Stadt Bern
Fach- und Aufsichtsstelle
Datenschutz FADS

Fach- und Aufsichtsstelle
Datenschutz

Tätigkeitsbericht 2025

Fach- und Aufsichtsstelle Datenschutz der Stadt Bern FADS

Leiterin FADS: Sophie Haag, Rechtsanwältin und Datenschutzbeauftragte

Mitarbeitende: Markus Hochuli, MA Governance, Techniker HF Elektrotechnik, wissenschaftlicher Mitarbeiter Informatik

Patrick Rohrbach, Fürsprecher, wissenschaftlicher Mitarbeiter Recht

Daniela Mäder, administrative Mitarbeiterin

Adresse: Effingerstrasse 4, 3011 Bern

Telefon: +41 31 312 09 12

E-Mail: datenschutz@bern.ch

Öffnungszeiten: Montag bis Donnerstag, 08.00–12.00 Uhr und 13.30–16.30 Uhr

www.bern.ch/datenschutzaufsicht

Impressum

Herausgeberin: Fach- und Aufsichtsstelle Datenschutz der Stadt Bern
Layout: Logistik Stadt Bern, Layout und Design
Abbildung Titelseite: Ocskaymark

Inhaltsverzeichnis

Vorwort

Geschätzte Mitglieder des Stadtrates, Mitglieder des Gemeinderates,
Mitarbeitende der Stadtverwaltung und der stadtnahen Betriebe,
geschätzte Bevölkerung der Stadt Bern, geschätzte Leser*innen

Ich freue mich, Ihnen gestützt auf Artikel 37 Abs. 3 des Datenschutzgesetzes des Kantons Bern vom 19. Februar 1986 (KDSG, BSG 152.04) und auf Artikel 5 des Datenschutzreglements der Stadt Bern (DSR; SSSB Nr. 152.06) mit der Unterstützung meines Teams über die Tätigkeit im Jahr 2025 zu berichten.

Nicht das Datenschutzrecht ist komplexer geworden, sondern die digitale Welt. Die rasante Digitalisierung der Verwaltung, die stetig zunehmende Vernetzung von Systemen und Prozessen, aber auch die wachsende Bedrohung durch Cyberkriminalität stellen die Akteur*innen in der Stadt vor neue und anspruchsvolle Herausforderungen. Daten werden heute schneller verarbeitet und vielfältiger genutzt und ausgetauscht als je zuvor. Damit steigen auch die damit verbundenen Risiken.

Vor diesem Hintergrund war das Berichtsjahr geprägt von einer nochmals intensivierten Zusammenarbeit zwischen der FADS und den verschiedenen Verwaltungsstellen. Ziel war es, digitale Vorhaben frühzeitig datenschutzkonform zu gestalten, Risiken realistisch einzuschätzen und tragfähige Lösungen zu entwickeln. Die FADS nahm dabei ihre Doppelrolle als Beratungs- und Aufsichtsorgan wahr. Sie vermittelte Wissen zum Datenschutz, unterstützte bei der praktischen Umsetzung und sensibilisierte für die Anliegen des Datenschutzes. Der Bedarf an solcher Begleitung bleibt in der Stadtverwaltung hoch, und die Arbeit wird der FADS auch in Zukunft nicht so rasch ausgehen.

Im kommenden Jahr tritt zudem das revidierte kantonale Datenschutzrecht in Kraft. Entgegen gewissen Vorurteilen bedeutet dies für die Stadt keinen grundlegenden höheren Aufwand. Viele der neuen Vorgaben entsprachen bereits bisher geltendem Recht oder der Praxis in der Stadt Bern, werden nun jedoch klarer und präziser geregelt. Dies erleichtert die Anwendung, gerader im Umgang mit den neuen digitalen Herausforderungen.

Die Stadt hat die notwendigen Vorbereitungsarbeiten für das neue Datenschutzrecht frühzeitig in Angriff genommen. Ich bin zuversichtlich, dass sie den Übergang damit ohne grosse Mühen und mit der erforderlichen Sorgfalt vollziehen kann.

Gleichwohl bleibt der Datenschutz aber kein Selbstläufer. Es braucht weiterhin den Willen, sich damit auseinanderzusetzen und bestmögliche Lösungen dafür anzustreben. Daher ist es wichtig, dass auch Politik und Bevölkerung dies von der Stadtverwaltung immer wieder einfordern.

Sophie Haag
Datenschutzbeauftragte der Stadt Bern

Bern, im Januar 2026

1

Rückblick

Die Zusammenarbeit mit der Stadtverwaltung entwickelt sich erfreulich. Die top Themen blieben dabei im Vergleich zu den Vorjahren unverändert. Zugenommen hat jedoch die Komplexität der bearbeiteten Themen.

Themen im Berichtsjahr
Die zunehmende Komplexität der digitalen Welt stellt auch die Mitarbeitenden der Stadtverwaltung vor Herausforderungen. Im Berichtsjahr hat sich gezeigt, dass z.B. die für den Informations- und Datenschutz zentrale Klassifizierung von Dokumenten im Arbeitsalltag nicht immer ganz einfach ist. So hat die FADS im Berichtsjahr diverse Beratungsanfragen dazu bearbeitet und war auch in die Verbesserung der diesbezüglichen Informationen für die städtischen Mitarbeitenden involviert (siehe Kapitel 3, S. 10 ff.). Immer wieder musste die FADS auch den Umgang mit Datenschutzrisiken bei der Planung zu neuen Applikationen beanstanden (siehe Kapitel 4, S. 13 ff.).

Erneut betraf der grösste Teil der von der FADS bearbeiteten Fälle geplante neue Applikationen. Dem im Vorjahr überarbeiteten ISDS-Prozess (siehe Tätigkeitsbericht 2024 S. 8 ff.) folgend hat die FADS diverse Schutzbedarfsanalysen geprüft und Vorabkontrollen durchgeführt. Besorgniserregend ist eine feststellbare Entwicklung bei der Beschaffung von Fachapplikationen. So wird es zunehmend schwieriger, ein Produkt zu finden, bei dem keine Datenbearbeitung auf der Infrastruktur von US-Hyperscalern wie Microsoft stattfindet (siehe Kapitel 5, S. 16 f.).

Die FADS hat im Berichtsjahr aber auch die bereits laufende Datenbearbeitung durch die Einwohnerkontrolle einer ordentlichen Kontrolle unterzogen.

«Die zunehmende Komplexität der digitalen Welt stellt die Mitarbeitenden vor Herausforderungen»

Neben neuen Applikationen und grösseren städtischen Projekten gehörten einmal mehr Videoüberwachungen und die Weitergabe von Personendaten zu den top Themen im Berichtsjahr, wobei einige Beratungsanfragen die Weitergabe von Informationen an die Kantonspolizei betroffen haben.

Vernetzung, Austausch und Weiterbildungen

Die Zusammenarbeit mit der Stadtverwaltung hat sich im Berichtsjahr erfreulich weiterentwickelt. Die FADS wird nun auch vermehrt im Vorfeld von Stadtrats- oder Gemeinderatsgeschäften für eine Stellungnahme begrüsst. Auch fand erstmalig ein Austausch mit dem Gemeinderat statt, der nun regelmässig weitergeführt werden soll. Auch die Zusammenarbeit mit ICT-Security hat sich etabliert, so dass die FADS nun früher Kenntnis von datenschutzrelevanten Vorhaben erhält und sich früher aktiv in Projekte einbringen kann. Ebenfalls intensiviert wurde die Zusammenarbeit mit Digital Stadt Bern. So konnte die FADS bei den Vorbereitungen auf das kommende revidierte Datenschutzrecht oder an der Erarbeitung einer Governance zu grossen Themen wie KI mitwirken. Durch den Austausch konnten aber auch grosse Informatikvorhaben koordiniert werden, was sich für beide Seiten als gewinnbringend erwiesen hat. Für die Koordination der Aufsichtstätigkeit war auch der Austausch mit der Finanzkontrolle und den weiteren Legislativstellen wertvoll.

Weitergeführt wurde auch die Zusammenarbeit mit anderen Datenschutzbehörden. Dies hat der FADS bei der Bearbeitung von Aufsichtsfällen geholfen. Im Hinblick auf das revidierte Datenschutzrecht wurden auch Gespräche mit der kantonalen Datenschutzaufsicht und der Datenschutzaufsicht anderer Städte im Kanton geführt.

Im Berichtsjahr konnte die FADS an mehreren Veranstaltungen in der Stadtverwaltung wichtige Themen zum Datenschutz präsentieren, was zu einem bewussteren Umgang mit Personendaten beiträgt. Sie hat aber auch selbst regelmässig an Weiterbildungen teilgenommen, um ihr Wissen aktuell zu halten.

«Die Zusammenarbeit mit der Stadtverwaltung entwickelt sich erfreulich»

Die Zusammenarbeit mit der GPK war für die FADS auch im Berichtsjahr wichtig und wertvoll. Mit dem spürbaren politischen Rückhalt für ihre Tätigkeit ist es ihr möglich, den Datenschutz in der Stadt weiterhin zu verbessern.

2

Ausblick: Revidiertes Datenschutzrecht im Kanton Bern

Im Sommer 2026 wird voraussichtlich das totalrevidierte kantonale Datenschutzrecht in Kraft treten. Auf den ersten Blick werden damit für die öffentlichen Verwaltungen im Kanton Bern namhafte neue Vorgaben zum Datenschutz eingeführt. Vieles davon entspricht jedoch bereits der jetzigen Praxis in der Stadt Bern, die nach Einschätzung der FADS gut auf diesen Wechsel vorbereitet ist.

Im Dezember des Berichtsjahres verabschiedete der Grosse Rat des Kantons Bern ein totalrevidiertes kantonales Datenschutzgesetz. Vorbehältlich eines dagegen ergriffenen Referendums soll es im Sommer 2026 in Kraft treten. Die dazugehörigen Verordnungen sind zurzeit in Vernehmlassung.

Mit den revidierten kantonalen Erlassen erhält die Stadt Bern einen grundlegend überarbeiteten rechtlichen Rahmen für den Datenschutz in der Verwaltung, und auf den ersten Blick scheint sich viel zu ändern. Die Pflichten für datenbearbeitende Behörden werden erweitert, die Rechte der Betroffenen klarer definiert, der Katalog der besonders schützenswerten Personendaten modernisiert und ergänzt, und mit dem Profiling mit hohem Risiko wird eine Bearbeitungsmethode ins Recht gefasst, um den Risiken beim Einsatz neuer Technologien besser gerecht zu werden. Zudem werden Stellung, Unabhängigkeit und Befugnisse der Datenschutzaufsichtsstellen gestärkt. Insgesamt wird das kantonale Datenschutzrecht an dasjenige des Bundes und der EU angeglichen, was mit Blick auf die Weiterentwicklung des Schengen-Besitzstands und die Gleichwertigkeit des Datenschutzes im europäischen Rechtsraum nötig geworden ist.

«Die Stadt ist auf das revidierte Datenschutzrecht gut vorbereitet»

Die FADS ist optimistisch, dass die Stadtverwaltung auf das revidierte Datenschutzgesetz gut vorbereitet ist und die Änderungen für sie gut umsetzbar sind. Dies zeigt sich an folgenden Beispielen:

Erweiterte Pflichten der Behörden
Das revidierte Datenschutzgesetz schreibt die Pflichten bei der Planung einer neuen, wiederkehrenden Datenbearbeitung nun ausführlicher vor. Die neuen Regelungen entsprechen jedoch der bisherigen Praxis bei Informatikprojekten in der Stadt Bern.

Trotzdem bereitet sich die Stadt aktiv auf die Rechtsänderung vor: Zurzeit laufen die Arbeiten an einer neuen städtischen Weisung für die Beschaffung neuer IT-Mittel, mit der die bisherige Praxis und damit das neue Datenschutzrecht für die Mitarbeitenden der Stadt verbindlich geregelt werden sollen. Die Weisung soll verständlich aufzeigen, welche Arbeiten bei der Einführung neuer Applikationen für eine datenschutzkonforme Planung anfallen, wann diese zu erfolgen haben und wer dafür verantwortlich ist. Damit erhalten die Projektverantwortlichen in der Stadt nun zwar klarere Leitplanken für eine IT-Beschaffung in Einklang mit dem (neuen) Recht, am einzuhaltenden Prozess ändert sich jedoch wenig. Die FADS wurde in die Arbeiten an dieser Weisung mit einbezogen.

Auch die erweiterte Informationspflicht bei der Beschaffung von Personendaten und die neu eingeführte Informationspflicht bei automatisierten Einzelfallentscheidungen dürften in der Stadt zu keinem grossen Mehraufwand führen. Erstere wird voraussichtlich in den meisten Fällen und wie bisher durch den Eintrag im Register der Datensammlungen erfüllt werden, und Zweitere fällt aktuell kaum ins Gewicht, da nach Kenntnis der FADS zurzeit in der Stadt keine Systeme mit automatisierten Einzelfallentscheidungen im Einsatz sind.

Ebenfalls neu sind die Meldepflichten bei schweren Datensicherheitsvorfällen. Allerdings muss die Stadt ihre Pflichten zur Gewährung der Datensicherheit ohnehin ernst nehmen, und zwar unabhängig davon, welches Datenschutzrecht in Kraft ist. Nur so kann verhindert werden, dass es überhaupt zu schweren Datenpannen kommt. Die FADS unterstützt dabei, dass die Stadt diese Pflichten wahrnehmen kann und den Herausforderungen in diesem Bereich gewachsen ist.

Stellung, Unabhängigkeit und Befugnisse der Datenschutzaufsichtsstellen
Die bisher föderalistisch ausgestaltete Datenschutzaufsicht soll grösstenteils zentralisiert werden. Anstelle der kommunalen Aufsichtsstellen wird die Datenschutzaufsicht über die Gemeinden nach neuem Recht durch die kantonale Stelle übernommen. Damit sollen die Gemeinden entlastet und der erhöhten Komplexität des Datenschutzes Rechnung getragen werden. Dies gilt jedoch nicht für Gemeinden mit mehr als 25'000 Einwohner*innen, welche auch unter neuem Recht ihre eigenen Datenschutzbehörden haben. Die FADS bleibt damit weiterhin zuständig für Datenschutzbelange der Stadt Bern.

Eine markante Änderung ist jedoch die neue Kompetenz der Datenschutzbehörden, bei einer drohenden oder bestehenden erheblichen Verletzung von Datenschutzbestimmungen eine Verfügung gegen die fragliche Datenbearbeitung zu erlassen. Die FADS ist und bleibt kein reines Aufsichtsorgan. Sie wird auch unter dem neuen Recht einen starken Fokus auf die Beratung von Behörden und Bevölkerung legen und als Fachstelle den Datenschutz durch eine beratende Zusammenarbeit mit den Behörden verbessern, um von der neuen Verfügungskompetenz nur in Ausnahmefällen Gebrauch machen zu müssen.

3

Klassifizierung, Daten- und Informationsschutz, Amtsgeheimnis und besondere Geheimhaltungspflichten

Im Zusammenhang mit Beratungen wurden von städtischen Stellen im Berichtsjahr vermehrt auch Fragen zur Klassifizierung von Informationen, zur Rolle des Amtsgeheimnisses und besonderer Geheimhaltungspflichten sowie allgemein zum Unterschied zwischen Daten- und Informationsschutz aufgeworfen. Die FADS nimmt dies zum Anlass, nachstehend einen Überblick über die zusammenhängenden und komplexen Fragestellungen zu schaffen.

Informationssicherheit bezweckt den umfassenden Schutz sämtlicher durch die Stadt Bern bearbeiteten Informationen, einschliesslich Personendaten, vor Bedrohungen und dient damit den Interessen der Stadt Bern als Gemeinwesen. Der Begriff Informationssicherheit umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Nachvollziehbarkeit von Informationen und Daten aller Art sowie die Verfügbarkeit und die Integrität von Informatikmitteln geschützt werden. Der hier beleuchtete Informationsschutz zielt auf die Gewährleistung der Vertraulichkeit von Informationen ab und stellt eine Teilmenge der Informationssicherheit dar.

«Datenschutz als Schutz von Rechten und Freiheiten»

Datenschutz bezieht sich demgegenüber ausschliesslich auf Personendaten und will damit die Rechte und Freiheiten der betroffenen Personen schützen. Das Recht auf Datenschutz ist ein Grundrecht, welches in Art. 13 Abs. 2 der Bundesverfassung als informationelle Selbstbestimmung und in Art. 18 der Kantonsverfassung als Recht auf Datenschutz verankert ist und im KDSG konkretisiert wird. Das kantonale Datenschutzrecht regelt vorab die Grundsätze, nach welchen Behörden Personendaten bearbeiten dürfen. Dazu gehören nebst denjenigen der Gesetzmässigkeit, Verhältnismässigkeit, Zweckbindung und Transparenz auch die Verpflichtung, für die Sicherheit der bearbeiteten Personendaten mit technischen und organisatorischen Massnahmen zu sorgen (Art. 17 KDSG und Art. 4 f. Datenschutzverordnung). In diesem Bereich

überschneiden sich Datenschutz und Informationssicherheit. Nur mit einem wirksamen Informationsschutz können auch die Ziele des Datenschutzes erreicht werden.

Um die zu ergreifenden Sicherheitsmassnahmen festlegen zu können, müssen Informationen, einschliesslich solcher mit Personendaten, nach ihrem Schutzbedarf, d.h. nach ihrer Sensibilität und Kritikalität, eingestuft werden. Diesem Zweck dient die Klassifizierung als Massnahme des Informationsschutzes. Für die Stadt Bern erfolgt die Klassifizierung nach der im Rahmen der Einführung von M365 erlassenen Weisung über die Klassifizierung von elektronischen Daten (Klassifizierungsweisung). Mit der Zuweisung der Klassifizierungsstufe werden gleichzeitig die darauf anwendbaren Bearbeitungsregeln festgelegt. Die Klassifizierungsweisung legt folgende vier Klassifizierungsstufen sowie entsprechende Bearbeitungsregeln fest:

Öffentlich
Als öffentlich werden Daten bezeichnet, die von der zuständigen Stelle zur Veröffentlichung freigegeben sind (Art. 6 Klassifizierungsweisung). Bezüglich Bearbeitung öffentlicher Daten bestehen keine Einschränkungen. Beispiele für öffentliche Daten sind Medienmitteilungen des Gemeinderats oder Open Government Data (frei zugängliche Verwaltungsdaten). Öffentliche Daten enthalten meist keine Personendaten.

Intern
Als intern werden Daten klassifiziert, die nur für die Mitarbeitenden der Stadtverwaltung bestimmt sind. Interne Daten können ohne Einschränkung an Mitarbeitende der Stadtverwaltung übermittelt werden, sofern diese dienstlich benötigt werden. Sie müssen zugriffsbeschränkt gespeichert bzw. aufbewahrt werden (Art. 7 Klassifizierungsweisung) und dürfen im Rahmen der Bürokommunikation mit M365 bearbeitet werden. Für elektronisch bearbeitete Daten stellt die Stufe intern die defaultmässige Klassifizierungsstufe dar. Damit sind alle einzig dem Amtsgeheimnis unterstehenden Informationen, die keine besonders schützenswerten Personendaten enthalten, als intern zu klassifizieren.

«Mit der Klassifizierung werden die anwendbaren Bearbeitungsregeln festgelegt»

Vertraulich
Als vertraulich werden Daten klassifiziert, die nur für einen definierten Personenkreis bestimmt sind. Die Kenntnisnahme vertraulicher Daten durch Unbefugte kann der Stadtverwaltung einen wesentlichen Schaden verursachen oder Dritte in ihren persönlichen Verhältnissen verletzen (Art. 8 Abs. 1 Klassifizierungsweisung). Vertraulich klassifizierte Daten unterliegen den strengeren, in Art. 8 Abs. 2 aufgeführten Bearbeitungsregeln. Bezüglich elektronischem Versand wird festgehalten, dass dieser verschlüsselt zu erfolgen hat. Beispiele für als vertraulich zu klassifizierende Daten sind Gemeinderatsgeschäfte oder Sicherheitsdokumentationen zu städtischen Applikationen. Ebenfalls als vertraulich zu klassifizieren sind aufgrund der erhöhten Sensibilität ihrer Inhalte besonders schützenswerte Personendaten nach Art. 3 KDSG; also Angaben zu Religion, politischer Einstellung und Betätigung, Rassenzugehörigkeit, Gesundheit, sexueller Orientierung, Massnahmen der sozialen Fürsorge oder des Kindes- und Erwachsenenschutzes sowie solche zu polizeilichen Ermittlungen und Strafverfahren.

Im Weiteren sind Daten als vertraulich zu klassifizieren, welche besonderen Geheimhaltungspflichten wie dem Sozialhilfegeheimnis, der Schweigepflicht von Ärzt*innen und medizinischen Fachpersonen oder dem Steuergeheimnis unterstehen. Besondere Geheimhaltungspflichten werden in der jeweiligen Fachgesetzgebung statuiert. Zu beachten ist in diesem Zusammenhang, dass das Amtsgeheimnis keine besondere Geheimhaltungspflicht darstellt. Es gilt für sämtliche städtischen Angestellten und für alle dienstlichen Informationen, auch für Sachdaten. Besonderen Geheimhaltungspflichten bestehen nur im entsprechenden Aufgabenbereich (Sozialhilfe, Gesundheitswesen, Steuern, etc.). Schutzobjekt bilden die Persönlichkeitsrechte und damit die in aller Regel besonders schützenswerten Personendaten der Betroffenen. Verletzungen sowohl des Amtsgeheimnisses wie auch besonderer Geheimhaltungspflichten können strafrechtliche Folgen nach sich ziehen (Art. 320 StGB).

Geheim

Als geheim werden Daten klassifiziert, die nur für einen eingeschränkten, explizit festgelegten Personenkreis der obersten Führungsebene bestimmt sind. Die unberechtigte Kenntnisnahme geheimer Informationen ist geeignet, der Stadt Bern einen schweren Schaden beizufügen. Entsprechend sind die Bearbeitungsregeln für geheime Informationen äusserst eingeschränkt. In der Praxis betrifft dies nur ganz wenige Informationen, wie z.B. das gesamtstädtische Sicherheits- und Versorgungsdispositiv. Nebst Sachdaten könnten auch Personendaten von speziell exponierten Persönlichkeiten als geheim klassifiziert werden, wenn durch deren Offenbarung z.B. eine unmittelbare Gefahr für Leib und Leben bestünde. Nachstehend zur Übersicht eine Konkordanztabelle zu den anwendbaren Klassifizierungstufen beim Datenschutz und dem Amtsgeheimnis sowie den besonderen Geheimhaltungspflichten:

Klassifizierungsstufe	Datenschutz	Amtsgeheimnis, beso. Geheimhaltungspflichten
öffentlich	-	-
intern	**Normale Personendaten**	**Amtsgeheimnis**
vertraulich	**Besonders schützenswerte Personendaten**	**Besondere Geheimhaltungspflichten**
geheim	-	-

Konkordanztabelle Klassifizierungsstufen

4

Umgang mit Datenschutzrisiken

Der Umgang mit Datenschutzrisiken war im Berichtsjahr in beratenden wie auch in aufsichtsrechtlichen Geschäften der FADS immer wieder ein zentrales Thema. Nebst der Identifikation von potenziellen Risiken für Personen, die von einer geplanten Datenbearbeitung betroffen sind, ging es dabei auch um geeignete Massnahmen zur Risikominderungen sowie um die transparente Darlegung der verbleibenden Restrisiken.

Der korrekte Umgang mit Risiken ist im modernen Datenschutzrecht zentral. Dass eine gänzlich risikofreie Personendatenbearbeitung nicht existiert, setzt sich als Erkenntnis immer mehr durch, womit der Fokus nun auf der Frage liegt, welche Massnahmen notwendig sind, um die bestehenden Risiken auf ein vertretbares Mass zu reduzieren. In der Stadt Bern muss für die Bearbeitung von Daten mit erhöhtem Schutzbedarf bereits bei deren Planung eine Risikoanalyse durchgeführt werden. Sie ist Teil der geforderten ISDS-Dokumentation und ist auch im laufenden Betrieb aktuell zu halten, damit auf Veränderungen angemessen reagiert werden kann.

«Eine gänzlich risikofreie Personendatenbearbeitung existiert nicht»

Als Risiko wird grundsätzlich die Möglichkeit eines Schadens bezeichnet. Um potenzielle Schäden zu ermitteln, wird der Blick auf Gefährdungen gerichtet, die zu Störfällen führen können.[1] Wichtig dabei ist, immer den ganzen Lebenszyklus von Daten, von der Erhebung über den Transport resp. der Übermittlung und Speicherung bis zur Archivierung und Löschung, im Blickfeld zu haben. Nach der Formulierung von Risiken, die sich aus den ermittelten Gefährdungen ergeben können, wird eruiert, welche Sicherheitsmassnahmen die Wahrscheinlichkeit oder das Schadensmass von

1 Siehe dazu auch den hilfreichen Katalog «Elementare Gefährdungen» des deutschen Bundesamtes für Informationssicherheit BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4

Störfällen begrenzen können, und welche Restrisiken auch nach Umsetzung dieser Massnahmen verbleiben. Je nach Art des identifizierten Restrisikos muss auch geklärt und bestimmt werden, von welcher Stelle dieses getragen werden muss.

Die FADS hat wiederholt festgestellt, dass der korrekte Umgang mit Datenschutzrisiken herausfordernd sein kann. Den Projektverantwortlichen ist dabei auch oft nicht klar, wie eine Risikoanalyse korrekt durchzuführen ist. Nachfolgend sollen daher beispielhaft für den Datenschutz relevante Gefährdungen und Risiken beschrieben und geeignete Massnahmen zu deren Mitigation diskutiert werden. Der Text orientiert sich dabei an den wichtigsten Schutzzielen «Vertraulichkeit», «Verfügbarkeit» und «Integrität» von Personendaten. Nebst diesen allgemeinen Risiken bestehen für Cloud-Anwendungen weitere, Cloud-Spezifische Risiken. Genaueres dazu kann dem Merkblatt von Privatim entnommen werden.[2]

«Aus Eintretenswahrscheinlichkeit und Schadensmasses wird Risiko ermittelt»

Vertraulichkeit
Mit dem Schutzziel der Vertraulichkeit soll eine Kenntnisnahme personenbezogener Daten durch unbefugte Dritte verhindert werden. Das unbefugte und möglicherweise auch unbeabsichtigte Offenlegen oder Einsehen von Personendaten kann dabei durch Hackerangriffe, Zugriffe von US-Behörden gestützt auf den CLOUD-Act, fehlerhaftes Berechtigungsmanagement, ungenügende Authentifizierung oder auch menschliche Fehler geschehen. Wichtige Massnahmen, um diese Risken zu senken, sind die Verschlüsselung von Daten bei der Übertragung und während der Speicherung sowie dem Schutzbedarf entsprechende und nach Need-to-Know vergebene Zugriffsrechte auf Datenbestände. Nebst diesen technischen Massnahmen können auch physische Massnahmen wie eine Zutrittssicherung oder auch organisatorische Massnahmen wie Richtlinien, Schulungen und Prozesse die Risiken senken.

Verfügbarkeit
Verfügbarkeit meint, dass Daten, Software und Hardware für autorisierte Nutzer jederzeit zugänglich, abrufbar und nutzbar sein sollen. Eine Beeinträchtigung der Verfügbarkeit kann bspw. durch einen sog. DDoS-Angriff[3], durch Schwachstellen und ungenügende Lasttests der Software oder auch durch Ausfälle der Hardware erfolgen. Mögliche Massnahmen dagegen sind Backups und Ersatzrechner sowie redundante Komponenten, die Lastverteilung mit Server-Cluster oder auch Qualitätssicherung von Software sowie das Erkennen von Anomalien mittels Intrusion Detection Systemen und zentraler Logauswertung.

Integrität
Integrität bedeutet, dass Daten über ihren gesamten Lebenszyklus hinweg korrekt, vollständig, konsistent und unverändert vorhanden sind, also vor unbefugter Änderung, Zerstörung oder Verlust geschützt werden. Unbefugterweise oder versehentlich verfälschte oder veränderte Daten können bspw. durch Identitätsdiebstahl,

2 Online abrufbar unter: https://www.privatim.ch/wp-content/uploads/2023/10/privatim_Cloud-Merkblatt_v3_01_20220203_def._DE.pdf

3 DDoS = Distributed Denial of Service. Verhinderung von Diensten durch bspw. gezielte Überlastung von Diensten eines Servers

durch Fehlfunktionen von Software oder Übermittlungsfehler oder durch Fehlverhalten von Personen wie bspw. eine Fehlbedienung von Anwendungen resultieren. Mögliche Massnahmen dagegen sind der Einsatz von Hash-Funktionen für Prüfsummen und digitale Signaturen, eine angemessene Identitätsprüfung für Zugriffsberechtigungen sowie die Absicherung von Zugriffen mit einem zweiten Faktor und umfassende Softwaretests. Nebst diesen technischen Massnahmen können auch organisatorische Massnahmen wie Schulungen und Richtlinien sinnvoll sein.

«Reduzierung des Risikos durch geeignete Massnahmen»

Ausweisung und Tragbarkeit Restrisiko

Die so ermittelten Risiken sind in einer Risikoanalyse durch Beurteilung von Eintretenswahrscheinlichkeit und Schadensmass zu bewerten. Dabei wird das Bruttorisiko vor und die Minderung des Risikos nach Umsetzung der technischen und organisatorischen Massnahmen sowie das verbleibende Restrisiko (Nettorisiko) beurteilt. Oftmals kann mit geeigneten Massnahmen die Eintretenswahrscheinlichkeit eines Risikos gesenkt werden, auf das Schadensmass haben die Massnahmen jedoch nur selten einen Einfluss. Die auch nach Umsetzung der Massnahmen verbleibenden Restrisiken sind transparent auszuweisen und von geeigneter Stelle zu übernehmen.

5

US-Hyperscaler als Unterauftragsnehmerinnen

Anbieterinnen von Software-as-a-Service nutzen für den Betrieb ihres Produktes vermehrt die Infrastruktur grosser Cloud-Anbieterinnen. Um zu verhindern, dass es auf diesem Weg zu einer systematischen Bearbeitung besonders schützenswerter Personendaten der Stadt auf den Servern von US-Hyperscalern kommt, ist die Frage der genutzten Infrastruktur bereits bei der Beschaffung von Fachapplikationen zu klären.

Werden für Datenbearbeitung der Stadtverwaltung Cloud-Dienste in Anspruch genommen, muss dabei die Weisung Cloud Computing der Stadt Bern (WCC) eingehalten werden. Diese schreibt für das Bearbeiten besonders schützenswerter Personendaten in der Cloud eine Verschlüsselung vor. Wenn die für die Verschlüsselung verwendeten privaten Schlüssel nicht ausschliesslich der Stadt bekannt sind, muss sich die Cloud-Anbieterin ausserdem vertraglich verpflichten, sie nur mit der ausdrücklichen Zustimmung der Stadt zu verwenden (Ziff. 5.1 Anhang 2 WCC). Der Gemeinderat hat in seinem Risikoübernahmeentscheid zu Microsoft 365 (siehe Tätigkeitsbericht 2023 S. 11 ff.) zusätzlich gefordert, dass besonders schützenswerte Personendaten nicht systematisch in der Microsoft Cloud bearbeitet werden dürfen, sondern hierzu geeignete Fachapplikationen zu verwenden sind.

«Bei Fachapplikationen ist auf die Infrastruktur von US-Hyperscalern zu verzichten»

Die FADS interpretiert den Entscheid des Gemeinderates wie folgt: In den geforderten Fachapplikationen darf keine Bearbeitung von besonders schützenswerten Personendaten auf Servern von Microsoft erfolgen. Anderenfalls würde der zusätzliche Schutz der Daten durch den Einsatz der Fachapplikation wegfallen. Die Vorgabe des Gemeinderates muss ausserdem auch auf weitere Cloud-Anbieterinnen mit Sitz in den USA ausgedehnt werden. Die Bedenken hinsichtlich der Vertraulichkeit der auf den Servern von Microsoft bearbeiteten Daten basie-

ren nicht auf Gründen, die bei Microsoft selbst liegen, sondern auf der Tatsache, dass die Firma mit Sitz in den USA dem US-Cloud Act unterliegt. Offenbar schätzt der Gemeinderat bei einer Ermittlungsanfrage durch eine US-Behörde das Risiko einer Herausgabe entgegen anderslautenden vertraglichen Zusicherungen für die systematische Bearbeitung besonders schützenswerter Personendaten als nicht tragbar ein. Dies muss für sämtliche Anbieterinnen gelten, die dem US-Cloud-Act unterstehen, weshalb bei Fachapplikationen nicht nur die Microsoft Cloud, sondern auch Clouddienste anderer US-Anbieterinnen ausgeschlossen werden müssen.

Im Berichtsjahr stellte die FADS fest, dass bei der Beschaffung von Fachapplikationen zwar darauf geachtet wird, Anbieterinnen mit Sitz ausserhalb der USA zu wählen, oft kommen sogar Anbieterinnen aus der Schweiz zum Zug. Allerdings wurde dabei wiederholt übersehen, dass die gewählten Anbieterinnen die Infrastruktur von US-Hyperscalern wie Microsoft oder Amazon als Unterauftragnehmerinnen nutzen. Während dies aus wirtschaftlichen Überlegungen nachvollziehbar ist, kann es dazu führen, dass besonders schützenswerte Personendaten der Stadt auf diesem Umweg doch wieder in den Anwendungsbereich des US-Cloud Acts gelangen.

«Die Beurteilung der Datenschutzkonformität ist komplexer geworden»

Eine naheliegende Lösung wäre es, die Daten so zu verschlüsseln, dass die US-Hyperscaler keinen Zugriff auf Klardaten haben und die Entschlüsselung technisch unterbunden ist. Oft lässt sich dies jedoch nicht umsetzen. Einerseits kann eine diese Anforderung erfüllende Verschlüsselung aufwändig sein und die Möglichkeiten der Stadt oder kleiner Anbieterinnen übersteigen. Andererseits handelt es sich bei Fachapplikationen vermehrt um Software-as-a-Service, bei der die Infrastruktur der US-Hyperscaler nicht für eine einfache Datenspeicherung genutzt wird, sondern die eigentliche Datenbearbeitung selbst dort stattfindet. Zur Bearbeitung müssen die Daten unverschlüsselt vorliegen. Damit würde genau das passieren, was der Gemeinderat mit seinem Risikoentscheid zu Microsoft 365 verhindern wollte.

Dieses Beispiel zeigt deutlich: Aufgrund der zunehmenden weltweiten digitalen Vernetzung ist es komplexer geworden, die Datenschutzkonformität von Systemen und Applikationen zu beurteilen. Gerade bei Software-as-a-Service reicht es nicht mehr, nur die unmittelbare Anbieterin zu prüfen. Bei der Beschaffung von Fachapplikationen, mit denen besonders schützenswerte Personendaten bearbeitet werden, muss vielmehr auch darauf geachtet werden, dass keine Unterauftragsbearbeiterinnen mit Sitz in den USA oder Ländern ohne angemessenes Datenschutzniveau eingesetzt werden, sofern das Schlüsselmanagement nicht vollständig durch die Stadt selbst erfolgen kann.

6

Statistik

Die Zahl der bearbeiteten Dossiers hat erneut zugenommen, wobei insbesondere die Zunahme bei den formellen Stellungnahmen ins Auge springt. Die Statistik zeigt auch, dass das Thema KI in der Stadtverwaltung angekommen ist.

Die Fach- und Aufsichtsstelle Datenschutz unterscheidet bei ihrer täglichen Arbeit zwischen Fällen und Anfragen. Als Anfragen werden Anliegen erfasst, welche mit geringem Aufwand beantwortet werden können. Fälle benötigen demgegenüber eine vertiefte Abklärung und intensivere Beratung.

Im Berichtsjahr hat die Zahl der bearbeiteten Dossiers zugenommen, es wurden insgesamt 184 davon bearbeitet (Vorjahr 151). Von 24 aus dem Vorjahr übertragenen und 118 neu eröffneten Fällen sowie 42 eröffneten Anfragen konnten 157 abgeschlossen werden. 27 Fälle wurden zur Weiterverarbeitung auf das Folgejahr übertragen.

Die Anzahl der bearbeiteten Fälle hat gegenüber dem Vorjahr um rund 18% zugenommen. Die auffälligste Zunahme ist bei den formellen Stellungnahmen zu verzeichnen, welche von 2 im Vorjahr auf 12 im Berichtsjahr gestiegen sind. Dies ist erfreulich, zeigt es doch, dass sich die Zusammenarbeit zwischen der FADS und der städtischen Verwaltung bei der Vorbereitung datenschutzrelevanter Stadtrats- oder Gemeinderatsgeschäfte stark verbessert hat. Erneut zugenommen hat auch die Zahl der verwaltungsinternen Beratungen (+ 21%). Wie bereits im letzten Jahr berichtet, werden Projektverantwortliche im städtischen ISDS-Prozess nun stärker durch die ICT-Sicherheit von IBE begleitet (vgl. Tätigkeitsbericht 2024 S. 23), so dass im Berichtsjahr kein Bedarf an ISDS-Workshops bei der FADS mehr bestand. Damit konnte sich die FADS im Vorfeld von Vorabkontrollen auf Reviews von ISDS-Unterlagen sowie auf die Prüfung einer möglichen Vorabkontrollpflicht einzelner Projekte konzentrieren.

Neu werden in der Statistik Beratungen für andere Legislativstellen sowie Anfragen anderer Datenschutzbehörden ausgewiesen. Hier zeigt sich, dass die FADS nicht

nur für die Verwaltung im engeren Sinne, sondern für alle Behörden der Stadt Bern tätig ist. Und Dank der Vernetzung mit anderen Datenschutzbehörden können wichtige Informationen, insb. zu bereits kontrollierten Applikationen, ausgetauscht werden, was die Arbeit der FADS erleichtern kann.

Während sich die Zahl der Vorabkontrollen in einem mit den Vorjahren vergleichbaren Rahmen bewegt, hat die Zahl der Beratungen von Privatpersonen erneut abgenommen.

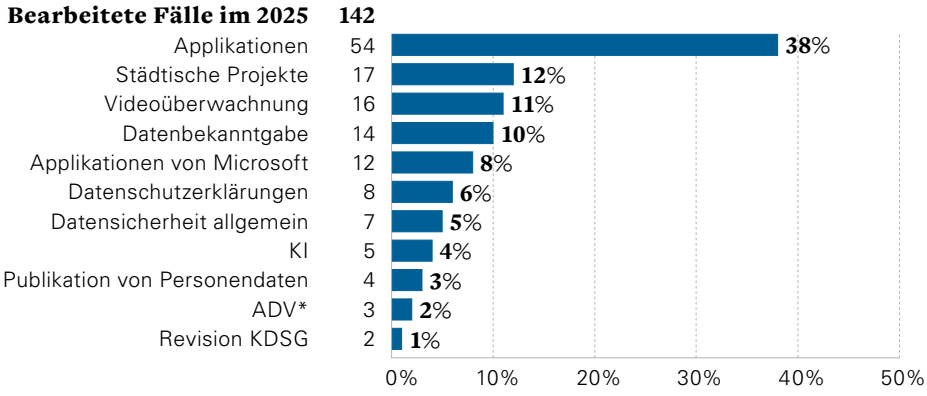
Kennzahlen Gesamtübersicht	2025	2024
Fälle	**142**	**120**
Fälle aus dem Vorjahr	24	28
Neu eröffnete Fälle	118	92
Anfragen	**42**	**31**
Total Fälle und Anfragen	**184**	**151**
Pendent per Ende Jahr	27	24

Kennzahlen bearbeitete Fälle	2025	2024
Bearbeitete Fälle von Privatpersonen	**6**	**12**
Beratung	2	8
Aufsichtsrechtliche Anzeigen	4	2
Auskunftsgesuche	0	2
Bearbeitete Fälle Verwaltung und Betriebe	**124**	**108**
Beratung	92	76
ISDS-Workshop	0	2
Prüfung Vorabkontrollpflicht	7	0
Review	29	20
Beratung im engeren Sinn	56	54
Nachträgliche Überprüfung	0	5
Vorabkontrolle	19	18
Audit	1	1
Formelle Stellungnahme	12	2
Führen Register der Datensammlung	0	5
Umsetzung Empfehlungen	0	1
Bearbeitete Fälle Legislativstellen	**7**	-
Anfragen anderer Datenschutzaufsichtsstellen	**5**	-

Ein Blick auf die von der FADS im Berichtsjahr bearbeiteten Themengebiete zeigt Folgendes: Erneuter Spitzenreiter sind neue Applikationen, welche im Berichtsjahr 38% der Fälle betrafen. Deutlich zugenommen hat die Anzahl der grösseren städtischen Projekte, also von Fällen, bei denen deutlich mehr als nur eine einzelne Applikation zu beurteilen war (17 im Berichtsjahr, im Vorjahr 7). Erneut separat erfasst wurden Fälle in Zusammenhang mit Microsoft. Im Vergleich zum Vorjahr haben die Fälle wieder zugenommen (12 im Berichtsjahr, im Vorjahr 4), was einerseits damit zusammenhängt, dass sich in der täglichen Nutzung von Microsoft-Produkten immer wieder Datenschutzfragen stellen, andererseits wird die von der Verwaltung genutzte Produktepalette aber auch laufend erweitert.

Nach wie vor beschäftigt das Thema Videoüberwachung die FADS in etwa gleichbleibendem Rahmen, während Fragen zur Datenbekanntgabe deutlich zugenommen haben, was mit der zunehmenden Vernetzung der Behörden zu tun haben könnte. Neu aufgeführt wurde das Thema KI. Es ist unterdessen in der Stadtverwaltung angekommen, und die FADS hat sich im Berichtsjahr zeitweise sehr intensiv damit auseinandergesetzt.

Anteile Themenbereiche der im 2025 bearbeiteten Fälle



* Verträge mit Auftragsdatenbearbeiterinnen

7

Einblick in die Praxis

Die FADS hat sich im Berichtsjahr mit einem bunten Strauss an Themen auseinandergesetzt. Nachdem im vorgehenden Kapitel die Statistik behandelt wurde, soll der Einblick in die Praxis exemplarisch zeigen, welche Fälle hinter den Zahlen stecken. Ausgewählt wurden Beispiele, in denen sich typische oder eben gerade aussergewöhnliche Fragen gestellt haben, um damit einen breiten Einblick in den Arbeitsalltag der FADS zu vermitteln. Das Kapitel ist nach Themenbereichen geordnet.

Applikationen

In ihrer täglichen Arbeit setzt sich die FADS am häufigsten mit neuen oder bereits eingesetzten Applikationen auseinander. Einerseits berät sie die Verwaltung bei der Beschaffung oder dem Einsatz von Applikationen, andererseits führt sie dazu Vorabkontrollen und ordentliche Kontrollen durch.

Ordentliche Kontrolle Innosolv

Im Berichtsjahr hat die FADS ihr erstes grosses Kontrollprojekt durchgeführt und dabei das Führen des Einwohnerregisters der Stadt Bern und die dazu eingesetzte Fachapplikation unter die Lupe genommen.

Die Fachapplikation InnosolvCity wurde bereits im Sommer 2020 in Betrieb genommen, damals noch unter dem Namen nest. Im Frühling 2021 wurden der FADS die dazugehörigen ISDS-Unterlagen zur Prüfung eingereicht und in der Folge aufgrund von Rückmeldungen der FADS mehrere Male überarbeitet. Zu Beginn des Jahres 2023 erhielt die FADS die finalisierten Dokumente zur unterdessen in InnosolvCity (nachfolgend «Innosolv») unbenannten Anwendung zur Vorabkontrolle.

Im letztjährigen Tätigkeitsbericht hat die FADS darauf hingewiesen, dass die Vorabkontrolle, welche eine rein dokumentenbasierte Überprüfung des Soll-Zustands einer geplanten Datenbearbeitung ist, für die Prüfung bereits laufender Applikationen nicht das geeignete Instrument darstellt. Der mit der Vorabkontrolle verbundene Hauptzweck besteht darin, datenschutzrechtliche Mängel einer Datenbearbeitung bereits im Planungsstadium zu erkennen und zu beseitigen, was nach deren Beginn nicht mehr mög-

lich ist. Daher ist es bei bereits laufenden Applikationen angezeigt, den Ist-Zustand, d.h. die tatsächlich durchgeführte Datenbearbeitung, im Rahmen einer ordentlichen Kontrolle zu überprüfen (zum Ganzen Tätigkeitsbericht 2024 S. 12 f.).

«Ordentliche Kontrolle statt Vorabkontrolle bei bereits laufenden Applikationen»

Die FADS beschloss daher, bei der bereits während mehreren Jahren betriebenen Applikation Innosolv keine Vorabkontrolle mehr durchzuführen. Da das Führen des Einwohnerregisters jedoch das Herzstück der städtischen Einwohnerdatenbearbeitung darstellt und die Einhaltung der datenschutzrechtlichen Vorgaben dabei zentral ist, entschied sich die FADS, die mit Innosolv durchgeführten Datenbearbeitungen einer ordentlichen Kontrolle zu unterziehen: Als Basis der Prüfung dienen zwar auch hier die ISDS-Dokumentation sowie weitere, betriebsrelevante Dokumente (bspw. das Betriebskonzept). Jedoch werden bei der ordentlichen Kontrolle die tatsächlichen Begebenheiten und Sachverhalte vor Ort begutachtet.

Dies wurde EMF in der zweiten Jahreshälfte 2024 mitgeteilt und das folgende weitere Vorgehen aufgezeigt: Die FADS prüft, ob die Applikation wie in den Konzepten geplant betrieben wird. Dabei wird zuerst der relevante Sachverhalt durch die FADS festgestellt, wobei EMF die Gelegenheit erhält, sich zur Sachverhaltsfeststellung zu äussern. Gestützt auf diesen bereinigten Sachverhalt erfolgt anschliessend eine Beurteilung durch die FADS, nötigenfalls verbunden mit Empfehlungen zu Anpassungen der durchgeführten Datenbearbeitungen. Für die Kontrolle legte sie aufgrund der bereits geprüften ISDS-Unterlagen die Prüfungsschwerpunkte Zugriffsberechtigungen, Rechtsgrundlagen, Schnittstellen, Umsetzung der Massnahmen aus der Risikoanalyse und die fachlichen Prozesse bei EMF fest.

Bereits im Vorfeld hatte sich gezeigt, dass das Thema Direktzugriffe durch städtische Behörden auf Innosolv diverse Fragen aufwarf. So ging aus den zur ursprünglichen Vorabkontrolle eingereichten Unterlagen nicht abschliessend hervor, über welche Zugriffsrechte die einzelnen Verwaltungseinheiten der Stadt verfügen. Auch die formellgesetzliche Grundlage resp. die zwingende Erforderlichkeit zur Aufgabenerfüllung für über das Basisprofil hinausgehenden Zugriffsrechten war nicht vollständig erstellt. Die Vergabe der Zugriffsberechtigungen nach dem need-to-know-Prinzip war damit nicht sichergestellt.

Da die korrekte Vergabe von Direktzugriffsrechten an städtische Behörden ein zentrales Element einer datenschutzkonformen Einwohnerdatenbearbeitung ist, entschied sich die FADS dazu, diese Frage mit EMF vorab gesondert zu behandeln. Eine dazu geführte Besprechung zu Beginn des Berichtsjahres ergab zu diesem Punkt dringenden Handlungsbedarf, und EMF begann mit den notwendigen Bereinigungsarbeiten sofort.

Im weiteren Verlauf des Kontrollprojektes zeigte sich, dass eine derart umfassende Kontrolle für alle Beteiligten herausfordernd sein kann. Die FADS als Kleinstbehörde muss einen grossen Teil ihrer Ressourcen darin investieren, so dass eine gute Planung und eine vorausschauende Koordination mit ihren anderen Aufgaben unabdingbar sind. Aber auch die geprüfte Behörde muss sicherstellen,

dass die relevanten Personen verfügbar sind und die Prüffragen auch beantworten können. Daher wurden die weiteren Prüfschwerpunkte in drei Prüfblöcke aufgeteilt und die jeweils zu den Prüfblöcken gehörigen Prüffragen EMF bereits anfangs Jahr zur Vorbereitung zugestellt. Dies ermöglichte in der zweiten Jahreshälfte eine effiziente Durchführung der Kontrolltermine vor Ort. Der Sachverhalt konnte auf diese Weise bis zum Ende des Berichtsjahres festgestellt und mit EMF bereinigt werden. Die Beurteilung und der Abschluss der Kontrolle sind für den Beginn des Folgejahres geplant.

«Einwohnerregister als Herzstück der städtischen Einwohnerdatenbearbeitung»

Vorabkontrolle SAP SuccessFactors Modul Recruiting

Die Fachapplikation für den Personalgewinnungsprozess wurde der FADS zur Vorabkontrolle eingereicht. Nachdem die grundlegenden Fragen geklärt werden konnten, wurde die Applikation mit dem Einverständnis der FADS vor dem vollständigen Abschluss der Vorabkontrolle aufgeschaltet.

Im August des Berichtsjahres wurden der FADS die ISDS-Dokumente für die geplante Applikation SAP SuccessFactors Modul Recruiting (im Folgenden «SAP SF Recruiting») zur Vorabkontrolle eingereicht. SAP SF Recruiting soll künftig als Fachapplikation bei der Personalgewinnung in der Stadt Bern eingesetzt werden. Unter anderem sollen damit die Bewerbungsdossiers von Bewerber*innen bewirtschaftet werden, womit nicht ausgeschlossen werden kann, dass auch besonders schützenswerte Personendaten bearbeitet werden. Entsprechend diesem potentiell erhöhten Schutzbedarf der bearbeiteten Daten gelten erhöhte Anforderungen, insbesondere im Bereich Datensicherheit.

Die erste summarische Prüfung durch die FADS ergab, dass die ISDS-Dokumente noch nicht vollständig sind und diverser Nachbesserungen bedürfen. Obschon in der Folge die verlangten Dokumente umgehend nachgereicht wurden und mehrere Besprechungen zwischen der FADS und dem Programm stattfanden, schritten die Verbesserungsarbeiten nur langsam voran. Am 22. September 2025 kontaktierte die FADS daher die Programmleitung, da sie aufgrund der nur langsam fortschreitenden Verbesserungsarbeiten und einiger nach wie vor ungeklärter, sehr grundlegender Fragen bezweifelte, dass der geplante Termin für die Aufschaltung der Applikation eingehalten werden kann. So musste z.B. geklärt werden, wie damit umzugehen ist, dass mit SAP SF Recruiting möglicherweise dem US-Cloud Act unterstehende Bearbeitungen von besonders schützenswerten Personendaten der Stadt Bern vorgenommen werden. Damit rückte die Frage, wie diese Daten verschlüsselt werden und wer Kenntnis vom verwendeten Schlüssel hat, in den Vordergrund.

In der Folge intensivierte das Programm die Arbeiten an den ISDS-Dokumenten. Zudem wurde vereinbart, die zentrale Frage des Schlüsselmanagements vorab separat zu behandeln. Dazu fand u.a. eine Besprechung mit Vertreter*innen von SAP unter Beteiligung der FADS statt, in der einige wesentliche Punkte geklärt werden konnten.

Am 13. Oktober 2025 konnte die FADS feststellen, dass die wichtigsten von ihr

verorteten Befunde so weit bereinigt worden sind, dass die Aufschaltung trotz noch nicht vollständig abgeschlossener Vorabkontrolle vertretbar ist. Die Applikation wurde daraufhin, wie geplant, am 16. Oktober 2025 in Betrieb genommen.

Anschliessend fanden weitere Besprechungen zur Bereinigung der noch bestehenden Mängel statt, und die Dokumentation wurde noch einmal überarbeitet, bevor der FADS am 6. November 2025 eine weitere Version unterbreitet wurden. Nachdem die letzten Befunde der FADS kurz vor Weihnachten besprochen werden konnte, wird die Vorabkontrolle zu Beginn des nächsten Jahres abgeschlossen werden können.

Beratung Data Hosting bei Fachapplikation für Arbeitszeugnisse

Im Rahmen der Beschaffung einer neuen Applikation zur Erstellung von Arbeitszeugnissen wurde für die Datenhaltung auf die Azure Cloud von Microsoft gesetzt. Nach Intervention der FADS entschied sich das Projekt, für das Hosting auf die Infrastruktur einer Schweizer Anbieterin zu wechseln.

Im Berichtsjahr wurde die FADS von der ICT-Sicherheit in Zusammenhang mit den datenschutzrechtlichen Anforderungen an das Datenhosting der neu zu beschaffenden Fachapplikation für das Erstellen von Arbeitszeugnissen kontaktiert. Das Projekt hatte sich für eine Lösung einer Schweizer Anbieterin entschieden, welche für die Datenhaltung jedoch die Azure Cloud von Microsoft nutzt.

Wie in Kapitel 5 vorstehend ausgeführt, kann eine solche Lösung mit dem Risikoübernahmeentscheid des Gemeinderates zu M365 in Konflikt stehen, wenn damit besonders schützenswerte Personendaten bearbeitet werden und der Zugriff durch Microsoft auf Klardaten nicht technisch unterbunden ist. So auch im vorliegenden Fall: Die geforderte technische Unterbindung des Zugriffes durch Microsoft auf Klardaten der Stadt war gemäss den der FADS bekannten Informationen nicht sichergestellt. Daher kontaktierte die FADS die Projektverantwortlichen für eine Besprechung des Schlüsselmanagements und der Zugriffsmöglichkeit von Microsoft auf die Daten der Stadt.

An dieser Besprechung, an welcher auch Vertreter*innen der Herstellerfirma teilnahmen, zeigte sich, dass sich das Projekt unter anderem wegen der Kompatibilität mit der bereits verwendeten Microsoft Produktepalette für die Datenhaltung in der Azure Cloud von Microsoft entschieden hatte. Die von der Herstellerfirma ebenfalls angebotene lokale Datenhaltung im Rechenzentrum der Stadt oder in der Cloud einer Schweizer Anbieterin wurde daher vom Projekt nicht mehr weiter geprüft.

«Nach Intervention der FADS fand der Wechsel zu einem CH-Provider statt»

Nach der Besprechung mit der FADS nahm das Projekt jedoch weitere Abklärungen vor und entschied sich anschliessend, auf die Datenhaltung in der Microsoft Azure Cloud zu verzichten und die Fachapplikation auf der Infrastruktur der Schweizer Anbieterin zu betreiben. Die FADS begrüsst diesen Schritt. So werden die datenschutzrechtlichen Risiken vermieden, die bei der Nutzung von Dienstleistungen von

US-Hyperscalern anfallen, womit auch die Governance der Stadt zur Bearbeitung von besonders schützenswerten Personendaten in Fachapplikationen eingehalten ist.

Vorabkontrolle KitAjour

Die Applikation KitAjour, die bis anhin zur Administration im Kita-Büro eingesetzt wurde, soll neu für Kita-Mitarbeitende zur Verfügung gestellt werden, um via Tablet im Kitaalltag Informationen abzufragen und Abläufe zu dokumentieren. Die dazu aktualisierten ISDS-Unterlagen wurden der FADS im Berichtsjahr zur Vorabkontrolle eingereicht.

KitAjour steht für die Administration der Kitas im Kita-Büro bei Familie Quartier Stadt Bern (FQSB) bereits im Einsatz. Neu soll die Datenbearbeitung über Zugriffe mit Tablets auch vor Ort in den Kitas möglich sein. Im Zentrum stehen dabei die Erstellung eines Tagesplanes oder der Abruf von Informationen zu Gesundheit (Krankheiten, Allergien, notwendige Medikamente) und Ernährungsbedürfnissen der Kinder durch Kita-Mitarbeitende sowie die Einführung einer Journalführung pro Kind, in der zwecks Information von Erziehungsberechtigten Beobachtungen und Informationen aus dem Alltag und dem Befinden des Kindes festgehalten werden sollen.

Die FADS führte zu KitAjour bereits im Jahr 2023 eine Vorabkontrolle durch. Die damalige Prüfung der ISDS-Dokumente ergab zahlreiche Befunde. FQSB hat die ISDS-Unterlagen unterdessen überarbeitet und mit den geplanten neuen Anwendungen erweitert. Der Produktivbetrieb der erweiterten Datenbearbeitung durch die Kita-Mitarbeitenden wurde korrekterweise noch nicht aufgenommen. Die Sichtung der aktualisierten ISDS-Unterlagen ergab, dass von den ursprünglich 34 Befunden 22 erledigt wurden. So ist jetzt in den Dokumenten beispielsweise beschrieben, dass Beobachtungen und Informationen aus dem Alltag und dem Befinden des Kindes nach 3 Monaten nicht mehr benötigt und somit gelöscht werden. Auch wurde die Datenbearbeitung aufgrund von Use Cases transparent beschrieben.

Die weiterhin offenen Fragen zu Benutzerberechtigungen nach Need-to-Know und zu anonymisierten Datenfelder konnten in einem direkten Austausch mit dem Applikationsverantwortlichen geklärt werden und wird im ISDS-Konzept noch ergänzt. Darüber hinaus ist die bereits bestehende Weisung zur Nutzung von KitAjour mit Vorgaben für den Umgang mit Tablets zu erweitern. Dies ist wichtig, um ein Datenabflusses in die iCloud zu verhindern und die lokale Datenbearbeitung auf dem Tablet einzugrenzen. Die aktualisierten Dokumente wurden der FADS im Berichtsjahr noch nicht eingereicht.

Review ISDS Unterlagen MS Power Platform

Der Service Microsoft Power Platform zur Automatisierung von Geschäftsabläufen und Datenanalyse soll in der Stadt Bern genutzt werden können. Da dieser Dienst nicht Teil des ISDS M365 war, wurde im Berichtsjahr ein eingeständiges ISDS-Konzept erstellt und der FADS mit Bitte um ein Review zugestellt.

Zur Microsoft Power Plattform wurden ISDS-Dokumente erstellt. Dies war notwendig, da der Dienst zur Automatisierung von Geschäftsabläufen und zur Datenanalyse nicht Teil des ISDS von M365 war und somit auch nicht von der Vorabkontrolle M365 abgedeckt ist. Daher wurde in Abstimmung mit den Projekt-

verantwortlichen entschieden, einen Anhang zum ISDS M365 zu verfassen, welcher im Berichtsjahr der FADS mit Bitte um ein Review zugestellt wurde.

In der Applikation wird unterschieden zwischen der «Personal Productivity»- und der «Business Productivity»-Umgebung. In ersterer können Nutzende anhand ihrer persönlichen Daten Analysen und Prozesse erstellen, die nach ihrem Austritt gelöscht werden. Die Business-Umgebung dient der Erstellung von Analysen und Prozessen auf Team- und Abteilungsstufe anhand von M365-Daten. Beide Umgebungen verfügen über keine Konnektoren zu externen Datenbeständen, weshalb die Projektverantwortlichen zum Schluss gekommen sind, dass die Power Platform ein geschlossenes System in der M365-Umgebung darstelle. Daraus folgerten sie, dass die Einführung der Power Platform zu keinen neuen Risiken führe und die damals bei der Einführung von M365 gemachte Risikobetrachtung ausreichend sei.

Dieser Haltung widersprach die FADS. Sie zeigte auf, dass nebst der potenziellen Umgehung von Zugriffsrechten durch neue Datenverknüpfungen auch die Bearbeitung von Nutzungsdaten durch Microsoft für eigene Zwecke sowie der verschärfte Lock-In aufgrund der höheren Abhängigkeit von Microsoft und der sich daraus ergebende Einfluss auf die Exit-Strategie als neue resp. neu zu beurteilende Risiken zu behandeln sind.

Nebst der Thematik der fehlenden Risikoanalyse für die Power Platform bemängelte die FADS vorab das fehlende Benutzerberechtigungskonzept, in dem die spezifischen Rollen Administration, Entwickler, Designer und Nutzer und deren Belegung pro Umgebung beschrieben werden sollten. Auch die Umsetzung der Konfigurationsempfehlung des Center for Information Security (sog. CIS-Benchmarks) für die Power Platform sollten analog zu denjenigen von M365 dokumentiert werden, wobei nicht umgesetzte Empfehlungen als Restrisiko in der Risikoanalyse zu führen sind.

Diese und weitere Punkte wurden in einem Austausch mit den Verantwortlichen erörtert, und es wurde vereinbart, das ISDS-Konzept entsprechend anzupassen, eine Risikoanalyse für die Power Platform zu erstellen und der FADS zur ordentlichen Vorabkontrolle einzureichen.

Schutzbedarfsermittlung bei neuen Applikationen

Im Berichtsjahr hat die FADS insgesamt 19 Schutzbedarfsanalysen einem Review unterzogen und dabei nebst der Beurteilung des ausgewiesenen Schutzbedarfes auch beratend Hinweise zu einem datenschutzkonformen Vorgehen im weiteren Projektverlauf gegeben.

Schutzbedarfsermittlung in der Stadt Bern

Für jedes Informatikvorhaben in der Stadt Bern ist als erster Schritt im Security Compliance Check der ICT-Sicherheit die Erstellung einer Schutzbedarfsanalyse vorgeschrieben. Bei einer Cloudlösung muss zudem die Dokumentation der Einhaltung der Weisung Cloud Computing durch den Cloud-Provider ausgefüllt werden.

Der Schutzbedarf des geplanten Vorhabens wird aus Sicht Informationssicherheit und Datenschutz durch die Projektverantwortlichen dokumentiert

und durch Informatik-Koordinierende sowie die ICT-Sicherheit geprüft.

«Bei erhöhtem Schutzbedarf sind zwingend ISDS-Dokumente zu erstellen»

Bei einem erhöhten Schutzbedarf sind zwingend ISDS-Dokumente zu erstellen und der FADS zur Prüfung der Vorabkontrollpflicht nach Art. 17a KDSG einzureichen. Die FADS kann auch bereits im Vorfeld zur Vorabkontrolle zu spezifischen datenschutzrechtlichen Fragestellungen kontaktiert werden. Im Berichtsjahr wurden der FADS gesamthaft 19 Schutzbedarfsanalysen zum Review unterbreitet. So konnten die Aspekte des Datenschutzes zu einem frühen Zeitpunkt ins Projekt eingebracht werden. Wie die im Folgenden erläuterten Beispiele aufzeigen, ist dies für eine datenschutzkonforme Einführung von Applikationen oftmals von grosser Wichtigkeit.

Schutzbedarfsermittlung im Bereich M365

Die in der Stadt eingesetzte Palette an Microsoft-Produkten wird laufend erweitert. Die FADS hat bei der Ermittlung des Schutzbedarfs der damit bearbeiteten Daten beratend unterstützt.

Nach der Einführung vom M365 in der Stadtverwaltung wurden auch Tools für die Datenmigration in die MS-Cloudumgebung eingeführt. Dazu zählten die Applikationen TreeSize zur Ermittlung von Ordner- und Dateigrössen und ShareGate zur Migration von Daten von On-Premises-Fileservern im Rechenzentrum der Stadt Bern in die MS-Cloudspeicherlösung OneDrive. Hier war von grosser Bedeutung, dass nicht – wie ursprünglich geplant – auch vertraulich klassifizierte Dokumente automatisiert auf OneDrive migriert werden. Nach einer Besprechung mit den Verantwortlichen wurde der Migrationsprozess entsprechend angepasst, so dass keine vertraulichen und geheimen Dokumente über den ShareGate in die MS-Cloud migriert werden.

Auch bei den Schutzbedarfsanalysen zur MS Power Platform war die Datenbearbeitung in M365 ein Thema. Die ursprüngliche Schutzbedarfsanalyse zur Power Platform ging von einem normalen Schutzbedarf aus, obwohl grundsätzlich die Bearbeitung aller Daten in der M365-Umgebung geplant war. Auch wurde die alte Vorlage benutzt (vgl. Tätigkeitsbericht 2024 S. 9 ff.), so dass der Einsatz von Technologien mit erhöhten Risiken für die betroffenen Personen nicht abgehandelt wurde. Daher stellte die FADS die Ermittlung des Schutzbedarfs in Frage. In der Folgen wurden doch noch ISDS-Dokumente erstellt, in denen die offenen Punkte beschrieben wurden. Deren Review wird in diesem Bericht separat beschrieben (siehe S. 25. vorstehend).

«Keine Scan-to-Folder-Funktionen auf OneDrive»

Die Datenbearbeitung in M365 war auch bei der Ermittlung des Schutzbedarfes zu den neuen Multifunktionsgeräten ein wichtiges Thema. Vom Projekt war geplant, die Funktion Scan-to-Folder von einem lokalen Abteilungslaufwerk im Rechenzen-

trum der Stadt Bern auf das persönliche OneDrive-Verzeichnis in der MS-Cloud zu verlagern. Da mit der Scan-Funktion auch vertrauliche Dokumente mit besonders schützenswerten Personendaten bearbeitet werden, intervenierte die FADS. An einer Besprechung mit den Projektverantwortlichen wurde auf die Problematik aufmerksam gemacht, und die FADS setzte sich dafür ein, stattdessen bereits bestehende lokale persönliche Laufwerke zu nutzen. Eine neue Schutzbedarfsanalyse oder finale ISDS-Dokumente wurden im Berichtsjahr noch nicht eingereicht.

Schutzbedarfsermittlung bei Call-Center-Lösungen

Der Projektleiter von Informatik Stadt Bern kontaktierte die FADS mit der Bitte um ein Review der beiden Schutzbedarfsanalysen sowie der Deklarationen der Einhaltung der Weisung Cloud Computing zu zwei Call-Center-Lösungen, die beide auf MS Teams basieren. Die Dokumente wurden von der Projektleitung als Grundlage für den Beschaffungsentscheid erarbeitet.

Nach einer ersten Sichtung der Dokumente kam die FADS zur Auffassung, dass noch nicht abschliessend beurteilt werden kann, ob der Schutzbedarf korrekt ermittelt wurde oder nicht. Dies, weil in der Analyse bei den bearbeitenden Personendaten nur die Kategorien «Call Detail Records» und «Benutzerdetails» genannt, nicht aber die konkret bearbeiteten Personendaten aufgelistet wurden. Daher war unklar, ob auch besonders schützenswerte Personendaten mit den Call Center-Lösungen bearbeiten werden. Denkbar wäre dies zum Beispiel bei Sprachnachrichten, die, je nach Kontext, sensible Personendaten enthalten können. Zur Selbstdeklaration WCC konnte festgehalten werden, dass eine der geprüften Lösungen zahlreiche Anforderungen aus der Weisung Cloud Computing nicht oder noch nicht erfüllt.

Nach Überarbeitung der Schutzbedarfsanalysen durch die Verantwortlichen und der detaillierten Beschreibung der bearbeiteten Personendaten wurde klar, dass auf die Aufzeichnung von Telefonaten und Sprachnachrichten verzichtet wird und lediglich Kontakt- und Organisationsdaten sowie die Metadaten Datum, Dauer, Uhrzeit, Teilnehmer und Service von Gesprächen bearbeitet werden. Daher beurteilte die FADS den als normal ausgewiesenen Schutzbedarf als korrekt.

«Erfüllung WCC-Anforderungen als massgebendes Auswahlkriterium»

Nach diesen Rückmeldungen der FADS entschied sich das Projekt diejenige Lösung weiterzuverfolgen, die gemessen an den WCC-Anforderungen den städtischen Vorgaben zur Einführung von Cloudlösungen besser entspricht und zu voraussichtlich weniger Restrisiken in der Nutzung führt.

Schutzbedarfsermittlung bei Personenzählsystem

Das Sportamt reichte im Berichtsjahr die Schutzbedarfsanalyse für ein Personenzählsystem in städtischen Sport- und Freizeitanlagen mit der Bitte um ein Review ein.

Die in der Schutzbedarfsanalyse beschriebene Unkenntlichmachung von Personen direkt auf der Hardware wurde zu wenig

beschrieben, um einen Personenbezug ausschliessen zu können. Aufgrund dieser Rückmeldung fand eine Besprechung mit Vertretern der Herstellerfirma statt, an der sich die FADS versichern konnte, dass ein Personenbezug nahezu ausgeschlossen werden kann. Die Sensoren erfassen 3D-Livebilder von oben mit einer Frequenz von 12Hz (also 12 Bilder pro Sekunde). Aus den erfassten Bildern werden direkt auf der Kamera im Arbeitsspeicher die Anzahl Personen ermittelt, die eine Zähllinie überschreiten. Danach (nach 1/12 Sekunden) werden die Bilder aus dem RAM gelöscht. Zusätzlich konnte dargelegt werden, dass die Bilder in keiner hohen Auflösung aufgenommen werden.

Daraus schloss die FADS, dass mit dem Personenzählsystem keine Bearbeitung von Personendaten einhergeht und somit das kantonale Datenschutzgesetzt keine Anwendung findet. Das Sportamt wurde jedoch darauf hingewiesen, dass die Deklaration zur Einhaltung der Weisung Cloud Computing auszufüllen ist, da die Zähldaten in der Google-Cloud gehalten werden.

«Keine Bearbeitung von Personendaten durch das Personenzählsystem»

Schutzbedarfsermittlung bei Applikation in der Denkmalpflege

Die Denkmalpflege hat im Berichtsjahr ein Projekt gestartet zur Einführung einer Applikation für die digitale Verwaltung des Bauinventars. Die dazugehörige Schutzbedarfsanalyse wurde der FADS durch die ICT-Sicherheit mit Bitte um ein Review zugestellt.

Die Applikation besteht aus einem Modul zur Verwaltung von Adressdaten, des Bauinventars und von Subventionen. Den als normal ermittelten Schutzbedarf erachtete die FADS als grundsätzlich korrekt. In der Analyse wurde jedoch offengelassen, ob in der Fachapplikation auch Adressdaten von sensitiven Objekten, wie beispielsweise von Frauenhäusern, bearbeitet werden oder nicht. Solche Informationen wären zumindest als vertraulich zu klassifizieren, womit der Schutzbedarf erhöht werden müsste.

In der ebenfalls eingereichten Deklaration zur Einhaltung der Weisung Cloud Computing waren ausserdem alle Punkte als erfüllt ausgewiesen. Da es sich um eine SaaS-Lösung mit Datenhaltung in der Amazon-Cloud handelte, teile die FADS diese Einschätzung nicht (vgl. Kapitel 5 vorstehend). Auch fehlten der Applikation die geforderte Authentifizierung mit einem zweiten Faktor oder eine Verschlüsselung der ruhenden Daten auf Datenbankebene. Diese Punkte wurden der ICT-Sicherheit zurückgemeldet.

Schutzbedarfsermittlung bei der Jugend-Job-Börse

Bezüglich der Schutzbedarfsanalyse des Vermittlungstools der Jugend-Job-Börse war die FADS im Berichtsjahr in Kontakt mit den Projektverantwortlichen von Familie Quartier Stadt Bern (FQSB) und der ICT-Sicherheit. Die Applikation wird von einem Verein betrieben, an dem die Stadt Bern, die Gemeinde Köniz und die reformierten Kirchen Bümpliz und Bethlehem beteiligt sind.

In der Schutzbedarfsanalyse wird die geplante Datenbearbeitung wie folgt beschrieben: Nach Kontaktaufnahme durch jugendliche Jobsuchende wird im Gespräch ein Profil der Jugendlichen erstellt und manuell im Tool hinterlegt. Wenn eine Stelle auf der

Jugend-Job-Börse ausgeschrieben wird, die auf das Profil passt, wird die entsprechende Person kontaktiert. An einer Besprechung mit FQSB wurde bestätigt, dass es sich beim Betrieb der Jugend-Job-Börse als Angebot der offenen Jugendarbeit um eine öffentliche Aufgabe handelt. Somit war das kantonale Datenschutzgesetz anwendbar und die Zuständigkeit der FADS gegeben.

Inhaltlich war von Interesse, welche Daten in dem erfassten Profil der Jugendlichen vorhanden waren. Nach Rückfrage der FADS wurde versichert, dass keine Daten zu Leistungsfähigkeit oder zum Gesundheitszustand der Jugendlichen erfasst und somit auch keine besonders schützenswerten Personendaten bearbeitet würden. Ebenfalls von Interesse war, ob die Zuordnung der Profile der Jugendlichen zu den ausgeschriebenen Stellen automatisiert oder manuell durch Mitglieder des Vereins geschieht.

«Keine Daten zu Leistungsfähigkeit oder zum Gesundheitszustand und daher normaler Schutzbedarf»

Da Zweiteres der Fall ist, erachtete die FADS die Ermittlung eines normalen Schutzbedarfes als korrekt. Weil die Job-Börse jedoch als Cloud-Anwendung betrieben werden soll, müssen die Vorgaben der Weisung Cloud Computing auch dann eingehalten werden, wenn keine besonders schützenswerten Personendaten bearbeitet werden. Die entsprechende Deklaration fehlte in den Unterlagen. Die FADS empfahl den Verantwortlichen, die Unterlagen in diesem Sinne zu ergänzen.

Digitale Umfragen

Die FADS wurde im Berichtsjahr vermehrt mit Projekten und Vorhaben rund um digitale Umfragen konfrontiert. Nebst öffentlichen eMitwirkungen standen dabei vor allem Online-Umfragen im Schulumfeld im Zentrum.

Öffentliche Mitwirkungen bei Stadtgrün Bern

Im Berichtsjahr gelangte Stadtgrün Bern mit dem Anliegen an die FADS, eine bereits in anderem Zusammenhang vorabkontrollierte Applikation auch für eMitwirkungen einzusetzen. Nach einem Austausch mit den Projektbeteiligten wurde das ISDS-Konzept aktualisiert und der FADS zur Sichtung zugestellt.

Für öffentliche Mitwirkungen bei Tiefbau Stadt Bern (TSB) nach Art. 58 Baugesetzt (BauG; BSG 721.0) wurde die Applikation durch die FADS bereits im Jahr 2024 einer Vorabkontrolle unterzogen (siehe Tätigkeitsbericht 2024 S. 26).

Da sich der Einsatzzweck der Applikation bei Stadtgrün Bern (SGB) wie auch beim TSB auf die informelle und formelle Mitwirkung bei Planungs- und Bauprojekten im öffentlichen Raum beschränkt, beurteilte die FADS die Erweiterung des Anwenderkreises als keine wesentliche Änderung der bisherigen Datenbearbeitung im Sinne von Art. 17a Abs. 2 des kantonalen Datenschutzgesetzes (KDSG; BSG 152.04). Somit war die mit dem überarbeiteten ISDS-Konzept geplante Datenbearbeitung vom bisherigen Vorabkontrollbericht der FADS nach wie vor abgedeckt, und es war keine erneute Vorabkontrolle notwendig.

Nichtsdestotrotz versicherte sich die FADS anlässlich eines Reviews des ISDS-Konzeptes, dass die Implementation

grundlegender Anforderungen bei einer Erweiterung des Anwenderkreises, wie Mandantentrennung und jeweils eigene Administratorenrollen für SGB und TSB, im ISDS-Konzept berücksichtigt wurden.

Öffentliche Mitwirkungen ZöN

Die öffentliche Mitwirkung ZöN sollte mit dem Umfragetool ArcGIS Survey123 aus dem GIS-Produkteportfolio von Geoinformation Stadt Bern umgesetzt werden. Die FADS wurde zur Prüfung der Vorabkontrollpflicht kontaktiert.

ArcGIS Survey123 ist Teil eines Gesamtpakets GIS, zu dem der ISDS-Prozess durch Geoinformation Stadt Bern (GSB) gerade erst initiiert worden ist. Anlässlich einer Besprechung zwischen den Verantwortlichen und der FADS wurde daher vereinbart, den ISDS-Prozess für das Tool gesondert vom restlichen Gesamtpaket durchzuführen, damit die Vorabkontrolle rechtzeitig vor der geplanten eMitwirkung abgeschlossen werden kann.

Entsprechend wurden für ArcGIS Survey123 spezifische ISDS-Dokumente erstellt und der FADS zur Vorabkontrolle eingereicht. Eine erste Sichtung der ISDS-Dokumente durch die FADS offenbarte einige Mängel, die zusammen mit den Projektbeteiligten besprochen wurden. Dabei konnten wichtige Punkte, wie beispielsweise das Format und die Eindeutigkeit des Einladungslinks für die Teilnahme, der Ort der Datenspeicherung der exportieren Umfrageresultate und deren Pseudonymisierung sowie die Deaktivierung des Teilnahmelinks nach Abschluss der Eingabe durch Mitwirkende, angepasst resp. dokumentiert werden.

Auch wurde die Risikoanalyse ergänzt. Die Vorabkontrolle auf Basis der nochmals überarbeiteten und finalisierten ISDS-Dokumenten förderte 4 Befunde zu Tage, welche das GIS-Gesamtpaket betreffen und die im Rahmen des dazu bereits laufenden ISDS-Prozesses durch GSB angegangen werden müssen. Befunde mit hoher Wesentlichkeit, die einen datenschutzkonformen Betrieb nicht zulassen würden, bestanden keine.

Online-Umfragen im Schulbereich

Die FADS wurde im Berichtsjahr von Verantwortlichen des Schulamtes und Informatik Stadt Bern für einen Austausch zur datenschutzkonformen Nutzung von MS Forms angefragt. Seit der Einführung der Schulinformatikplattform base4kids2 steht auch den städtischen Schulen MS Forms zur Verfügung.

Aufgrund der Tatsache, dass Umfragedaten in der MS-Cloud gehalten werden und Microsoft Zugriff auf das Schlüsselmaterial hat, ist die Bearbeitung von besonders schützenswerten Personendaten wie Gesundheitsdaten, Absenzenmeldungen, Prüfungsergebnisse und Zeugnisse mit MS Forms nicht zulässig. Eine solche Nutzung würde auch dem in den ISDS-Dokumenten zu base4kids2 definierten Ampelsystem der Schulen widersprechen, welches eine Speicherung von besonders schützenswerten Personendaten im MS Cloudspeicher OneDrive untersagt.

Daher hat die FADS darauf hingewirkt, dass von den Verantwortlichen eine Governance dazu erarbeitet wird, wie und für welche Use Cases MS Forms im Schulumfeld eingesetzt werden darf. Folgende wesentliche Eckpunkte hat die FADS dabei den Verantwortlichen mitgeteilt: keine Bearbeitung von besonders

schützenswerten Personendaten, zwingende Erstellung der Umfrage innerhalb des b4k2-Tenants mit einem b4k-Account und eine transparente Datenschutzerklärung für Teilnehmende von Umfragen.

Städtische Projekte

Bei diversen städtischen Projekten hat sich die FADS im Rahmen ihrer Beratung oder Aufsichtstätigkeit mit weit mehr als nur einer einzelnen Applikation auseinandergesetzt. So spielten oft auch Vorgänge in der analogen Welt eine wesentliche Rolle, und es war eine ganzheitliche Betrachtung gefragt.

Mitarbeitenden-Befragung in der Stadt Bern

Die für das Jahr 2026 geplante Befragung der Mitarbeitenden der Stadtverwaltung soll durch eine externe Firma durchgeführt werden. Die FADS unterstütze das Personalamt bei der Ausarbeitung der Ausschreibungsunterlagen und führte zum Erstellen der notwendigen ISDS-Unterlagen Beratungen durch.

Bereits Ende 2024 wurde die FADS von der Bereichsleiterin Betriebliches Gesundheitsmanagement des Personalamtes mit Fragen zu den datenschutzrechtlichen Anforderungen bei der Durchführung einer Mitarbeitendenbefragung in der Stadtverwaltung kontaktiert. Die Befragung, die für das Jahr 2026 geplant ist, soll durch eine beauftragte externe Firma durchgeführt werden. In einem telefonischen Austausch erläuterte die FADS die für ein solches Vorhaben einzuhaltenden allgemeinen Vorgaben des Datenschutzes und besprach das Vorgehen, damit die vorgeschriebene Vorabkontrolle rechtzeitig durchgeführt werden kann.

Ende Januar des Berichtsjahres erhielt die FADS die Ausschreibungsunterlagen für die geplante Auftragserteilung mit der Bitte um Beratung zu den für den Datenschutz relevanten Punkten. Die FADS prüfte die Unterlagen und meldete Mitte Februar den von ihr festgestellten Anpassungsbedarf schriftlich zurück. So machte sie auf die aus dem Risikoübernahmeentscheid des Gemeinderats zu Microsoft 365 (siehe Tätigkeitsbericht 2023 S. 11 ff.) fliessenden Vorgaben für Fachapplikationen aufmerksam, ergänzte die notwendigen technischen Eigenschaften der von der Auftragnehmerin verwendeten Applikation und erklärte, was später alles in einem ISDS-Konzept zu beschreiben ist.

Hauptkritikpunkt war die angedeutete geplante Sekundärnutzung der in der Befragung erhobenen Daten. Den eingereichten Unterlagen war zu entnehmen, dass die Stadt diese Informationen mit Daten aus weiteren Systemen oder mit solchen aus künftigen Befragungen verknüpfen möchte. Die FADS hielt fest, dass die hierzu notwendige formellgesetzliche Grundlage aktuell nicht gegeben ist. Da die angedachten Verknüpfungen erhöhte Risiken für die teilnehmenden Mitarbeitenden bergen, wies sie auch auf die erhöhten Anforderungen, insb. im Bereich Transparenz und Datensicherheit, hin. In einer daraufhin durchgeführten Besprechung legte das Personalamt jedoch dar, dass die Sekundärnutzung ohne Bezug auf einzelne, bestimmbare Personen geplant sei. Entsprechend konnte die FADS zurückmelden, dass dies auch mit den bestehenden Rechtsgrundlagen möglich ist, sofern eine Reidentifikation der Mitarbeiter*innen ausgeschlossen ist.

Das Personalamt führte anschliessend die Beschaffung gestützt auf die überarbeiteten Ausschreibungsunterlagen durch und stellte der FADS anfangs September Entwürfe der für eine Vorabkontrolle notwen-

digen ISDS-Dokumente für ein Review zu. Die Prüfung der FADS ergab, dass insbesondere die Regelung der Zugriffsberechtigungen, der Umgang mit Freitextfeldern, die Deklaration zur Einhaltung der städtischen Weisung Cloud Computing (WCC) und die Risikoanalyse überarbeitet werden müssen. In einer Besprechung erläuterte sie die Resultate ihres Reviews und stellte anschliessend eine Liste mit den von ihr festgestellten Mängeln zu.

«Sekundärnutzung nur ohne Personenbezug zulässig»

Zur Bereinigung dieser Mängelliste fand anfangs November eine weitere Besprechung statt, an der auch Vertreter der Herstellerin der beschafften Applikation teilnahmen. So konnten vor allem einige Punkte technischer Natur geklärt werden. Anlass zu Diskussionen gaben aber die von einer Unterauftragsbearbeiterin verwendeten Server eines US-Hyperscalers. Die beschaffte Applikation könnte damit nicht als für die systematische Bearbeitung von besonders schützenswerten Personendaten geeignete Fachapplikation beurteilt werden, wie sie der Gemeinderat in seinem Risikoentscheid zu Microsoft 365 gefordert hat (siehe Kapitel 5 vorstehend). Die Vertreter der Herstellerin wurden daraufhin beauftragt, zur Klärung der zusätzlichen Fragen zum Datenschutz weitere Angaben zu machen und die Möglichkeiten für die Nutzung anderer Server zu prüfen.

Ende November reichte das Personalamt die unterdessen finalisierten ISDS-Dokumente zur Vorabkontrolle ein. Die Prüfung dieser Unterlagen konnte im Berichtsjahr noch nicht abgeschlossen werden.

Auslagerung des Schulzahnmedizinischen Dienstes

Der Stadtrat beschloss im Berichtsjahr, den bisher durch die Stadt betriebenen Schulzahnmedizinischen Dienst aufzuheben und dessen Aufgaben im Rahmen einer Aufgabenübertragung künftig durch die Zahnmedizinischen Kliniken der Universität Bern erfüllen zu lassen. Die FADS konnte im Vorfeld zu diesem Geschäft Stellung nehmen und unterstütze das federführende BSS danach auch bei der Umsetzung.

Bei der Auslagerung des Schulzahnmedizinischen Dienstes (SZMD) an die Zahnmedizinischen Kliniken der Universität Bern (ZMK) werden auch Patient*innendaten übertragen. Dementsprechend waren bei der Schaffung der für diese Aufgabenübertragung notwendigen rechtlichen Grundlagen auch wichtige datenschutzrechtliche Aspekte zu berücksichtigen. Daher lud das Generalsekretariat BSS die FADS bereits im Vorfeld dazu ein, zum Antrag an den Stadtrat inkl. den dazugehörigen Unterlagen Stellung zu nehmen. Nebst der Übernahme des SZMD sollte das ZMK im Auftrag der Stadt zudem auch die Akten nicht mehr aktiver Patient*innen bis zum Ablauf der gesetzlichen Aufbewahrungsfrist aufbewahren. Das BSS schlug vor, diesen nicht zur eigentlichen Aufgabenübertragung gehörenden Auftrag in einer separaten Vereinbarung zu regeln.

In ihrer Stellungnahme stimmte die FADS dem geplanten Vorgehen, die Aufbewahrung der Daten nicht mehr aktiver Patient*innen in einer separaten Vereinbarung zu regeln, zu und bot für die Erarbeitung dieser Vereinbarung ihre Unterstützung an. Da Patient*innendaten zu den besonders schützenswerten Personendaten gehören, wies die FADS in ihrer Stellungnahme ausserdem darauf hin, dass die neuen Reglementsbestimmun-

gen die Bearbeitung genügend klar regeln müssen, um für die Betroffenen Transparenz darüber zu schaffen, welche Daten zu welchen Zwecken bearbeitet werden.

Nachdem der Stadtrat im Sommer das Geschäft einstimmig gutgeheissen hat, bat das BSS im September die FADS um Unterstützung bei den datenschutzrechtlichen Belangen der Umsetzungsarbeiten. Insbesondere galt es, den Umgang mit den noch vom SZMD angelegten Patient*innenakten korrekt zu regeln, da diese nun vollständig an die ZMK übermittelt werden. Je nach Art des Patient*innenverhältnisses ist bei der Weiterbearbeitung durch ZMK unterschiedlichen datenschutzrechtlichen Anforderungen Rechnung zu tragen:

– Während die ZMK für zahnmedizinische Behandlungen Einsicht in die Akten aktiver Patient*innen benötigt, ist dies für die reine Aufbewahrung inaktiver Akten nicht nötig.
– (Vor)schulpflichtige Personen sind von Gesetzes wegen aktiven Patient*innen, solange keine – ebenfalls zulässige – private Behandlung gewählt wird. Für sie betreffende Akten besteht somit ein Einsichtsrecht der ZMK, sofern keine Widerspruchserklärung vorliegt. Nicht mehr schulpflichtige Personen werden hingegen immer auf privater Basis behandelt, so dass ein aktives Patient*innenverhältnis nicht einfach vermutet werden darf. Dementsprechend müssen sie in eine Einsichtnahme durch die ZMK explizit einwilligen.
– Beide Fälle setzen jedoch voraus, dass die Betroffenen über die geplante Auslagerung an die ZMK in Kenntnis gesetzt werden.

Das BSS schlug daher vor, dass sämtliche Betroffenen mit einem Schreiben über die bevorstehende Auslagerung informiert werden. Während nicht schulpflichtige Patient*innen darum gebeten werden, im Falle einer Weiterbehandlung durch die ZMK die Einwilligung zur Einsicht in die bisherigen Akten des SZMD zu erteilen, werden schulpflichtige Patient*innen (resp. die Erziehungsberechtigten) auf die Widerspruchsmöglichkeit hingewiesen. Die FADS war mit diesem Vorgehen einverstanden. Zur ebenfalls vorgelegten Beschreibung der Grundzüge der Datenübermittlung von SZMD zu ZMK sowie der anschliessenden Bearbeitung durch die ZMK machte sie zudem Vorschläge, wie die Datensicherheit und die Datensparsamkeit mit Blick auf das geplante Vorgehen verbessert werden können.

Im November unterbreitete das GS BSS der FADS schliesslich den Entwurf für den Auftragsbearbeitungsvertrag mit ZMK, welcher die Aufbewahrung der Akten nicht mehr aktiver Patient*innen regelt. Auch hierzu machte die FADS kleinere Verbesserungsvorschläge.

Abschluss Vorabkontrolle der Schulinformatik-Plattform base4kids2

Im bereits im Jahr 2023 begonnen Vorabkontrollverfahren zur Schulinformatik-Plattform base4kids2 hat die FADS zu Beginn des Berichtsjahres einen zweiten Vorabkontrollbericht verfasst. Obschon noch immer Befunde mit hoher Wesentlichkeit bestehen, hat die FADS die Vorabkontrolle abgeschlossen. Sie wird die Datenschutzkonformität im Rahmen einer ordentlichen Kontrolle überprüfen.

Die FADS hat sich bereits zu Beginn des Jahres 2023 ein erstes Mal mit der Vorabkontrolle der Schulinformatik-Plattform base4kids2 beschäftigt, im Oktober 2023 einen ersten Vorabkontrollbericht verfasst und in der Folge diverse Beratungen

durchgeführt. Im November 2024 wurden ihr noch einmal überarbeitete Unterlagen zur erneuten Vorabkontrolle eingereicht (vgl. zum Ganzen Tätigkeitsbericht 2023 S. 11 sowie Tätigkeitsbericht 2024 S. 32).

«Die Bereinigung der festgestellten Mängel wird im Rahmen einer ordentlichen Kontrolle überprüft»

Die Prüfung der FADS ergab in der Folge, dass die eingereichten Unterlagen unvollständig sind und trotz mehrerer Beratungsgespräche auch inhaltliche Mängel mit hoher Wesentlichkeit bestehen. So war z.B. das Nutzer- und Berechtigungskonzept noch immer nicht genügend, die Umsetzung von Best Practices zur sicheren Konfiguration von IT-Systeme wurden nicht ausreichend dargelegt, und das Risikomanagement entsprach nicht den in der Stadt Bern geltenden Anforderungen. Nachdem die Plattform jedoch trotz nicht abgeschlossener Vorabkontrolle und nicht bereinigter grundlegender Fragen bereits seit längerem in Betrieb genommen wurde, beschloss die FADS, die Vorabkontrolle abzuschliessen. Die FADS hielt die bestehenden Mängel in ihrem Abschlussbericht fest und kündigte an, die Bereinigung dieser Mängel im Rahmen einer ordentlichen Kontrolle zu überprüfen.

Videoüberwachung

Auch im Berichtsjahr konnte sich die FADS wieder mit zahlreichen Fragen rund um das Thema Videoüberwachung im Rahmen von Vorabkontrollen und Beratungen befassen. Im Vordergrund standen dabei Videoüberwachungen durch städtische Behörden zum Schutz öffentlicher Gebäude oder Anlagen nach Art. 124 des kantonalen Polizeigesetzes. Solche Videoüberwachungen erfordern nebst der datenschutzrechtlichen Vorabkontrolle durch die FADS ein Rückspracheverfahren bei der Kantonspolizei sowie die Bewilligung des Stadtrats aufgrund des städtischen Videoreglements. Eine weitergehende rechtliche Einordnung der sog. polizeilichen Videoüberwachungen erfolgte im Tätigkeitsbericht 2022 (S. 49/50). Nachstehend wird über einige Videoüberwachungen nach Polizeigesetz, aber auch über andere, atypische Videoüberwachungen berichtet.

Videoüberwachung bei Schutz und Rettung Bern

An den Standorten Murtenstrasse 98 und 111 von Schutz und Rettung Bern (SRB) wurden Videoüberwachungskameras eingesetzt, damit die Einsatzzentrale die Zugangs- und Ausfahrtswege von Sanitätspolizei und Feuerwehr auf Hindernisse oder Gefahren überwacht werden konnten.

Der öffentliche Raum wurde bei der Videoüberwachung teilweise miterfasst. Auf die Anforderungen nach Polizeigesetz aufmerksam geworden, startete SRB das Rückspracheverfahren bei der Kantonspolizei. Diese gelangte mit den eingereichten ISDS-Unterlagen an die FADS zur Durchführung der Vorabkontrolle.

Eine erste Prüfung der Unterlagen warf nebst fehlenden Angaben technischer Art eine grundlegende Frage zur Zuständigkeit auf. Einerseits war SRB als verantwortliche Behörde aufgeführt. Andererseits wurde im Zusammenhang mit den fehlenden Angaben auf die Zuständig-

keit der Kantonspolizei als Betreiberin der betreffenden Videoüberwachung verwiesen. Die Frage war deshalb von Belang, weil die kantonale Datenschutzaufsichtsstelle für die Vorabkontrolle zuständig wäre, wenn die Datenschutzverantwortung für die Anlage bei der Kantonspolizei läge. Die FADS bat SRB daher, die offenen Fragen zu klären und die ISDS-Unterlagen zu überarbeiten.

«Die betreffende Anlage wäre vor Inbetriebnahme vorabkontrollpflichtig gewesen»

Wie sich zeigte, war die Kantonspolizei der Meinung, dass sie die Anlage im Auftrag von SRB betreibe und damit nicht die Datenschutzverantwortung innehabe. Gleichzeitig war sie aus Sicherheitsgründen zunächst nicht bereit, die fehlenden technischen Angaben zu liefern. Die städtische Datenschutzbeauftragte tauschte sich in der Folge mit dem kantonalen Datenschutzbeauftragten aus. Dieser Austausch hatte zur Folge, dass die Kantonspolizei nun einige, aber noch nicht alle erforderlichen Angaben machte. Nach einiger Zeit meldete sich SRB wiederum bei der FADS und teilte mit, dass man zwischenzeitlich nach erfolgter Überprüfung der einzelnen Kameras zur Einsicht gelangt sei, dass für den Einsatzzweck lediglich einige wenige Kameras benötigt werden, welche die Ausfahrtstore der Feuerwehr im Fokus haben und den öffentlichen Raum nicht miterfassen. Der Einsatzbereich dieser Kameras ist zudem nicht öffentlich zugänglich. Alle übrigen Kameras würden abgeschaltet bzw. auf Rat der FADS zurückgebaut.

Bei dieser veränderten Sachlage konnte die FADS feststellen, dass keine polizeiliche und damit auch keine nach städtischem Videoreglement durch den Stadtrat zu bewilligende Videoüberwachung mehr vorlag. Entsprechend zog SRG das Rücksprachebegehren bei der Kantonspolizei zurück. Die FADS wies abschliessend darauf hin, dass die betreffende Anlage vor deren Inbetriebnahme vorabkontrollpflichtig gewesen wäre (Art. 17a Abs. 1 Bst. d KDSG und Art. 7 Abs. 1 Bst. d Datenschutzverordnung). Da die Anlage aber bereits in Betrieb war, fiel eine Vorabkontrolle nicht mehr in Betracht. Die FADS behielt sich die Durchführung einer Kontrolle vor.

Vorabkontrolle Videoüberwachung bei teilbetreutem Wohnangebot

Um auf Gewalt und Sachbeschädigung im teilbetreuten Wohnangebot reagieren zu können, wollte der Betreiberverein den Eingangsbereich aussen und innen mittels Kameras überwachen.

Im teilbetreuten Wohnangebot eines Vereins traten aufgrund unkontrollierter Besucherströme regelmässig Sachbeschädigungen, Gewaltvorfälle und damit verbunden erhebliche Störungen der Nachtruhe auf. Trotz Anwesenheit eines Sicherheitsdienstes gelangten nachts unerwünschte Personen, auch solche mit Hausverbot, ins Haus. Anzeigen wegen Hausfriedensbruch zeigten kaum eine abschreckende Wirkung. Bei der Videoüberwachung sollten nur Aufzeichnungen erfolgen; eine Echtzeitüberwachung mittels Monitoren war nicht vorgesehen. Der öffentliche Raum sollte von der Videoüberwachung nicht miterfasst werden.

Die betreffende Liegenschaft ist nicht öffentlich zugänglich. Der privatrechtliche

Verein betreibt das teilbetreute Wohnangebot gestützt auf einen Leistungsvertrag. Durch die damit verbundene Übertragung einer öffentlichen Aufgabe kommt dem Verein aufgrund von Art. 2 Abs. 6 Bst. b KDSG Behördenstellung zu, und er untersteht damit dem KDSG direkt.

Mangels öffentlicher Zugänglichkeit der Liegenschaft lag hier keine Videoüberwachung zum Schutz eines öffentlichen und allgemein zugänglichen Gebäudes nach Art. 124 Polizeigesetz vor. Rechtsgrundlage für die Videoüberwachung bildete ein überwiegendes Sicherheitsbedürfnis und damit die Erforderlichkeit für die Erfüllung der mit Leistungsvertrag überbundenen gesetzlichen Aufgabe. Unter das städtische Videoreglement fallen ausschliesslich Videoüberwachungen nach Polizeigesetz. Aus diesem Grund musste die geplante Anlage nicht dem Stadtrat zur Bewilligung vorgelegt werden. Insofern handelte es sich um eine atypische Videoüberwachung. Wie bei sämtlichen Bearbeitungen von Personendaten mit Bildaufzeichnungs- und Bearbeitungsgeräten war jedoch die datenschutzrechtliche Vorabkontrolle bei der FADS durchzuführen (Art. 17a Abs. 1 Bst. d KDSG und Art. 7 Abs. 1 Bst. d Datenschutzverordnung).

«Mangels öffentlicher Zugänglichkeit keine Videoüberwachung nach Polizeigesetz»

Die bei der FADS eingereichten ISDS-Unterlagen konnten in zwei Iterationen so bereinigt werden, dass sich die FADS im Rahmen der Vorabkontrolle davon überzeugen konnte, dass die Videoüberwachung datenschutzkonform konzipiert worden war.

Einsatz von Bodycams durch Sicherheitsdienst bei teilbetreutem Wohnangebot

Nach Inbetriebnahme der Videoüberwachungsanlage gelangte der Anbieter des teilbetreuten Wohnangebots mit einem Anliegen des privaten Sicherheitsdienstes an die FADS. Dieser wollte in Nächten, in welchen nur eine mitarbeitende Person eingesetzt wird, diese mit einer Bodycam ausstatten. Als Einsatzgründe wurde eine allgemein deeskalierende Wirkung genannt sowie die Möglichkeit, Rassismusvorwürfen begegnen zu können.

Der Verein wollte wissen, ob die FADS Einwände gegen das Vorhaben habe oder dieses bewilligen könne. Die FADS hielt dazu einmal grundsätzlich fest, dass sie keine Bewilligungsbehörde ist, sondern die Datenschutzkonformität beurteilt. Die Verantwortung für den Datenschutz kommt immer der Behörde selbst, hier dem Verein, zu. Im Unterschied zum Einsatz von Bodycams von Sicherheitsfirmen im privaten Umfeld gelten für den Einsatz im Auftrag des Vereins als Träger einer öffentlichen Aufgabe höhere Anforderungen an den Datenschutz. Die FADS beschied den Verein in der Folge dahingehend, dass im Unterschied zur vorabkontrollierten stationären Videoüberwachungsanlage Bodycams einen erheblich schwereren Eingriff in die Rechte und Freiheiten der betroffenen Personen bewirken. Die Gründe liegen in der Mobilität der Kameras, der Möglichkeit von Tonaufnahmen sowie im Umstand, dass auch Bereiche des öffentlichen Raums erfasst bzw. Personen im öffentlichen Raum gefilmt werden könnten. Aufgrund der Schwere der potentiellen Grundrechtseingriffe wäre für einen Einsatz von Bodycams durch bzw. im Auftrag von Behörden eine ausdrückliche gesetzliche Grundlage erforderlich

(vgl. z.B. Art. 122a Polizeigesetz für den Einsatz bei der Kantonspolizei). Die für die stationäre Videoüberwachung herangezogene Rechtsgrundlage war dafür nicht ausreichend. Anders als beim Einsatz von Bodycams durch Sicherheitsfirmen im privaten Umfeld konnte hier auch nicht ein überwiegendes Interesse als Rechtfertigungsgrund geltend gemacht werden.

Hinzu kam, dass selbst bei Vorhandensein einer genügenden gesetzlichen Grundlage der Einsatz von Bodycams im öffentlichen Raum durch städtische Behörden gestützt auf das städtische Videoreglement zusätzlich durch den Stadtrat zu bewilligen wäre.

Dem Verein wurde geraten, zur Abdeckung des Sicherheitsbedürfnisses mildere Mittel wie z.B. eine Erhöhung der Anzahl des Sicherheitspersonals oder eine Ausweitung der Beleuchtung zu prüfen. Daraufhin untersagte der Verein den Einsatz der Bodycams.

Verwendung Echtzeitüberwachung durch Sicherheitsdienst bei teilbetreutem Wohnangebot

Ebenfalls nach Inbetriebnahme der Videoüberwachungsanlage gelangte der Anbieter des teilbetreuten Wohnangebots mit einer erneuten Anfrage an die FADS. Seitens des beauftragten Sicherheitsdienstes war die Frage aufgeworfen worden, ob es zulässig wäre, den Live-Modus der Videokameras zu aktivieren. Der Sicherheitsdienst wollte sich damit einen besseren Überblick über den Eingangsbereich der Liegenschaft verschaffen.

Die FADS hielt dazu fest, dass im Vergleich zum Gegenstand der seinerzeitigen Vorabkontrolle die nun geplante Echtzeitüberwachung durch die beauftragte Sicherheitsfirma eine wesentliche Erweiterung der Datenbearbeitung im Sinne von Art. 17a Abs. 2 KDSG darstelle. Gemäss dieser Bestimmung sei die betreffende Erweiterung für sich genommen vorabkontrollpflichtig; sie werde durch die bisherige Vorabkontrolle nicht abgedeckt. Der Verein müsste die erweiterte Datenbearbeitung mitsamt den dazugehörigen Sicherheitsmassnahmen im ISDS-Konzept und der darin integrierten Risikoanalyse umfassend beschreiben. Die FADS wies darauf hin, dass darin insbesondere die Erforderlichkeit der Echtzeitüberwachung begründet werden müsste. Zudem müssten die Betriebszeiten der Echtzeitüberwachung auf den Einsatz des Sicherheitsdienstes während der Nacht beschränkt werden; es müsste im Weiteren sichergestellt werden, dass der Bildschirm ausschliesslich für den Sicherheitsdienst einsehbar ist und dass der Sicherheitsdienst keinen Zugang und Zugriff auf den Netzwerkrekorder mit den Bildaufnahmen erhalte. Sodann sei mit den Angestellten der Sicherheitsfirma eine Geheimhaltungsvereinbarung auf der Basis der städtischen Vorlage abzuschliessen. Abschliessend machte die FADS darauf aufmerksam, dass die geplante Echtzeitüberwachung keinesfalls aktiviert werden darf, bevor mit Abschluss der Vorabkontrolle deren Datenschutzkonformität festgestellt werden konnte.

Videoüberwachung durch Verein auf Gemeinschaftsflächen von Familiengärten

Im Rahmen einer Beratungsanfrage des Generalsekretariats TVS wurde die FADS darum gebeten, eine durch einen privaten Verein betriebenen Videoüberwachung zu beurteilen.

Ein Familiengartenverein betrieb eine Videoüberwachung, welche auf die Gemeinschaftsflächen des betreffenden

Familiengartens gerichtet war. Der Verein hatte bereits mehrfach Videoaufnahmen von angeblichen Verstössen gegen die Benutzungsordnung der Gemeinschaftsflächen an Stadtgrün Bern (SGB) gesandt. SGB habe bei diesen Gelegenheiten jeweils darauf hingewiesen, dass die Videoüberwachung nicht zulässig sei und die Aufnahmen nicht gesichtet werden. Gleichzeitig wurde der Rückbau der Anlage verlangt, was jedoch nicht erfolgt war. TVS GS wollte wissen, mit welchen Mitteln gegen diese unzulässige Videoüberwachung vorgegangen werden könne.

Da die Videoüberwachung durch einen privaten Verein betrieben wurde, stellt die FADS fest, dass es sich hier um eine Datenbearbeitung durch Private im Anwendungsbereich des Bundesgesetzes über den Datenschutz handelt. Entsprechend ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) für die Datenschutzaufsicht zuständig. Von der Videoüberwachung Betroffene müssten sich grundsätzlich an den EDÖB wenden oder ihre Rechte auf dem Weg der Zivilklage geltend machen.

«Zuständigkeit EDÖB für private Datenbearbeitungen»

Die FADS riet TVS GS als Eigentümerin und Betreiberin der Stadtgärten, allgemeine verwaltungsrechtliche Instrumente gegen den Einsatz der Videoüberwachung auf ihrem Grund zu prüfen. Parallel dazu trat sie mit dem EDÖB in Kontakt, um allfällige Möglichkeiten zu prüfen, trotz fehlender Aufsichtszuständigkeit z.B. mit einem Abmahnschreiben an den betreffenden Verein zu gelangen. Im Laufe dieser Bemühungen teilte TVS GS der FADS mit, dass aufgrund von erneuten Gesprächen von SGB mit dem Verein erreicht werden konnte, dass dieser die Videoüberwachungsanlage entfernt hatte.

Anfrage Privatperson betreffend Videokamera Kreuzung Inselplatz

Eine Privatperson wandte sich im Zusammenhang mit einer Videokamera an der Kreuzung Inselplatz an die FADS. Die Person war darüber besorgt, dass die betreffende Kamera den Hauseingang in der Nähe miterfassen könnte.

Auf Nachfrage bestätigte die Person, dass die Kamera an der Lichtsignalanlage angebracht ist. Eine Rückfrage bei Tiefbau Stadt Bern ergab, dass wie bei anderen Verkehrsknotenpunkten auch bei der Lichtsignalanlage Inselplatz Videokameras verbaut sind.

«Keine personenbezogene Datenbearbeitung bei Videokameras an Lichtsignalanlagen»

Im Jahr 2023 hatte sich die FADS eingehend mit Videokameras an Lichtsignalanlagen befasst (vgl. Tätigkeitsbericht 2023; S. 20). Die damaligen Abklärungen hatten ergeben, dass die Videokameras an Lichtsignalanlagen ausschliesslich die Identifikation von Fehlerverhalten und Behebung von Störungen an den Lichtsignalanlagen bezwecken. Der Bearbeitungszweck ist nicht personenbezogen; die Kameras werden zudem nur punktuell eingesetzt und es erfolgen keine Aufzeichnungen. Aufgrund einer sehr tiefen Bildauflösung ist die Identifikation von Personen oder

Nummernschildern von Fahrzeugen mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen. Damit stand auch fest, dass es sich um keine durch den Stadtrat bewilligungspflichtige Videoüberwachung nach Polizeigesetz handelt. Dies konnte der Privatperson mitgeteilt werden.

Datenweitergabe an die Kantonspolizei

Im Berichtsjahr hatte die FADS in mehreren Fällen Zulässigkeit, Umfang sowie Art und Weise von Datenweitergaben durch städtische Behörden an die Kantonspolizei zu prüfen. Die Beurteilung erfolgte dabei anhand der Einordnung des konkreten Falls aufgrund von verschiedenen Rechtsgrundlagen. Eingehend geklärt wurde insbesondere der Fall der Sicherstellung von Bildaufnahmen im Rahmen von polizeilichen Ermittlungen bei Videoüberwachungen städtischer Behörden.

Herausgabe von Videoaufnahmen des teilbetreuten Wohnangebots an die Kantonspolizei

Zur Regelung der Zusammenarbeit für die Herausgabe von Videoaufnahmen als Beweismittel war die Kantonspolizei an das teilbetreute Wohnangebot mit einem Musterherausgabeersuchen, einem Merkblatt der Staatsanwaltschaft sowie mit Vorschlägen zum Vorgehen in drei Varianten herangetreten. Diese Unterlagen wurden der FADS zur Prüfung unterbreitet.

Zunächst nahm die FADS davon Kenntnis, dass seit der Einführung der Schweizerischen Strafprozessordnung (StPO) im Jahre 2011 sämtliche Strafbehörden Dritte zur Herausgabe von zu beschlagnahmenden Gegenständen auffordern können (Art. 365 Abs. 3 StPO). Beschlagnahmt werden können nach dem Wortlaut von Art. 263 Abs. 1 Bst. a StPO Gegenstände und Vermögenswerte des Beschuldigten oder Dritter, wenn diese Gegenstände und Vermögenswerte voraussichtlich als Beweismittel gebraucht werden. Darunter fallen ebenfalls Videoaufnahmen von Überwachungskameras. Da es sich bei diesem Herausgabeersuchen noch nicht um eine Zwangsmassnahme handelt, kann es auch durch die Kantonspolizei gestellt werden. Erst im Falle einer Verweigerung der Herausgabe kann der Weg über eine eigentliche Editionsverfügung der Staatsanwaltschaft beschritten werden (Art. 265 Abs. 4 StPO). Das Herausgabeersuchen ist schriftlich und mit einer kurzen Begründung versehen zu stellen. Ausnahmsweise kann das Ersuchen bei Dringlichkeit auch mündlich erfolgen; die schriftliche Bestätigung ist jedoch nachzuholen (Art. 263 Abs. 2 StPO). Die FADS konnte sich davon vergewissern, dass die eingereichten Unterlagen wie auch die Varianten zum konkreten Vorgehen den Vorgaben der StPO entsprechen. Wie diese Vorgaben in der Praxis umgesetzt werden, kann erst im Rahmen einer allfälligen Kontrolle der gesamten Videoüberwachung überprüft werden.

Digitale Parkkarte: Datenbekanntgabe an die Kantonspolizei

Mit der Einführung der digitalen Parkkarte erhält die Kantonspolizei zum Zweck der Kontrolle der Parkierberechtigung beschränkten Zugriff auf die entsprechende Applikation des städtischen Polizeiinspektorats. Die Kantonspolizei wünschte, dass nebst Kontrollschild und Angaben zum Fahrzeug ebenfalls die hinterlegte Telefonnummer zugänglich gemacht werde.

Als Begründung wurde angeführt, dass der oder die Parkkarteninhaber*in informiert werden kann, wenn ein Fahrzeug in einer Parkzone steht, welche temporär anderweitig verwendet wird (z.B. Umzonung infolge eines Anlasses). Die Person würde angerufen, um das Fahrzeug umzuparkieren, damit eine Busse oder gar ein Abschleppen des Fahrzeugs verhindert werden kann. Bisher wurden solche Anfragen von der kontrollierenden Person einzeln an das Polizeiinspektorat gestellt, was entsprechend länger dauerte und auf die Öffnungszeiten des Amts beschränkt war.

«Die Gemeinden sind zur Übermittlung an die Kantonspolizei verpflichtet»

Das Polizeiinspektorat gelangte mit der Frage an die FADS, ob für die zusätzliche Bekanntgabe der Telefonnummer eine Rechtsgrundlage bestehe. Dabei war das Polizeiinspektorat bereits zum Schluss gekommen, dass der geplante Zugriff im sog. Abrufverfahren erfolgen soll, bei welchem im Unterschied zur bisherigen Datenbekanntgabe im Einzelfall nach Art. 10 Abs. 1 KDSG nicht mehr vor jeder Datenbekanntgabe überprüft werden kann, ob die anfragende Behörde berechtigt ist, Zugang zu den betreffenden Daten zu erhalten. Die FADS bestätigte, dass es sich beim geplanten Zugriff auf die Parkkartenapplikation um ein Abrufverfahren handelt. Gleichzeitig wies sie darauf hin, dass dafür aufgrund der damit verbundenen Risiken für die Rechte und Freiheiten der Betroffenen eine ausdrückliche gesetzliche Grundlage erforderlich ist. Eine solche war mit Art. 29 der kantonalen Polizeiverordnung (PolV; BSG 551.111) geschaffen worden. Die Bestimmung verpflichtet die Gemeinden, welche die Parkplatzbewirtschaftung elektronisch betreiben, der Kantonspolizei die für die Kontrolle erforderlichen Daten zu übermitteln. Im Weiteren wird ausdrücklich festgehalten, dass die Kantonspolizei Inhalt und Umfang der zu liefernden Daten festlegt. Die FADS riet zusätzlich dazu, aus Transparenzgründen auf dem Gesuchsformular für die Parkkarte sowie auf der entsprechenden Webseite ausdrücklich auf den Datenbezug durch die Kantonspolizei hinzuweisen.

Weitere Datenbekanntgaben

Ob eine Behörde befugt ist, Personendaten einer anderen Behörde oder Privatpersonen bekannt zu geben, ist eine zentrale Frage im Datenschutz. Die FADS hat sich im Berichtsjahr in einigen Fällen auch mit der Datenbekanntgabe ausserhalb des Polizeibereichs beschäftigt.

Weitergabe Emailadressen aus Klapp für Anmeldung Kinderparlament

Um Zugang zur Plattform für Elternkommunikation zu erhalten, müssen sich die Erziehungsberechtigten mit einer Emailadresse registrieren. Familie & Quartier Stadt Bern bat das Schulamt um Weitergabe dieser Emailadressen, damit bei Anmeldungen für das Kinderparlament geprüft werden kann, ob die Anmeldung vom erziehungsberechtigten Elternteil ausgeht. Das Schulamt gelangte an die FADS mit der Bitte um Beurteilung des Anliegens.

Die FADS stellte zunächst fest, dass die Durchführung des Kinderparlaments eine Aufgabe von Familie & Quartier Stadt Bern (FQSB) gestützt auf das Reglement über die Mitwirkung von Kindern und Jugendlichen (Mitwirkungsreglement, MWR; SSSB 144.1) darstellt. Bei der von FQSB erbetenen Weitergabe der Emailadresse handelte es sich um eine Datenbekanntgabe an Behörden nach Art. 10 KDSG. Nebst den dort genannten Voraussetzungen sind dafür vorab auch die generellen Vorgaben für die Bearbeitung von Personendaten nach Art. 5 ff. KDSG zu beachten.

«Die Mittelung der Mailadressen aller Erziehungsberechtigten ist unverhältnismässig»

Problematisch erschien der FADS, dass FQSB nicht nur die Angaben zu Eltern derjenigen Kinder, welche für das Kinderparlament tatsächlich angemeldet werden, sondern die Mailadressen aller Erziehungsberechtigten gleichsam auf Vorrat mitgeteilt werden sollten. Letztere Angaben wären nach Massgabe von Art. 5 Abs. 3 KDSG für die Aufgabenerfüllung eben gerade nicht notwendig. Hinzu kommt, dass die Mailadressen der Erziehungsberechtigten zum Zweck der Registrierung bei Klapp erhoben wurden. Eine Verwendung durch FQSB zur Prüfung der Rolle als Erziehungsberechtigte bei der Anmeldung für das Kinderparlament würde eine Verletzung des datenschutzrechtlichen Zweckbindungsgebots darstellen (Art. 5 Abs. 2 und 4 KDSG). Schliesslich stellte die FADS in Frage, dass die bei Klapp verwendete Emailadresse ein taugliches Mittel zur Beurteilung der Erziehungsberechtigung darstellt, da einige Eltern verschiedene Emailadressen verwenden und daher für die Anmeldung für das Kinderparlament durchaus eine andere Emailadresse als bei Klapp benutzen könnten. In diesem Fall würde FQSB bei der Prüfung der Anmeldung fälschlicherweise davon ausgehen, dass sie nicht durch eine erziehungsberechtigte Person erfolgt ist. Insofern erschien der FADS auch die Geeignetheit der Datenbearbeitung fraglich (Art. 5 Abs. 3 KDSG).

Nach dem Gesagten erwies sich die von FQSB erbetene Datenweitergabe als nicht zulässig. Als datenschutzkonforme Möglichkeit machte die FADS den Vorschlag, ein zusätzliches Feld im Anmeldeformular zu schaffen, in dem die Anmeldenden angeben müssen, ob sie Erziehungsberechtige des anzumeldenden Kindes sind oder nicht.

Weitergabe Personendaten von Schüler*innen beim Wassersicherheitscheck

Das Schulamt gestaltete die Prozesse für die Anmeldung zum kostenlosen Schwimmunterricht bei nicht bestandenem Wassersicherheitscheck neu und legte diese der FADS zur Beurteilung vor.

Zum Schwimmunterricht in den Volksschulen sieht der Lehrplan 21 vor, dass sich Schüler*innen im Zyklus 2 sicher im Wasser bewegen und schwimmen können. Dazu wird in der Regel in der 4. Klasse ein sog. Wassersicherheitscheck (WSC) durchgeführt. Schüler*innen, welche diesen WSC nicht bestehen, haben die Möglichkeit, sich beim Schwimmklub Bern für einen kostenlosen Wiederholungskurs anzumelden. Es hatte sich gezeigt, dass sich für diese Kurse jeweils auch zahlreiche Kinder anmelden liessen, welche den WSC bestanden hatten und damit nicht zum kostenlosen Kursbesuch berechtigt waren.

Die FADS stellte fest, dass dabei einige Prozessschritte erfolgen, jeweils verbunden mit der Bekanntgabe von Personendaten, deren Erforderlichkeit für die Aufgabenerfüllung hinterfragt werden muss. Dies betraf insbesondere die verschiedenen Datenaustausche zwischen dem Schwimmklub Bern und dem Schulamt zum Zweck der Feststellung, welche Schüler*innen zur kostenlosen Teilnahme an einem Wiederholungskurs berechtigt sind.

Dieser Zweck kann deutlich datensparsamer erreicht werden, wenn bei der Kursanmeldung ein Beleg für die Berechtigung zur kostenlosen Teilnahme mit eingereicht werden muss. So würde es genügen, im Vorfeld der Anmeldungen ausdrücklich darauf hinzuweisen, dass ausschliesslich Schüler*innen, welche den WSC nicht bestanden haben, zur kostenlosten Teilnahme berechtigt sind. Bei der Kursanmeldung wäre dann der Elternbrief, in welchem mitgeteilt wird, dass der WSC nicht bestanden wurde, dem Schwimmklub Bern als Beleg vorzulegen. Zusammenfassend riet die FADS, auf die vorgesehenen gegenseitigen Datenbekanntgaben zwischen Schwimmklub Bern und Schulamt zu verzichten. Dies auch vor dem Hintergrund, dass es sich beim Schwimmklub Bern nicht um eine Behörde, sondern um eine private juristische Person handelt, für welche erhöhte Anforderungen an eine Datenbekanntgabe seitens Schulamt gelten (Art. 11 KDSG).

Datenaustausch Schulorgane mit Sozialdienst, Amt für Erwachsenen- und Kindesschutz und Ärzt*innen

Das Schulamt gelangte an die FADS mit der Frage, unter welchen Voraussetzungen sich Schulleitungen und Lehrpersonen mit Schulsozialarbeiter*innen, mit dem Sozialdienst, mit dem Amt für Erwachsenen- und Kindesschutz sowie mit Ärzt*innen über komplexe Fälle von Schüler*innen austauschen können. Sodann erkundigte sich das Schulamt nach der Rolle des Amtsgeheimnisses.

Dem Schulamt war klar, dass mehrheitlich besonders schützenswerte Personendaten betroffen sind und dass besondere Geheimhaltungspflichten wie das Sozialhilfegeheimnis oder die Schweigepflicht von Fachpersonen im Gesundheitswesen zu beachten sind.

Zum Informationsaustausch zwischen Schulleitung, Lehrperson und Schulsozialarbeit hielt die FADS fest, dass ein solcher aufgrund der spezifischen Datenschutzbestimmung von Art. 73 Abs. 2 Volksschulgesetz (VSG; BSG 432.210) grundsätzlich zulässig ist. Dabei ist jedoch die zwingende Erforderlichkeit der betreffenden Angaben für die Aufgabenerfüllung zu beachten. Ebenfalls vorbehalten bleiben besondere Geheimhaltungspflichten.

«Besondere Geheimhaltungspflichten sind zu beachten»

Bezüglich Informationen von Seiten Sozialdienst an Schulorgane wies die FADS darauf hin, dass diese dem Sozialhilfegeheimnis als besondere Geheimhaltungspflicht unterstehen (Art. 57a Sozialhilfegesetz, SHG; BSG 860.1). Eine Datenbekanntgabe wäre in diesem Kontext nur mit Einwilligung der betroffenen Personen (Art. 57a Abs. 2 Bst. b SHG) zulässig. Ein Verstoss gegen diese Bestimmung könnte als Verletzung des Amtsgeheimnisses strafbar sein (Art. 320 StGB). Für eine Datenbekanntgabe von Schulorganen an den Sozialdienst sind die Datenschutzbestimmun-

gen des SHG anwendbar. Nach Art. 57e Abs. 1 Bst. a SHG besteht eine Auskunftspflicht städtischer Behörden gegenüber dem Sozialdienst. Allerdings müssen diese Angaben einen Bezug zum Vollzug des SHG aufweisen (vgl. Art. 57e Abs. 2 SHG). Gestützt auf Art. 57e Abs. 3 SHG können städtische Behörden dem Sozialdienst von sich aus Informationen zukommen lassen, wenn sie sichere Kenntnis davon haben, dass die von der Meldung betroffenen Personen Sozialhilfe beziehen und die Informationen für die Abklärung der Ansprüche nach diesem Gesetz zwingend erforderlich sind. Informationen, welche nicht für den Vollzug des SHG zwingend erforderlich sind, dürfen Schulorgane daher nur mit Einwilligung der Betroffenen an das Sozialamt weitergeben.

Im Weiteren führte die FADS die gesetzliche Zusammenarbeitspflicht zwischen Erwachsenen- und Kindesschutzbehörden und Schulorganen an (Art. 25 Gesetz über den Kindes- und Erwachsenenschutz, KESG; BSG 213.316). Diese ermöglicht den gegenseitigen Informationsaustausch, wobei auch hier die (zwingende) Erforderlichkeit für die Aufgabenerfüllung zu beachten ist.

Bezüglich Ärzt*innen und medizinische Fachpersonen gilt die gesetzliche Schweigepflicht (Art. 27 Gesundheitsgesetz, GesG, BSG 811.01) als besondere Geheimhaltungspflicht. Ein Verstoss kann als Verletzung des Berufsgeheimnisses strafrechtlich verfolgt werden (Art. 321 StGB). Die Bekanntgabe von Informationen durch Ärzt*innen und medizinische Fachpersonen darf vorliegend daher nur mit Einwilligung der betroffenen Person erfolgen. Bei einer Informationsweitergabe von Schulorganen an Ärzt*innen handelt es sich um eine Datenbekanntgabe an eine private Person, welche sich nach Art. 11 KDSG richtet. Eine gesetzliche Verpflichtung oder Ermächtigung von Schulorganen zur Datenbekanntgabe besteht nicht, weshalb die Einwilligung der betroffenen Person (Erziehungsberechtigte; je nach Alter auch Schüler*in) erforderlich ist (Art. 11 Abs. 1 Bst. b KDSG).

Zur Rolle des Amtsgeheimnisses hielt die FADS schliesslich fest, dass dieses die Weitergabe dienstlich erlangter Informationen durch einzelne Mitarbeitende städtischer Behörden ausserhalb vorgesehener Verfahren und Zuständigkeiten untersagt. Das Amtsgeheimnis steht einer Datenweitergabe unter Behörden aber nicht im Wege, solange diese Weitergabe datenschutzrechtlich zulässig ist.

Datenschutzerklärungen

Der FADS wurden vermehrt Entwürfe von Datenschutzerklärungen zur Prüfung vorgelegt. Diese sollten auf spezifischen Webseiten für besondere städtische Angebote, so z.B. bei der Förderung von Kindern im Vorschulalter oder auch bei Webshops, zur Anwendung kommen.

Datenschutzerklärungen städtischer Behörden

Diverse der bei der FADS eingereichten Datenschutzerklärungen wurden mit Hilfe von Vorlagen für private Webseitenbetreiber erstellt. Datenschutzerklärungen städtischer Behörden müssen jedoch andere Anforderungen erfüllen als solche von privatrechtlichen Akteuren.

Im privatrechtlichen Verkehr im Anwendungsbereich des Bundesgesetzes über den Datenschutz soll eine Datenschutzerklärung die Nutzenden über Art und Umfang der Bearbeitung ihrer Personendaten

informieren, damit sie gestützt darauf die gesetzlich vorgeschriebene Einwilligung als Rechtsgrundlage der betreffenden Datenbearbeitung erteilen können. Städtische Behörden dürfen Personendaten demgegenüber nur bearbeiten, wenn das Gesetz ausdrücklich dazu ermächtigt oder wenn das Bearbeiten der Erfüllung einer gesetzlichen Aufgabe dient (Art. 5 Abs. 1 KDSG). Dies gilt auch für den Umgang mit Personendaten, welche beim Besuch von behördlichen Webseiten anfallen. Auch hier gilt, dass die Behörde Personendaten nur in dem Umfang bearbeiten darf, wie dies zur Aufgabenerfüllung erforderlich ist. Entsprechend kommt einer Datenschutzerklärung bei behördlichen Webseiten nicht derselbe Stellenwert wie im Privatrechtsverkehr zu.

«Für Behörden gilt bei Personendatenbearbeitungen das Legalitätsprinzip»

Vor dem Hintergrund des Transparenzprinzips und des behördlichen Informationsauftrags werden gezielte Angaben für die Benutzenden zum Umgang mit deren Personendaten ausdrücklich begrüsst. Wichtig ist jedoch, dass die entsprechenden Informationen mit der erforderlichen Sorgfalt und Genauigkeit sowie zielgruppengerecht verfasst werden. Im Internet frei verfügbare generische Vorlagen für Datenschutzerklärungen genügen diesen Anforderungen dann nicht, wenn diese nicht in Bezug auf das anwendbare Datenschutzrecht adaptiert und darin nicht die tatsächliche Datenbearbeitung abgebildet wird, welche im Rahmen des Betriebs einer behördlichen Webseite oder eines Services erfolgt. Voraussetzung für eine korrekte Ausfertigung einer Datenschutzerklärung ist, dass der verantwortlichen Behörde bekannt ist, welche Personendaten wie, zu welchem Zweck und durch wen bearbeitet werden und wann diese gelöscht werden; ob eine Bekanntgabe ins Ausland und/oder eine Weitergabe an Dritte zu offengelegten Zwecken erfolgt, etc. Erst wenn alle entsprechenden Informationen vorliegen, kann eine inhaltlich korrekte Datenschutzerklärung erstellt werden. So macht es wenig Sinn, der FADS in einer frühen Projektphase eine unvollständige Datenschutzerklärung als erstes Projektdokument zur Prüfung vorzulegen, wie dies in einem Fall im Berichtsjahr erfolgt ist.

Geoinformation Stadt Bern

Die FADS hat im Berichtsjahr zwei Datenschutzerklärungen von Geoinformation Stadt Bern aus sehr unterschiedlichen Bereichen geprüft.

Die erste Datenschutzerklärung betraf das vom städtischen Wirtschaftsamt gemeinsam mit Geoinformation Stadt Bern (GSB) auf deren Infrastruktur betriebene Online-Tool für das Angebot und für die Suche von Wirtschaftsflächen[5]: Der FADS wurde hier ein bereits in guter Qualität verfasster Entwurf für eine Datenschutzerklärung zur Prüfung vorgelegt. Dazu waren nur wenige inhaltliche Anpassungen und Ergänzungen erforderlich.

Ebenfalls in Zusammenarbeit mit GSB hat das Stadtplanungsamt einen Entwurf für eine Datenschutzerklärung für die bevorstehende öffentlichen Mitwirkung zur Revision der Zonen für öffentliche

5 https://gisapp.bern.ch/portal/apps/experiencebuilder/experience/?id=b20ddae5ee9b42af9f502a6dd262d7ff

Nutzungen (ZöN-Revision) mittels digitaler Mitwirkungsplattform (eMitwirkung) vorgelegt. Da bei der eMitwirkung auch besonders schützenswerte Personendaten, nämlich solche über politische Ansicht, Zugehörigkeit und Betätigung (Art. 3 Abs. 1 Bst. a KDSG) der Teilnehmenden bearbeitet werden, war die Datenschutzerklärung besonders sorgfältig zu verfassen. Art und Weise der Datenbearbeitung, die damit verbundenen Risiken und die dagegen getroffenen Massnahmen waren von den verantwortlichen Behörden dokumentiert und von der FADS im Rahmen einer Vorabkontrolle geprüft worden (siehe S. 31 Öffentliche Mitwirkung ZöN). Entsprechend konnte eine Datenschutzerklärung vorgelegt werden, welche die Teilnehmenden transparent und umfassend über die vorgenommenen Datenbearbeitungen informiert.

Frühförderprogramm Gesundheitsdienst

Wie sich im Rahmen von Beratungsanfragen auch gezeigt hat, können ausreichende Kenntnisse über Art und Umfang der Datenbearbeitung und damit über den erforderlichen Inhalt einer Datenschutzerklärung bei Webangeboten fehlen, weil sie durch einen externen Hoster im Auftrag der Stadt betrieben werden.

Der FADS wurde eine vom externen Hoster erstellte Datenschutzerklärung der Webseite des Frühförderungsprogramms des Gesundheitsdienstes https://primano.ch vorgelegt. Diese war jedoch auf eine durch einen Privaten betriebene Webseite ausgelegt und musste unter Einbezug des Hosters vollständig überarbeitet werden. Zudem wurden dem Gesundheitsdienst Vorschläge für einen datenschutzfreundlicheren Betrieb der Webseite gemacht.

Glasdesign

Einen Sonderfall bilden Webshops städtischer Behörden wie derjenige des Kompetenzzentrums Arbeit mit der Bezeichnung Glasdesign[5]: Hier befindet sich die städtische Behörde in wirtschaftlichem Wettbewerb mit Privaten.

«Im Internet frei verfügbare generische Vorlagen genügen den Anforderungen an eine Datenschutzerklärung für behördliche Webseiten in der Regel nicht»

Damit untersteht die Behörde materiell den Bestimmungen des Bundesgesetzes über den Datenschutz (Art. 4 Abs. 2 Bst. a KDSG) sowie, wegen möglichen Kunden aus dem EU-Raum, ebenfalls der Datenschutz-Grundverordnung der EU. Unter Mitwirkung des Hosting Providers konnte eine entsprechende Datenschutzerklärung erstellt und der FADS zum Review vorgelegt werden. Anpassungsbedarf bestand im Wesentlichen dahingehend, dass die konkret gesammelten Personendaten, die jeweiligen Bearbeitungszwecke sowie die beteiligten Drittanbieter abschliessend und nicht nur «beispielsweise» aufgeführt werden sollten. Das Gleiche galt in Bezug auf die eingesetzten Cookies. Als datenschutzfreundliche Lösung konnte festgestellt werden, dass auf den Einsatz von Analysetools und Tracking verzichtet wurde.

5 https://glasdesignbern.ch/c/shop

Publikation von Bildern

Die FADS beriet im Berichtsjahr wiederholt zur Frage, welche Informationen von städtischen Behörden im Internet publiziert werden dürfen. Sie wies dabei darauf hin, dass insbesondere die Publikation von Bildern zumeist die Einwilligung der abgebildeten Personen voraussetzt.

Posten von Fotos auf dem Instagram-Konto der städtischen Kitas

Eine Kita-Angestellte wandte sich an die FADS mit konkreten Fragen zur Zulässigkeit und den Bedingungen für eine Veröffentlichung von Bildern mit Kindern, Eltern oder Angestellten auf dem Instagramm-Konto der städtischen Kitas.

«Die Einwilligung ist immer dann nötig, wenn eine Person auf dem Bild erkennbar ist»

Die FADS hielt fest, dass Fotos jeweils nur mit der Einwilligung der abgebildeten Personen auf solche Plattformen hochgeladen werden dürfen. Dies gilt nicht nur für städtische Kitas oder andere öffentliche Institutionen, sondern auch für Private, und es wird sogar in den Nutzungsbestimmungen vieler Plattformen auch so festgehalten. Einwilligen müssen alle Personen, die auf den Bildern erkennbar sind; bei Kindern unter 14 Jahren ist die Einwilligung der Erziehungsberechtigten notwendig. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Ist dies der Fall, dürfen keine weiteren Fotos hochgeladen werden, und bereits veröffentlichte Bilder müssen, wenn dies verlangt wird, gelöscht werden.

Für die Einwilligungserklärung gibt es keine Formvorschrift. Um in Streitfall dokumentiert zu sein, empfiehlt die FADS jedoch, sie schriftlich einzuholen.

Die Einwilligung ist immer dann nötig, wenn eine Person auf dem Bild erkennbar ist. Dies kann auch dann der Fall sein, wenn sie nur von hinten abgebildet ist, z.B. aus dem Kontext, aufgrund früherer Bilder oder aufgrund besonderer Charakteristika.

Für den Fall, dass ohne Einwilligung Fotos der Kita-Mitarbeiterin hochgeladen werden, wurde sie auf die Möglichkeit hingewiesen, bei der Kita Widerspruch einzulegen, die Löschung der Bilder zu verlangen und bei Bedarf auch zu untersagen, künftig weitere Bilder von ihr auf die Plattform zu stellen. Die Löschung könne auch dann verlangt werden, wenn zuvor eingewilligt wurde, die Betroffene nun mit der Publikation aber nicht mehr einverstanden ist. Ebenfalls könne die Löschung einzelner, z.B. unvorteilhafter Bilder verlangt werden. Sofern die Kita dem nicht nachkommen sollte, könne bei der FADS eine entsprechende Meldung gemacht werden. Diesfalls würde die FADS mit der Kita Kontakt aufnehmen und die Betroffene bei der Durchsetzung ihrer Rechte unterstützen.

Zustimmung für Verwendung von Bild- und Tonaufnahmen im Kinderparlament

Im Zusammenhang mit der geplanten Möglichkeit zu einer online-Anmeldung für das Kinderparlament hatte Familie & Quartier Stadt Bern die von den Erzie-

hungsberechtigten im Rahmen der Anmeldung einzuholende Einwilligung für die Verwendung der während der Sessionen gemachten Bild- und Tonaufnahmen überarbeitet. Die neuen Texte wurden der FADS zu Beurteilung vorgelegt.

In der überarbeiteten Einwilligungserklärung wurde neu einlässlicher darüber informiert, dass Foto-, Video- und Tonaufnahmen für die Öffentlichkeitsarbeit wie Webseite, soziale Medien, Zeitungen und andere Medien (TV) gemacht werden. Die Einwilligung sollte im Rahmen der Anmeldung zum Kinderparlament erfolgen, damit diese nicht mehrfach vor den einzelnen Sessionen eingeholt werden muss. Direkte Zitate sollten jeweils nur mit Einverständnis der Betroffenen erfolgen. Ebenfalls erwähnt wurde die Möglichkeit, die Einwilligung jederzeit zu widerrufen.

«Die Einwilligung wird künftig explizit eingeholt»

Die FADS begrüsste, dass sie künftig explizit eingeholt werden soll. Sie wies jedoch darauf hin, dass sie nicht mit der Unterschrift zur Anmeldung bzw. mit dem Abschicken des Anmeldeformulars (elektronisch) verknüpft werden darf. So wäre ohne Einwilligung gar keine Anmeldung möglich und die Einwilligung damit nicht freiwillig. Die FADS empfahl daher, eine separate Checkbox mit einer Einwilligungserklärung zu gestalten. Im Weiteren erschien der FADS wesentlich, dass bei der Veröffentlichung von Aufnahmen in Medien keine Namensnennungen von Kindern erfolgen. Die FADS verband ihre Hinweise mit konkreten Formulierungsvorschlägen.

Diverses

Der Datenschutz ist eine Querschnittmaterie. So kommt es, dass sich die FADS in ihrer Tätigkeit mit einer grossen Zahl unterschiedlicher Themen beschäftigt.

Zutritts- und Bezahlsystem Velostationen

Die Stadt Bern möchte für die Velostationen ein automatisiertes Zutritts- und Bezahlsystem testen. Die FADS hat die Abteilung Verkehrsplanung von TVS beim Erstellen der Ausschreibungsunterlagen beraten.

Das Zutrittssystem soll den automatischen und kontrollierten Zugang zu einer Velostation ermöglichen, insbesondere ausserhalb der regulären Öffnungszeiten oder in Stationen ohne Personal. Mit dem Bezahlsystem soll eine Bezahlung entsprechend der Parkdauer möglich werden. In Bern ist bis jetzt noch kein solches Zutritts- und Bezahlsystem im Einsatz. Durch den Pilotbetrieb sollen erste Erfahrungen gesammelt und offene Fragen geklärt werden. Das Projekt beinhaltet die Ausschreibung, die Beschaffung und den Betrieb eines automatisierten Zutritts- und Bezahlsystems.

Von Beginn weg war klar, dass sich die Kund*innen der Velostationen registrieren müssen, damit sie die Velostation nutzen können. Mittels einer App oder dem Swisspass sollen die Türen geöffnet werden, und die Velofahrenden müssen ein- und auschecken, damit die Parkdauer respektive die Kosten bestimmt werden können. Da damit Daten über die Nutzung der Velostation erhoben werden, welche einem Benutzerkonto / einer Person zugeordnet werden können, hat sich die Abteilung Verkehrsplanung von TVS bereits im Sommer 2024 an die

FADS gewandt und um Beratung hinsichtlich den bei der Ausschreibung relevanten Datenschutzaspekten gebeten.

Nach der damals erfolgten telefonischen Beratung wurden der FADS zu Beginn des Berichtsjahres die Ausschreibungsunterlagen zur informellen Prüfung zugeschickt. Die Prüfung der Unterlagen ergab, dass sich der frühzeitige Beizug der FADS gelohnt hat. So waren die wesentlichsten datenschutzrechtlichen Aspekte durch das eingereichte Pflichtenheft bereits abgedeckt, so dass die FADS nur noch wenige kleinere Verbesserungsvorschläge machen musste.

Mobile Mapping

In der Stadt Bern wurde im Jahr 2025 eine neue Mobile-Mapping-Befahrung durchgeführt. Die Anbieterin handelte dabei nicht als Auftragsbearbeiterin der Stadt, sondern führte die Befahrungen als private Datenbearbeiterin durch. Sie musste sich dabei an die Vorgaben des Bundesrechts halten.

Die FADS wurde im Frühling des Berichtsjahres von Geoinformation Stadt Bern (GSB) kontaktiert: 2025 soll im Auftrag der Stadt Bern eine neue Mobile-Mapping-Befahrung durch eine private Anbieterin durchgeführt werden. Ähnlich wie bei Google Street View sollen die Strassen der Stadt dabei mittels 360 Grad Kameras aufgenommen und ein Bilddienst erstellt werden. Die Bildqualität sei deutlich höher als diejenige von öffentlich verfügbaren Anbieterinnen und ermögliche nebst virtuellen Begehungen auch andere Funktionen, wie z.B. Vermessungen von Örtlichkeiten direkt ab den Bildern.

Bereits 2019 wurde von der damaligen Datenschutzaufsicht der Stadt Bern eine Vorabkontrolle zum Mobile Mapping durchgeführt und festgehalten, dass die Befahrung zulässig sei, sofern die Rechtsprechung i.S. Google Streetview beachtet werde, also z.B. die dort gemachten Vorgaben zur vorgängigen Information der Bevölkerung, zum Aufnahmewinkel und zur Anonymisierung. Die dabei gewonnenen Daten dürfen jedoch nicht veröffentlicht, sondern ausschliesslich den Mitarbeitenden der Stadt Bern zur Erfüllung ihrer öffentlichen Aufgaben zur Verfügung gestellt werden. In der Folge wurde von der Anbieterin eine erste Befahrung vorgenommen, und die Bilder wurden anschliessend in einem Bilddienst im Intranet der Stadtverwaltung aufgeschaltet.

Die im Berichtsjahr geplante Befahrung sollte sich in einem vergleichbaren Rahmen bewegen, weshalb sich die Frage stellte, ob eine erneute Vorabkontrolle durch die FADS nötig ist.

«Nutzt die Stadt das Produkt lediglich für Abfragen, ist nicht mehr von einer Auftragsdatenbearbeitung auszugehen»

In der dazu durchgeführten Besprechung wurde klar, dass eine erneute Vorabkontrolle durch die FADS nicht nötig ist. GSB legte dar, dass die konkrete technische Ausgestaltung der Datenbearbeitung, von der Bildaufnahme bis zur Darstellung für städtische Angestellte, nach wie vor unverändert sei. Gewisse Softwareupdates seien erfolgt, der Umfang der Bearbeitung bleibe aber unverändert. Es wurde vereinbart, dass aufgrund neuer Vorgaben in der Stadt gewissen Anpassungen an die vertraglichen Grundlagen mit der Anbieterin erfolgen müssen.

Wie sich in der Folge jedoch zeigte, hat die Anbieterin ihr Geschäftsmodell grundlegend geändert. Die bei den Kamerafahrten erhobenen Daten verbleiben gemäss ihren neuen Vertragsbedingungen in ihrem Eigentum, und die Stadt Bern erwirbt lediglich eine Lizenz zu deren Nutzung. Damit ändert sich die datenschutzrechtliche Einordnung wesentlich:

Nutzt die Stadt das Produkt lediglich für Abfragen und ist dabei ausgeschlossen, dass städtische Daten an das System übermittelt werden, ist nicht mehr von einer Auftragsdatenbearbeitung auszugehen. Vielmehr liegt eine eigenständige Datenbearbeitung durch eine private Firma vor.

In diesem Fall liegt die Verantwortung für die Datenerhebung bei der privaten Anbieterin, welche sich an die Vorgaben des Bundesgesetzes über den Datenschutz (DSG) halten muss. Die Verantwortung der Stadt hingegen beschränkt sich bei der Datenerhebung darauf sicherzustellen, dass sie kein Produkt nutzt, das widerrechtlich erhobene Daten beinhaltet.

Zudem muss die Stadt sich bei der Nutzung innerhalb ihrer eigenen rechtlichen Vorgaben bewegen. Die Nutzung von Mobile Mapping muss also, soweit Personendaten betroffen sind, auf einer Rechtsgrundlage beruhen, und die im Rahmen der Vorabkontrolle von 2019 gemachten Vorgaben sind einzuhalten. Ausserdem ist technisch sicherzustellen, dass keine über die technisch notwendigen Nutzerdaten hinausgehenden Informationen von der Stadt an die Anbieterin übermittelt werden, und die personenbezogene Bearbeitung von Nutzerdaten muss, soweit nicht technisch notwendig, untersagt sein.

Antrag

Kenntnisnahme des Tätigkeitsberichts 2025 der Fach- und Aufsichtsstelle Datenschutz der Stadt Bern durch den Stadtrat.

Dank

Die Leiterin Fach- und Aufsichtsstelle Datenschutz und Datenschutzbeauftragte bedankt sich

– bei der Bevölkerung der Stadt Bern für das entgegengebrachte Vertrauen;

– beim Stadtrat und insbesondere bei der Geschäftsprüfungskommission für die Unterstützung und das entgegenbrachte Vertrauen;

– bei der Stadtverwaltung für die konstruktive und spannende Zusammenarbeit;

– bei der Abteilung Personal und Finanzen der PRD für die zuvorkommende und hilfsbereite administrative Unterstützung;

– bei der Ombudsfrau und ihrem Team für die bereichernde Büronachbarschaft;

– bei ihrem Team für das tägliche Engagement und die bereichernde Zusammenarbeit.