wurde deutlich, dass das UKBB zwar über entsprechende Instrumente verfügt, dass aber ein bereichsübergreifendes Datenschutzmanagementsystem (DSMS) fehlt und ein umfassendes Konzept zur regelmässigen Schulung aller Mitarbeitenden zum Zeitpunkt der Kontrolle noch nicht abschliessend umgesetzt war. Das UKBB hat bestätigt, auf Empfehlung der DSB sowohl ein DSMS wie auch ein Informationssicherheitsmanagementsystem (ISMS) zu etablieren und sein Schulungskonzept weiter auszubauen, so dass dieses aktuelle Entwicklungen der datenschutzrechtlichen Risiken und rechtlichen Anforderungen berücksichtigt.

### 3.2 Nachkontrolle zum Cyberangriff im Erziehungsdepartement

Im Jahr 2023 wurde das Erziehungsdepartement (ED) Opfer eines Cyberangriffs. Dabei haben sich kriminelle Zugriff auf (teilweise sensitive) Daten über Schüler:innen, Lernende, Lehrpersonen und weitere Mitarbeitende beschafft. Anschliessend veröffentlichten sie diese Daten im Darknet. Im Nachgang zum Angriff gab die DSB dem ED eine Reihe von Empfehlungen ab, um die Datenschutz-Risiken von Cyberangriffen für die Zukunft zu minimieren. Diese umfassten insbesondere Verbesserungen in der Überwachung der IT-Systeme, die Qualität der Log- und Backup-Files sowie den Abschluss einer wirksamen Auftragsdatenbearbeitungsvereinbarung mit der externen IT-Dienstleisterin.

Im Berichtsjahr kontrollierte die DSB den Stand der Umsetzung ihrer abgegebenen Empfehlungen. Erfreulicherweise konnte die DSB bei ihrer Nachkontrolle feststellen, dass alle ihre Empfehlungen vom ED umgesetzt worden waren.

### 3.3 Nachkontrolle im Care Management von HR BS

Das Care Management ist eine Abteilung von Human Resources Basel-Stadt (HR BS). Das Care Management unterstützt Mitarbeitende der kantonalen Verwaltung und ihre Vorgesetzten in schwierigen Situationen, etwa bei der Rückkehr zur Arbeit nach längerer Krankheit oder bei persönlichen Problemen, die sich auf das Arbeitsumfeld und die Arbeitsleistung auswirken. Im Rahmen dieses Angebots erhalten die Beratungspersonen des Care Managements Kenntnis von vielen sensitiven Informationen. Aus diesem Grund führte die DSB 2021 beim Care Management eine Datenschutz-Kontrolle durch und gab eine Reihe von Empfehlungen ab.

Im Berichtsjahr führte die DSB eine Nachkontrolle beim Care Management durch, um die Umsetzung ihrer Empfehlungen zu verifizieren. Die Nachkontrolle ergab, dass ein Teil der Empfehlungen umgesetzt war. Insbesondere war ein Aufbewahrungs- und Löschkonzept für die bearbeiteten Personendaten entwickelt worden. Zudem waren gezielte Massnahmen zur Sensibilisierung der Mitarbeitenden für den Datenschutz ergriffen worden. Andere Empfehlungen waren demgegenüber noch nicht umgesetzt. Darunter insbesondere die Präzisierung der gesetzlichen Grundlage für die Bearbeitung von besonderen Personendaten durch das Care Management sowie die Finalisierung der erforderlichen Risikodokumentation (u.a. ISDS-Konzept). Die DSB setzte dem Care Management eine letzte Nachfrist für die Umsetzung der noch offenen Empfehlungen.

### 3.4 Baustellenfortschrittcameras

Der Kanton Basel-Stadt betreibt verschiedene eigene Baustellen. Um den Fortschritt auf diesen Baustellen für die Öffentlichkeit nachverfolgbar zu machen, werden dort sogenannte Baufortschrittkameras eingesetzt. Diese nehmen an Werktagen von 6 bis 18 Uhr jeweils stündlich ein Bild auf. An Wochenenden und während der Nacht finden keine Aufnahmen statt. Die Kameras werden von einer externen Firma betrieben und die Aufnahmen im Internet für jedermann zugänglich gemacht.

Die von der DSB durchgeführte Kontrolle diente der Überprüfung, inwiefern die Kameraeinstellungen (Winkel, Distanz zur Baustelle usw.) derart gewählt wurden, dass aufgenommene Personen und Fahrzeuge nicht identifizierbar waren. Insbesondere prüfte die DSB, ob die an die Baustelle angrenzenden Wohnhäuser mittels Weichzeichnungsfilter so unkenntlich gemacht wurden, dass darin keine Personen erkennbar waren. Die Kontrolle ergab, dass die Kameraeinstellungen weitestgehend datenschutzkonform gewählt worden waren. Das BVD bestätigte im Übrigen die Umsetzung der wenigen Empfehlungen der DSB.

### 3.5 Mobile Überwachungsroboter an der Herbstmesse

Im Rahmen der Basler Herbstmesse wurde die DSB zum ersten Mal auf den Einsatz mobiler Überwachungsroboter im Kanton aufmerksam. Die Roboter patrouillierten unter anderem auf dem Petersplatz vor dem Hauptgebäude der Universität. Die DSB nahm dies zum Anlass, um das Vorgehen bei der zuständigen Dienststelle «Messen und Märkte» des Präsidialdepartements kurzfristig zu kontrollieren.

Die DSB stellte fest, dass viele Fragen im Zusammenhang mit den durch die Roboter aufgezeichneten Daten unklar waren. Gleichzeitig handelte es sich um eine neue, weitreichende Überwachungstechnologie, von der eine grosse Anzahl Menschen betroffen war. Die verantwortliche Dienststelle anerkannte, die Datenschutz-Risiken unterschätzt zu haben, zeigte sich jedoch von Anfang an bestrebt, eine konstruktive und rasche Lösung mit der DSB zu suchen. Es stellte sich heraus, dass die Überwachung der Messestände auch durch menschliches Sicherheitspersonal sichergestellt werden konnte. Daraufhin wurden die Roboter umgehend entfernt.

Durch die schnelle Intervention der DSB und die proaktive Kooperation der zuständigen Dienststelle konnten die Risiken für die Grundrechte prompt verringert und eine zweckmässige Alternative gefunden werden. Der Vorfall zeigt aber auch, dass die Sensibilisierung für den Datenschutz in den einzelnen öffentlichen Organen weiterhin verbessert werden kann.

### 3.6 Kantonales Bedrohungsmanagement

Per 1. März 2023 wurde im Kanton Basel-Stadt das Kantonale Bedrohungsmanagement (KBM) eingeführt. Dieses dient dazu, schwere Bedrohungen, die gegen Leib und Leben gerichtet sind, frühzeitig zu erkennen, einzuschätzen und rechtzeitig zu entschärfen. Zu diesem Zweck geniesst das KBM äusserst weitreichende Datenbearbeitungsbefugnisse. Gemäss dem revidierten Polizeigesetz kontrolliert die DSB das KBM und legt dem Grosse Rat dazu jährlich einen datenschutzrechtlichen Kontrollbericht vor. In Erfüllung dieses gesetzlichen Auftrages, führte die DSB auch im Berichtsjahr eine Kontrolle beim KBM durch.

Die Kontrolle im Berichtsjahr fokussierte schwergewichtig auf technische und organisatorische Bereiche, insbesondere auf das Zugriffsberechtigungskonzept und die Logfile-Prüfung des Fallführungssystems. Der Abschlussbericht der Kontrolle konnte nicht mehr im Berichtsjahr, sondern erst anfangs 2026 fertiggestellt werden.

## 4 Meldungen von Datenschutzverletzungen

**Seit Beginn des Berichtsjahres gilt eine neue Meldepflicht bei Datenschutzverletzungen. Öffentliche Organe müssen Datenschutzverletzungen ab einer gewissen Risikoschwelle der DSB melden und falls die Umstände es erfordern, die betroffenen Personen benachrichtigen. Die DSB nimmt die Meldungen entgegen und unterstützt die öffentlichen Organe im Bedarfsfall.**

### 4.1 Hintergrund und Zweck

Im Zuge der digitalen Transformation sind auch die Risiken im Zusammenhang mit Verletzungen der Datensicherheit, wie z. B. bei Cyber-Angriffen, gestiegen. Im Falle einer Datenschutzverletzung droht den betroffenen Personen ein erheblicher Schaden. Dieser kann beispielsweise in Form von Diskriminierungen, Identitätsdiebstahl, finanziellen Verlusten, Rufschädigung usw. auftreten. Die Meldepflicht soll die Transparenz über die Vorfälle fördern und sicherstellen, dass bei einer Datenschutzverletzung rechtzeitig und angemessen reagiert wird.

### 4.2 Hilfestellungen der DSB

Zur Unterstützung der öffentlichen Organe hat die DSB ein Meldeformular mit Erläuterungen ausgearbeitet und auf ihrer Webseite zur Verfügung gestellt. Im Laufe des Berichtsjahres hat sie diese Unterlagen aktualisiert und insbesondere um praktische Beispiele ergänzt. Aus den Erläuterungen geht neu hervor, ab welcher Risikoschwelle eine Datenschutzverletzung der DSB zu melden ist und in welchen Fällen die betroffenen Personen zu informieren sind.

### 4.3 Erfolgte Meldungen und Beschreibung ausgewählter Fälle

Es sind im Berichtsjahr 36 Meldungen eingegangen. Die Art der gemeldeten Verletzungen war breit gefächert. Ein beträchtlicher Anteil der Meldungen erfolgte aus dem Gesundheitsbereich. Diese Auffälligkeit könnte darauf zurückzuführen sein, dass in diesem Bereich eine hohe Sensibilisierung für Datenanliegen besteht.

Mehrfach gemeldet wurde die Versendung von E-Mails und Briefen an die falschen Empfangspersonen. Je nach Kontext und Inhalt der Sendungen kann dies ein hohes Risiko für die betroffenen Personen bergen. Hauptgründe für solche Sendungen an die falschen Personen sind Unachtsamkeiten (z. B. Tippfehler) und nicht mehr aktuelle, fehlerhafte oder fehlende Daten. Zur Vermeidung solcher Fehler müssen vor allem geeignete organisatorische Massnahmen umgesetzt werden. Diese können z. B. einen Prozess zur regelmässigen Überprüfung der Aktualität der Daten sowie die angemessene Schulung der Mitarbeitenden umfassen.

In einem Fall bezog eine Dienststelle der Kantonsverwaltung für die Bearbeitung von Personendaten, inklusive besonderen Personendaten, einen Service einer externen IT-Dienstleisterin. Versehentlich löschte die Dienstleisterin eine grosse Anzahl der bearbeiteten Daten. Weil kein brauchbares Backup aktiviert gewesen war, konnte ein Teil der gelöschten Daten nicht wiederhergestellt werden. Dieses Beispiel zeigt auf, dass der Beizug von externen Dienstleisterinnen (Auftragsdatenbearbeiterinnen) nicht ohne Weiteres zu Verbesserungen im Datenschutz führt. Um Datenschutzverletzungen vorzubeugen, müssen öffentliche Organe ihre Auftragsdatenbearbeiterinnen sorgfältig auswählen, mit ihnen wirksame Vertragsbedingungen abschliessen und sie regelmässig kontrollieren.

Der DSB wurden auch Vorfälle gemeldet, in denen Schwachstellen in Software zu kriminellen Zwecken ausgenutzt wurden bzw. hätten ausgenutzt werden können. Dabei sind jene Dienste besonders exponiert, die aus dem Internet allgemein erreichbar sind. Um solche Schwachstellen möglichst rasch zu erkennen und zu beheben, rät die DSB, regelmässige Schwachstellenanalysen durchzuführen und Sicherheits-Updates zeitnah zu übernehmen.

## 5 Schulungen und Sensibilisierung

**Die Umsetzung der Vorgaben zum Datenschutz und zum Öffentlichkeitsprinzip durch die öffentlichen Organe setzt die angemessene Schulung der Mitarbeitenden voraus. Dafür sind in erster Linie die jeweiligen öffentlichen Organe verantwortlich. Soweit es die Ressourcen zulassen, unterstützt die DSB die öffentlichen Organe bei diesem Unterfangen, indem sie eigene Schulungen und Weiterbildungen anbietet. Der DSB ist es ebenso ein Anliegen, soweit möglich auch Studierende, Lernende sowie Schüler:innen für die Anliegen des Datenschutzes und der Transparenz zu sensibilisieren. Im Weiteren bringt sich die DSB punktuell in nationalen Fachgremien und an Tagungen ein.**

### 5.1 Neue Merkblätter

Um die öffentlichen Organe bei der Einhaltung der Datenschutzbestimmungen zu unterstützen und betroffene Personen über ihre Rechte zu sensibilisieren, erarbeitete die DSB im Berichtsjahr diverse neue Merkblätter, welche sie auf ihrer Homepage veröffentlichte und darüber hinaus den Datenschutzberater:innen direkt zukommen liess. Unter anderem aktualisierte die DSB ihren Leitfaden zur Auftragsdatenbearbeitung. Weil es immer häufiger vorkommt, dass öffentliche Organe externe Dritte als Auftragsdatenbearbeiter beiziehen (z. B. für den Betrieb von IT-Dienstleistungen), ist die Sicherstellung des Datenschutzes in diesen Konstellationen von besonderer Wichtigkeit. Zudem hat die DSB ein Merkblatt zur Informationspflicht bei der Beschaffung von Personendaten veröffentlicht. Dieses soll es den öffentlichen Organen erleichtern, den neuen Transparenzvorgaben nachzukommen. Wo auch immer möglich, hat die DSB ihre Merkblätter mit praktischen Beispielen versehen, um die Verständlichkeit zu verbessern.

### 5.2 Fallkonferenzen

Die DSB führte gemeinsam mit dem kantonalen Informationssicherheitsbeauftragten (ISB) fünf Fallkonferenzen zum Thema Datenschutz und integrale Informationssicherheit durch. Zielgruppe der Fallkonferenzen waren die Datenschutzberater:innen (DSBer), die Informationssicherheitsbeauftragten (ISBD/CISO) und die Ansprechpersonen zum Öffentlichkeitsprinzip der öffentlichen Organe. Das neu geschaffene Format der Fallkonferenzen zielte neben der praxisnahen Wissensvermittlung durch die DSB und den ISB auch auf die Vernetzung und das aktive Einbringen eigener Erfahrungen und Fragen durch die Teilnehmenden.

Die im Berichtsjahr durchgeführten Fallkonferenzen befassten sich mit den Aufgaben der DSBer und ISBD/CISO bei geplanten Vorhaben, dem Umgang mit Cybersicherheitsvorfällen, den datenschutzrechtlichen und IT-Sicherheits-Anforderungen beim Gang in die Cloud, den Umgang mit Einsichtsgesuchen betroffener Personen, sowie dem Darknet und der Verschlüsselung.

### 5.3 Bedürfnis-Umfrage bei den Datenschutzberater:innen

Um ihr Angebot an Hilfestellungen und Schulungen möglichst eng an den tatsächlichen Bedürfnissen der öffentlichen Organe auszurichten, hat die DSB im Berichtsjahr eine Umfrage bei den Datenschutzberater:innen (DSBer) durchgeführt. Die DSB hat sodann ihre Arbeiten aufgrund der erhaltenen Rückmeldungen priorisiert. Ausgearbeitet wurde eine Reihe von neuen Merkblättern, welche anfangs 2026 veröffentlicht wurden. Diverse weitere vorgebrachte Punkte wird die DSB in ihr Schulungsangebot aufnehmen. Auf die spezifische Frage der DSB, ob eine vertiefte fachliche Weiterbildung zum kantonalen Informations- und Datenschutzgesetz (IDG) erwünscht sei, antworteten viele der DSBer positiv. Die DSB hat sich dementsprechend zum Ziel gesetzt, eine solche Weiterbildung im Jahr 2026 zusammen mit einer externen Fachperson aufzugleisen.

#### 5.4 Mitarbeitendenveranstaltung beim Amt für Wirtschaft und Arbeit

Auf Einladung des Amtes für Wirtschaft und Arbeit (AWA), hielt die DSB im Rahmen einer wiederkehrend stattfindenden Mitarbeitendenveranstaltung («AWA-Info») ein Referat zu den wichtigsten praktischen Neuerungen im revidierten Informations- und Datenschutzgesetz (IDG). Sie betonte dabei insbesondere die zunehmenden Risiken im digitalen Raum, die strengeren Vorgaben bei neuen Projekten sowie die neue Meldepflicht bei Datenschutzverletzungen.

#### 5.5 Partizipative Arbeitstagung des Bundesamts für Justiz zur Umsetzung der KI-Konvention des Europarats

Im Hinblick auf die vom Bundesrat beschlossene Umsetzung der KI-Konvention des Europarats veranstaltete das Bundesamt für Justiz (BJ) einen partizipativen Workshop mit einer Auswahl an Expert:innen aus Zivilgesellschaft, Politik, Wirtschaft, Wissenschaft und Verwaltung. Daran nahm auch die DSB teil. Ziel des Workshops war es, frühzeitig, unter Einbezug verschiedener Stakeholder, Regulierungsmöglichkeiten im Bereich von KI zu diskutieren und zu erarbeiten. Die DSB sprach sich in diesem Rahmen für Lösungen aus, welche die betroffenen Personen vor Grundrechtseingriffen durch KI-Systeme bestmöglich schützen. Sie fokussierte sich dabei auf die Herstellung von Transparenz beim Einsatz von KI-Systemen und auf die Regelung von Fällen, in denen KI-Systeme für automatisierte Einzelentscheidungen genutzt werden.

## 6 Zusammenarbeit mit anderen Datenschutzbehörden

**Die DSB arbeitet zur Erfüllung ihrer Aufgaben mit den Datenschutzbehörden anderer Kantone, des Bundes und des Auslands zusammen. Diese Zusammenarbeit ist für ein koordiniertes Vorgehen der Datenschutzbehörden und eine möglichst einheitliche Praxis förderlich. Auch angesichts der zahlreichen kantonsübergreifenden Themen ist die Vernetzung wertvoll.**

### 6.1 Privativim

Das wichtigste Zusammenarbeitsforum für die DSB ist privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, bei der die Datenschutzbehörden sämtlicher Kantone, des Bundes und bestimmter Städte vertreten sind. Die Beauftragte ist Mitglied des Vorstandes von privatim. In dieser Funktion nahm sie an fünf Vorstandssitzungen teil. Der Vorstand von privatim führt insbesondere die laufenden Geschäfte, übernimmt die Öffentlichkeitsarbeit, vertritt privatim nach aussen und nimmt an den Vernehmlassungen des Bundesrechts teil. Privatim veranstaltet pro Jahr jeweils zwei Mitgliederversammlungen, an denen aktuelle datenschutzrechtliche Themen und Herausforderungen behandelt werden. Im Fokus des Frühjahrsplenums standen unter anderem die Bearbeitung von Gesundheitsdaten in der Cloud sowie der Einsatz der Cloud-Lösung Microsoft 365 in der öffentlichen Verwaltung. Das Herbstplenium widmete sich sodann vor allem der Öffentlichkeitsarbeit des Verbandes, der Verabschiedung einer Resolution zur Auslagerung von Daten in Cloud-Lösungen sowie der Festlegung von Schwerpunktthemen für das Folgejahr.

Die DSB wirkt zudem in vier Arbeitsgruppen von privatim mit. Es sind dies die AG Sicherheit, die AG Digitale Verwaltung, die AG Gesundheit und die AG ICT. Die Arbeitsgruppen dienen dem Erfahrungsaustausch unter den Mitgliedern und der Koordination ihrer Praxis, was von der DSB als sehr wertvoll empfunden wird. Hervorzuheben in diesem Kontext ist die durch die DSB und andere Mitglieder der AG Sicherheit erfolgte Beratung der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) im Rahmen der Ausarbeitung eines Konkordats für den polizeilichen Datenaustausch. Die privatim-Mitglieder setzten sich dabei für eine möglichst datenschutzkonforme Umsetzung ein.

Im Berichtsjahr gründeten die Datenschutzbeauftragten der vier Nordwestschweizer Kantone Basel-Stadt, Basel-Landschaft, Aargau und Solothurn schliesslich ein neues regelmässiges Austauschforum. Ziel davon ist es, vor allem regionale Datenschutzthemen der Nordwestschweiz zu besprechen und vom gegenseitigen Know-how zu profitieren.

### 6.2 Schengen-Koordinationsgruppe

Die Schweiz ist Mitglied des Schengen-Assoziierungsabkommens. Dieses ist die Grundlage für eine Reihe von Informationssystemen, insbesondere das Schengener Informationssystem (SIS) und das Visa Informationssystem (VIS). Gesetzlich ist vorgesehen, dass die kantonalen Datenschutzbehörden und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) bei der Aufsicht über die Datenbearbeitungen im Rahmen dieser Informationssysteme zusammenarbeiten. Der EDÖB koordiniert die Aufsichtstätigkeit mit den kantonalen Datenschutzbehörden primär über eine entsprechende Koordinationsgruppe, in der die jeweiligen kantonalen Datenschutzbehörden und der EDÖB vertreten sind. Die Koordinationsgruppe hat im Berichtsjahr zwei Sitzungen abgehalten. Dabei wurde unter anderem die im Berichtsjahr erfolgte Schengen-Evaluation der Schweiz durch die EU-Kommission thematisiert. Der Evaluationsbericht enthielt mehrere auf die Datenschutzaufsichtsbehörden ausgerichtete Empfehlungen. Diese bestärkten insbesondere die Wichtigkeit, die Datenschutzaufsichtsbehörden mit genügenden Ressourcen auszustatten und ihnen die Kompetenz zu verleihen, verbindliche Anordnungen zu erlassen. Die DSB ist bereits seit längerem gesetzlich ermächtigt, verbindliche Weisungen in Form von Verfügungen zu erlassen. Mit den zugewiesenen Ressourcen gelingt es der DSB jedoch nur knapp, ihren gesetzlichen Auftrag zu erfüllen.

## 7 Personalbestand und Rechnung

**Die DSB stösst aufgrund der hohen Geschäftslast mit ihren vorhandenen Ressourcen zunehmend an Grenzen.**

Per Ende des Berichtsjahres umfasste der Personalbestand der DSB insgesamt 840 %: die Beauftragte zu 100 %, fünf Mitglieder im juristischen Team zu insgesamt 380 %, drei Mitglieder im IT-Team zu insgesamt 280 % sowie eine Assistenz zu 80 %. Weil keine geeigneten Bewerbungen auf die Volontariatsstelle für die zweite Hälfte des Berichtsjahres eingegangen waren, entschied sich die DSB, den bereits angestellten Volontär als fünften juristischen Mitarbeiter befristet weiter zu beschäftigen, um Engpässe bei der Aufgabenerfüllung zu vermeiden und dringende Pendenzen abzubauen.

Die Rechnung für das Berichtsjahr fiel mit CHF 1'874'600 ausgeglichen aus.

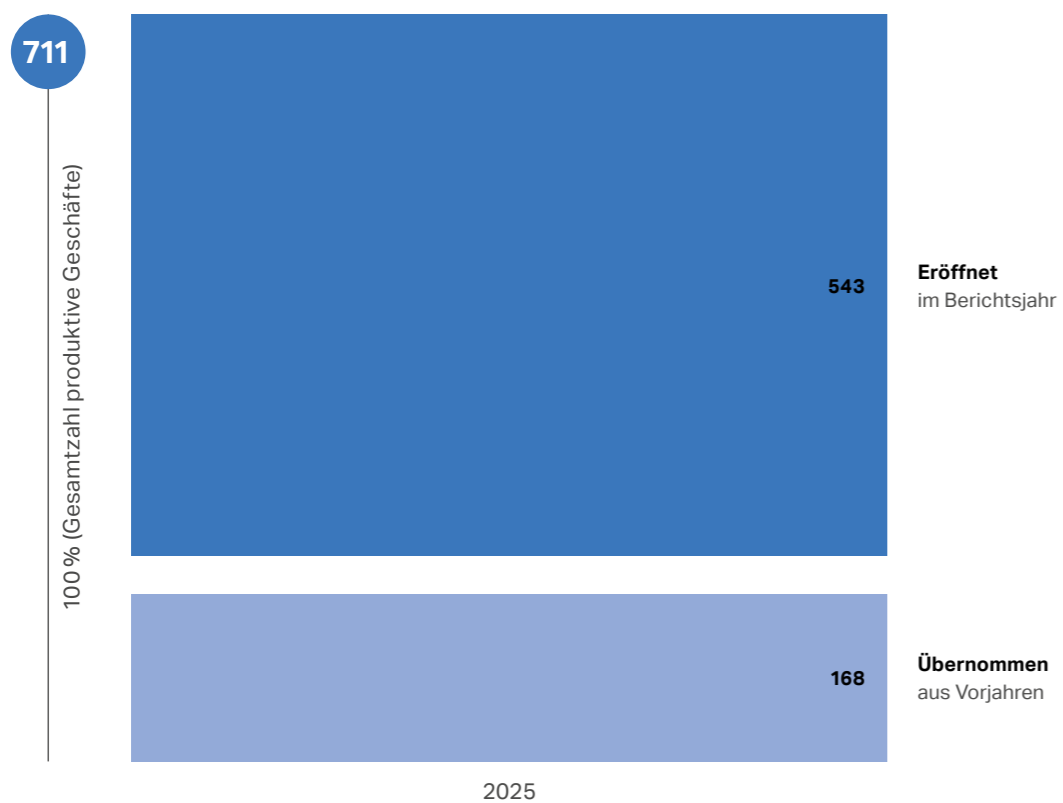
## 8 Zahlen zum Berichtsjahr

**Im Berichtsjahr bearbeitete die DSB insgesamt 711 verschiedene produktive Geschäfte (d. h. exklusive der administrativen Geschäfte).**

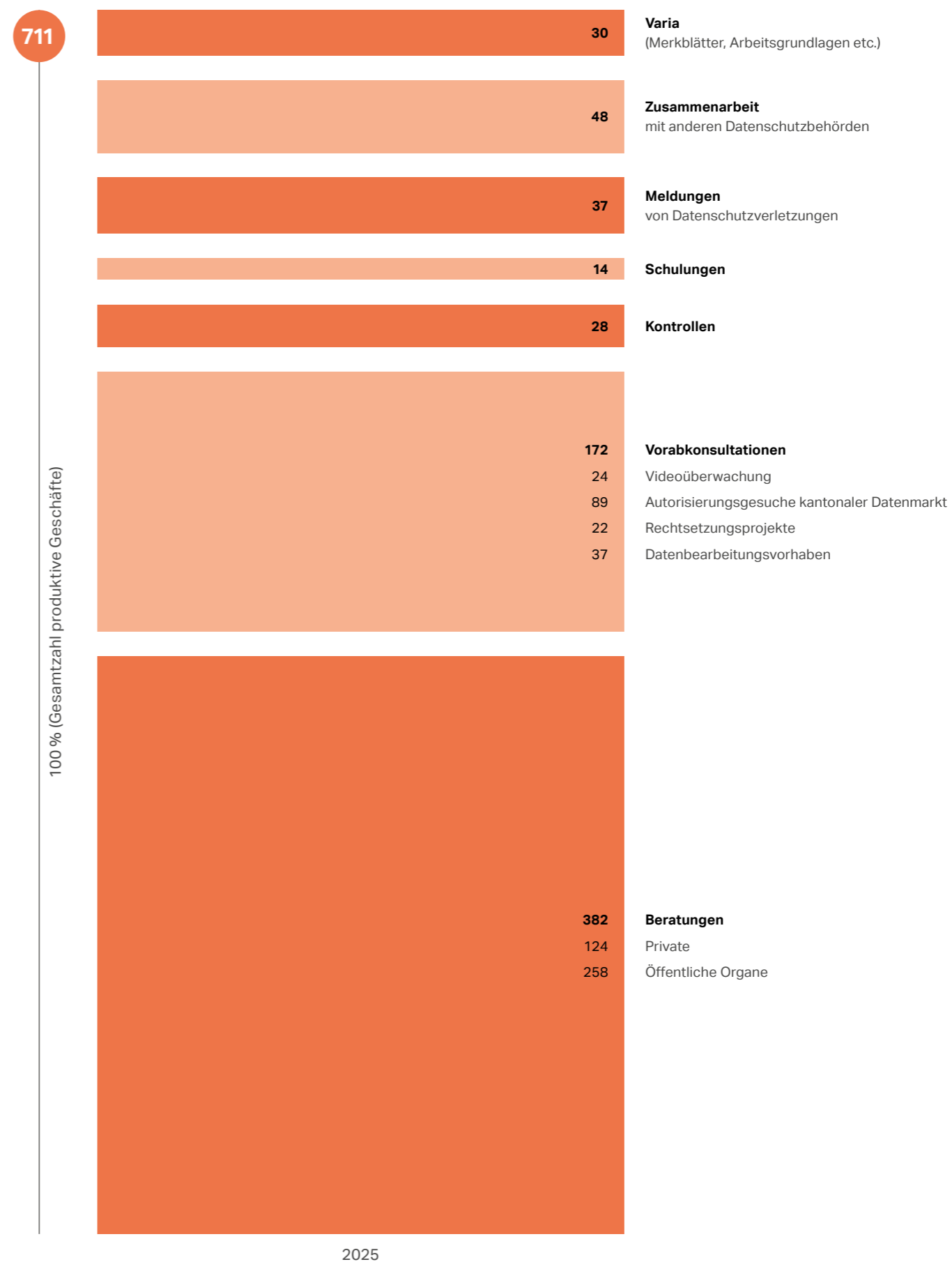
Davon wurden 168 aus den Vorjahren übernommen und 543 neu eröffnet. Die Aufteilung der bearbeiteten Geschäfte auf die verschiedenen Aufgaben der DSB kann den nachfolgenden Grafiken entnommen werden.

Zu beachten ist, dass die Kennzahlen der DSB mit dem Budget 2025 auf Wunsch der kantonalen Verwaltung neu definiert worden sind. Im Zuge der Revision des Informations- und Datenschutzgesetzes (IDG) hat die DSB sodann auch einen neuen Registrarplan definiert. Aus diesen Gründen sind die Kennzahlen ab dem vorliegenden Berichtsjahr nur sehr bedingt mit den Vorjahren vergleichbar. Dafür liefern sie ein akkurateres Abbild der Geschäftstätigkeit der DSB.

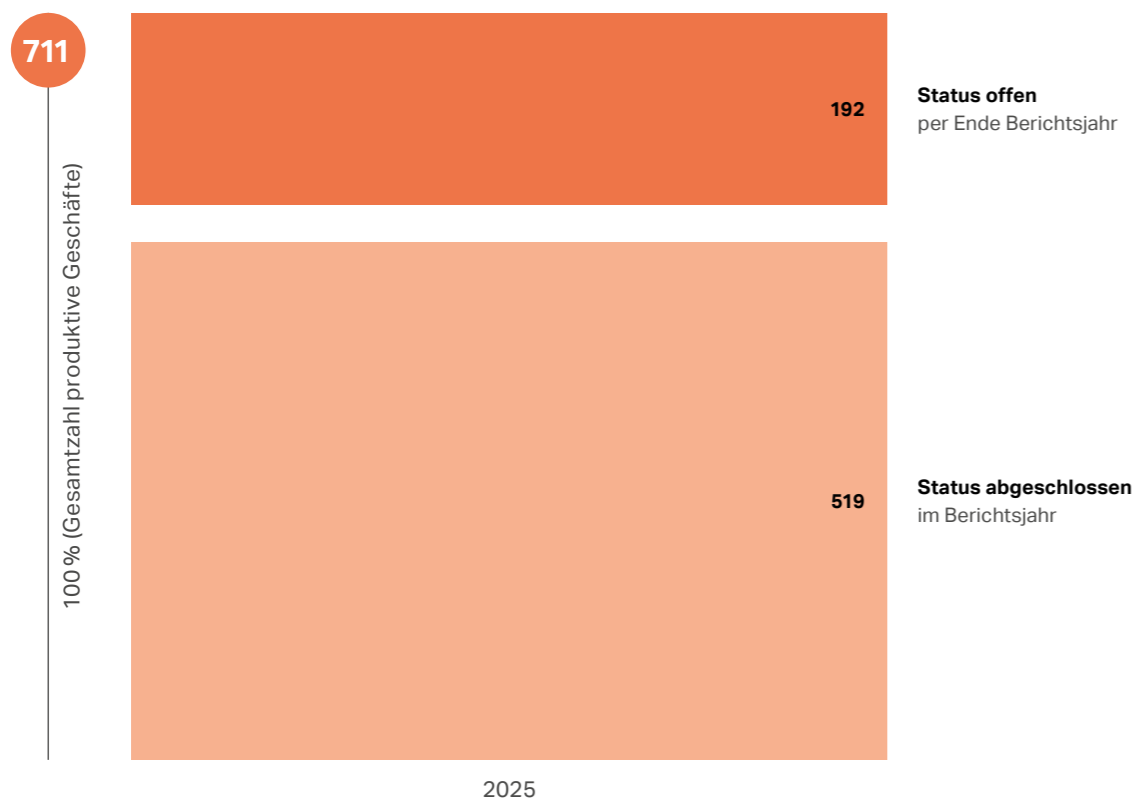
## Geschäfte nach Eröffnungszeitpunkt



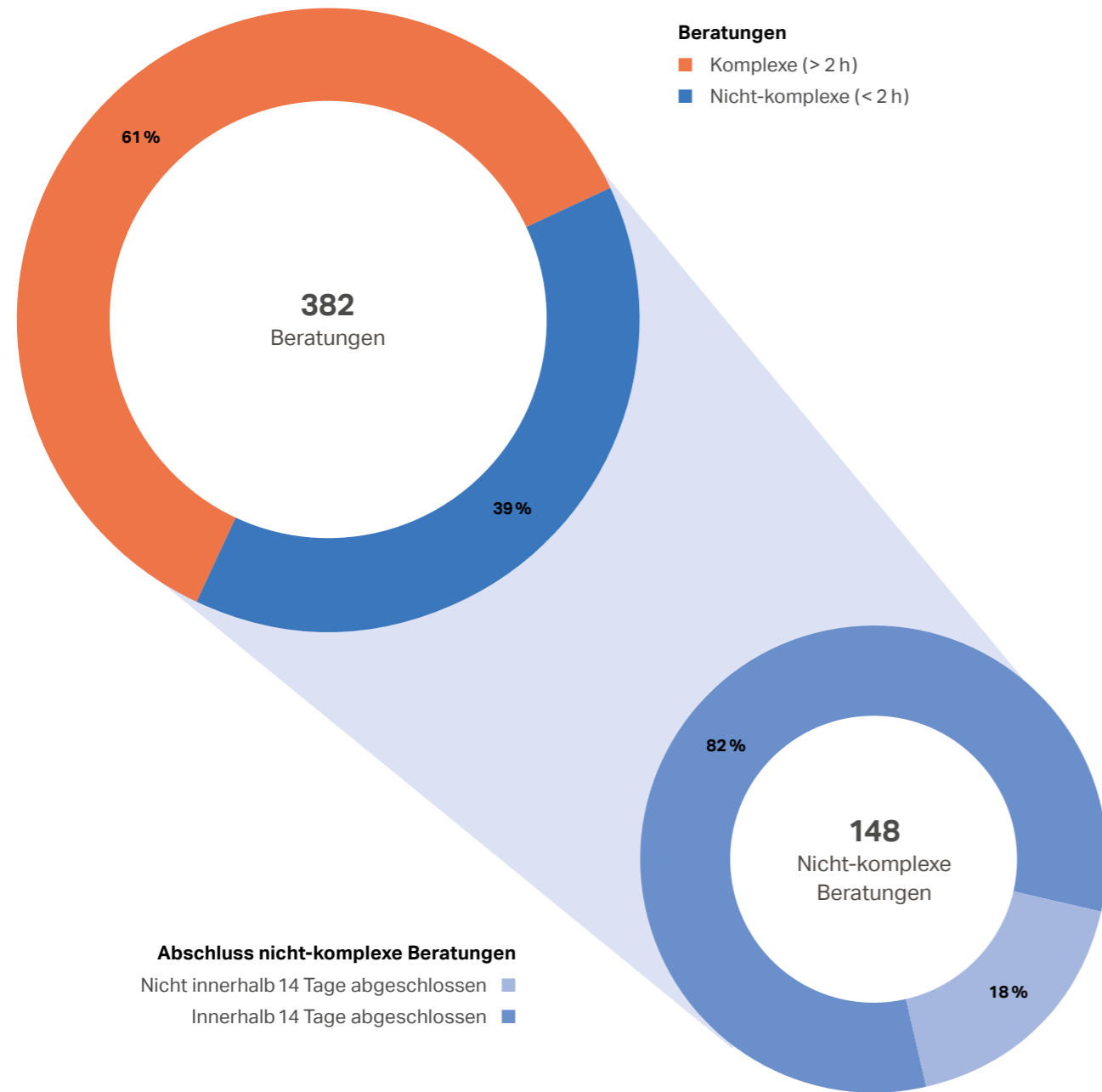
## Geschäfte nach Geschäftsart



## Geschäfte nach Status



# Beratungen





# Dank

Die Beauftragte dankt ihrem gesamten Team herzlich für die engagierte Mitarbeit während des Berichtsjahres. Darüber hinaus gebührt aber auch allen Führungspersonen und Mitarbeitenden der öffentlichen Organe ein grosser Dank für die konstruktive Zusammenarbeit und dafür, dass sie sich alltäglich sowohl für die Gewährleistung des Datenschutzes als auch für die Förderung der Transparenz in ihren Organisationseinheiten einsetzen.

