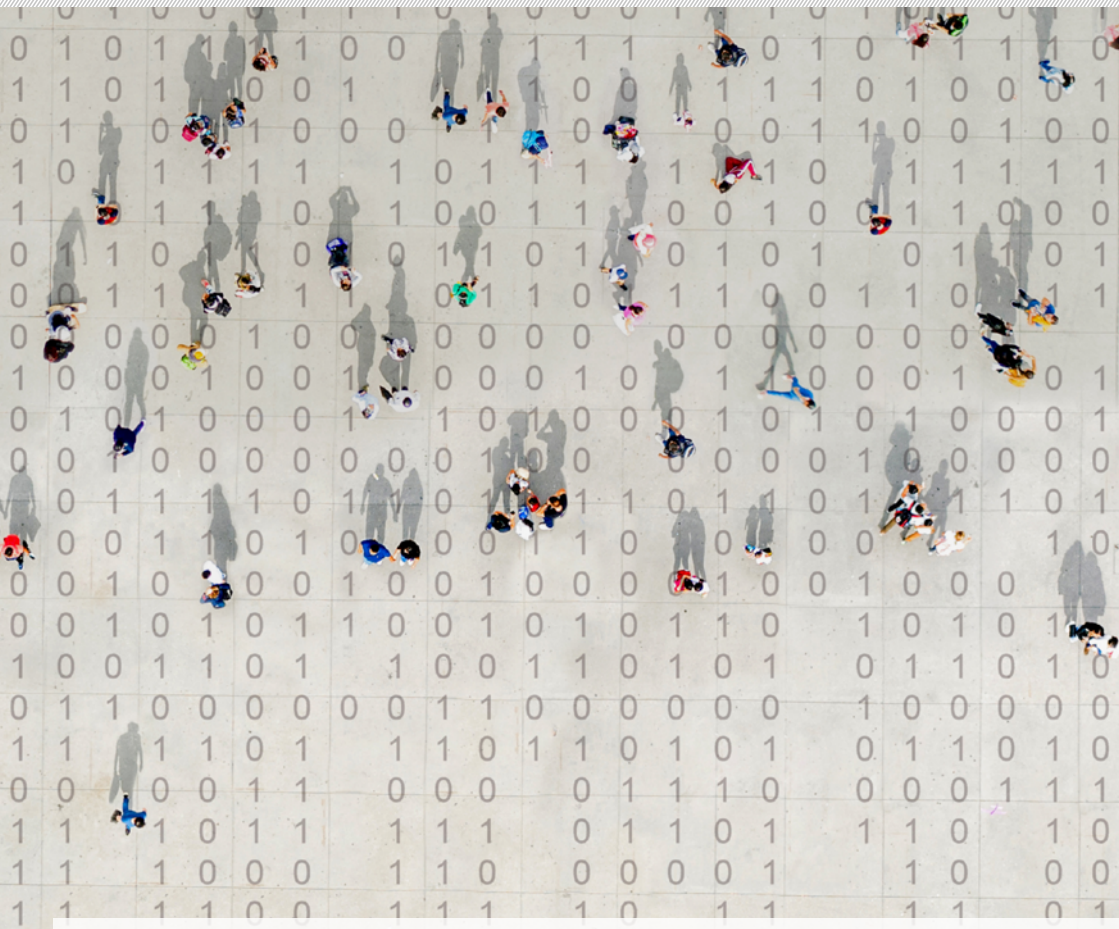
Stadt Bern
Fach- und Aufsichtsstelle
Datenschutz FADS

Fach- und Aufsichtsstelle

Datenschutz



Tätigkeitsbericht 2024

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, Medienlogistik
Abbildung Titelseite: Orbon Alija

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 2024 zu berichten.

Die Fach- und Aufsichtsstelle Datenschutz FADS konnte sich in ihrem zweiten Tätigkeitsjahr stark weiter entwickeln, und der im letztjährigen Tätigkeitsbericht thematisierte Lernprozess kam voll zum Tragen. Nachdem wir unterdessen diverse Vorabkontrollen durchgeführt haben, konnten wir aufgrund der dabei gemachten Erfahrungen unsere Prozesse überarbeiten und zu wiederkehrenden Themen eine gefestigte Praxis entwickeln. Durch die Standardisierung von Abläufen und Dokumenten wurde die Arbeit für alle Beteiligten vereinfacht und effizienter gestaltet. Bei der stark gestiegenen Anzahl von zu bearbeitenden Dossiers war dies dringend angezeigt, um eine zeitgerechte Erledigung unter Beibehaltung einer hohen Arbeitsqualität zu gewährleisten.

Besonders erfreulich ist, dass die Bekanntheit der FADS in der Stadtverwaltung spürbar gestiegen ist, dies nicht zuletzt auch durch die intensivierte Zusammenarbeit mit der ICT-Security von Informatik Stadt Bern (IBE). Insbesondere das Beratungsangebot der FADS wurde häufiger in Anspruch genommen. Ich erachte dies als umso wichtiger, als ein solides Know-How im Bereich Datenschutz für die Stadtverwaltung von wachsender Bedeutung ist. Durch die zunehmende Digitalisierung steigen auch die Komplexität der eingesetzten Systeme und die Anforderungen an einen korrekten Umgang mit den bearbeiteten Daten. Mit der vermehrten Auslagerung von Datenbearbeitungen, speziell auch an ausländische Anbieterinnen, geht auch ein Kontrollverlust einher, der gerade mit Blick auf die aktuelle geopolitische Lage eine Herausforderung darstellt. Dem kann nur mit der Kenntnis um die rechtlichen und technischen Rahmenbedingungen und dem Beharren auf datenschutzkonformen Produkten und Kontrollmöglichkeiten begegnet werden.

Wünschenswert ist jedoch auch eine verstärkte Diskussion dieser Themen auf politischer Ebene. Die Frage, wie weit die Digitalisierung trotz der damit verbundenen Risiken für die Persönlichkeitsrechte der Bevölkerung gehen soll, muss in einer Demokratie auf dieser Ebene beantwortet werden. Auch der dafür notwendige Willensbildungsprozess setzt Datenschutzkenntnisse voraus. Die FADS freut sich, wenn sie mit ihrer Arbeit auch hier einen Beitrag leisten kann.

Sophie Haag
Datenschutzbeauftragte der Stadt Bern

Bern, im März 2025

1

Rückblick

Die FADS hat im Berichtsjahr eine steigende Anzahl an Fällen bearbeitet. Der Themenschwerpunkt lag einmal mehr bei der Einführung neuer Applikationen, aber auch die Themen Videoüberwachung und mehrere Anfragen aus dem Schulbereich beschäftigen die FADS.

Themen im Berichtsjahr
Die FADS konnte im Berichtsjahr einige grosse Vorabkontrollverfahren aus dem Vorjahr abschliessen, so z.B. diejenige zu Microsoft 365 in der Stadtverwaltung oder zur Applikation Citysoftnet (vgl. Tätigkeitsbericht 2023 S. 26). Microsoft 365 war im Berichtsjahr auch anderweitig noch immer ein Thema für die FADS, sind bei den Mitarbeitenden der Stadtverwaltung doch diverse Fragen zur korrekten Nutzung aufgekommen. Zudem war es auch ein Schwerpunkt der Vorabkontrolle von base4kids2.

Neu kommen auch erste KI-Anwendungen in der Stadt Bern zur Anwendung. Die FADS hat die damit zusammenhängenden Fragen zum Datenschutz insbesondere bei den Vorabkontrollen der technischen Wasserüberwachung in der neuen Schwimmhalle und der Applikation zur automatisierten Transkription von Kommissionssitzungen vertieft geprüft.

Diverse Beratungsanfragen haben die FADS aus dem Schulbereich erreicht. Einige davon betrafen die Datenweitergabe an andere Behörden. Auch zu Videoüberwachungen bestand Beratungsbedarf, wobei die FADS in diesem Bereich auch Vorabkontrollen durchgeführt hat.

Auffallend ist der Anstieg der durch die FADS im Berichtsjahr bearbeiteten Fälle. So wurde ihr Beratungsangebot insbesondere durch die Stadtverwaltung rege benutzt, aber auch die Zahl der durchgeführten Vorabkontrollen nahm zu. Auch eine erste ordentliche Kontrolle konnte in der zweiten Jahreshälfte gestartet werden.

Vernetzung, Austausch und Weiterbildungen
Die FADS war auch zur Vernetzung und für den Austausch mit Behörden inner-

und ausserhalb der Stadtverwaltung im Berichtsjahr weiterhin aktiv. So konnte die Zusammenarbeit mit der ICT-Security von IBE intensiviert werden, was sich als sehr gewinnbringend erwiesen hat. Insbesondere konnte die FADS auch bei der Überarbeitung der ISDS-Vorlagen mitwirken, die den ISDS-Prozess inkl. einer allfällig daran anschliessenden Vorabkontrolle bei der FADS für alle Beteiligten vereinfachen sollen. Auch mit Digital Stadt Bern und den Verantwortlichen grosser IT-Vorhaben fanden Gespräche zu den die Stadtverwaltung hauptsächlich beschäftigenden Themen statt. Damit erhielt die FADS die Möglichkeit, ihren Standpunkt auf strategischer Ebene einzubringen und die Anliegen des Datenschutzes so auch projektübergreifend zu adressieren. Weitergeführt wurde der Austausch mit der Ombudsstelle und dem Ratssekretariat, und es wurden auch bereits erste Gespräche mit der neuen Finanzkontrolle der Stadt Bern geführt.

Auch der Austausch mit anderen Datenschutzbehörden konnte, insbesondere durch die Teilnahme an den Plenarversammlungen von Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, oder durch die Mitarbeit in deren Arbeitsgruppen, weitergeführt werden.

Sehr geschätzt wurden die regelmässigen Gespräche mit der GPK resp. mit einem Ausschuss der GPK. Für die FADS ist es wichtig, dass sie sowohl für organisatorische Anliegen als auch für fachliche Themen eine Ansprechpartnerin hat und die für ihre Tätigkeit nötige Unterstützung erhält.

Zudem hat das Team der FADS sein Wissen mit Weiterbildungen erweitert und aktuell gehalten. Durch die Teilnahme an diversen Angeboten, vom stadtverwaltungsinternen Webinar bis zu einem CAS aus dem Bereich ICT-Sicherheit und Audit, stellt es sicher, dass es auch künftig qualitativ hochstehende und fachlich fundiert Arbeit leisten kann.

Digitale Fallführung für FADS und OS

Die FADS konnte zusammen mit der Ombudsstelle die Vorbereitungsarbeiten zur Einführung der neuen Fallführungssoftware abschliessen und ihre Fallführung per 1. Januar 2025 auf das neue System umstellen. Erste Erfahrungen aus der Testphase haben gezeigt, dass damit das Fallmanagement in der täglichen Arbeit spürbar vereinfacht wird, was zu einer zusätzlichen Entlastung führen wird.

2

Schwerpunktthema: ISDS-Prozess und Vorabkontrolle bei der FADS

Die Zusammenarbeit zwischen der FADS und der ICT-Security bei Informatik Stadt Bern wurde im Berichtsjahr intensiviert. Der Austausch zu sicherheitsrelevanten Themen konnten verbessert, die Kontrollprozesse besser koordiniert und die ISDS-Vorlagen gemeinsam modernisiert werden. Die FADS hat zudem auch ihre eigenen Prozesse überarbeitet.

Zusammenarbeit mit ICT-Security
Die Zusammenarbeit mit dem neu geschaffenen Bereich Governance & Compliance konnte im Berichtsjahr dank der Besetzung von offenen Stellen bei der Informatik Stadt Bern (IBE) intensiviert werden. Das dabei auf fachlicher Ebene geteilte Wissen führte dank der internen Besetzung der Stellen bei IBE zu einem nachhaltigen Umgang mit den Themen Informationssicherheit und Datenschutz innerhalb der Stadt Bern und zu einer gemeinsamen Praxis in diesem Bereich. Diese Entwicklung begrüsst die FADS ausserordentlich, da sie dadurch ihre gesetzlichen Aufgaben der Beratung und Kontrolle der städtischen Behörden effektiver und effizienter ausführen kann.

Nebst einem zweiwöchig stattfindenden Austausch mit der ICT-Security, an dem wertvolle Informationen geteilt und neue Vorhaben im Compliance Check Prozess besprochen werden, etablierte sich eine regelmässige und konstruktive Zusammenarbeit in konkreten Fragestellungen im Bereich des Datenschutzes und der Informationssicherheit. Als Folge davon konnte die FADS im Berichtsjahr an der Aktualisierung der ISDS-Vorlagen sowie bei der Erstellung von Merkblättern mitarbeiten.

Überarbeitung von ISDS-Vorlagen
Mit dem Compliance Check Prozess soll sichergestellt werden, dass in der städtischen Verwaltung keine Applikationen in Betrieb genommen werden, welche die Sicherheitsvorgaben nicht erfüllen. Im Rahmen dieses Prozesses muss die datenbearbeitende Behörde Dokumente zu Informationssicherheit und Datenschutz (ISDS-Dokumente) erstellen. Unterstützt wird sie dabei von der ICT-Security von IBE. Die so erstellten Dokumente dienen ausserdem der FADS dazu, eine Applikation vor ihrer Inbetriebnahme auf ihre Datenschutz-

konformität hin zu überprüfen (vgl. dazu auch Tätigkeitsbericht 2023 S. 8 f.).

Als Grundlage zum Erstellen dieser ISDS-Dokumente dienen Vorlagen, welche die ICT- Security zur Verfügung stellt. Diese Vorlagen wurden im Berichtsjahr überarbeitet und bedienerfreundlicher gestaltet. In die Aktualisierung der Vorlagen für die Schutzbedarfsanalyse (Schuban), die Risikoanalyse sowie für das ISDS-Konzept war die FADS im Berichtsjahr beratend involviert.

Einfacheres Erstellen von ISDS-Dokumenten dank neuer Vorlagen

Für die FADS war die Aktualisierung dieser Vorlagen ein zentrales Anliegen. Damit wird es nicht nur den Projektverantwortlichen vereinfacht, die für eine geplante Datenbearbeitung notwendigen Dokumentationen in der geforderten Qualität zu erstellen. Werden bei der FADS zur Vorabkontrolle eingereichte Dokumente gestützt auf diese Vorlagen erstellt, kann eher sichergestellt werden, dass die nötige Maturität der Unterlagen gegeben und die Arbeiten der FADS standardisiert und effizient durchgeführt werden können. Bei der steigenden Anzahl von durchzuführenden Vorabkontrollen ist dies dringend angezeigt, wenn die FADS die damit verbundenen Arbeiten innert nützlicher Frist erledigen können soll. Die FADS fordert daher alle Projektverantwortlichen der städtischen Verwaltung dazu auf, ihre ISDS-Unterlagen gestützt auf diese Vorlagen zu erstellen.

Neue Vorlage zur Schutzbedarfsermittlung

In einer Schuban wird der Schutzbedarf einer geplanten Datenbearbeitung ermittelt. Die Einstufung geschieht dabei in den vier klassischen IT-Sicherheitsbereichen «Vertraulichkeit», «Verfügbarkeit», «Integrität» und «Nachvollziehbarkeit». Aus Sicht Datenschutz liegt ein erhöhter Schutzbedarf dann vor, wenn besonders schützenswerte Personendaten oder Informationen, die einer besonderen Geheimhaltungspflicht unterliegen (z.B. Sozialhilfegeheimnis) bearbeitet werden oder wenn die Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist (z.B. KI/ML, Cloud, automatisierte Einzelfallentscheidungen, systematische Überwachungen, Scoring oder Profiling, Verwendung biometrischer Daten, Gesichtserkennung, Vernetzung verschiedener Datenbanken).

Die bisherige Vorlage trug insbesondere den datenschutzrechtlichen Aspekten zu wenig Rechnung, so dass eine gestützt darauf durchgeführte Analyse kein aussagekräftiges Resultat ergab. So konnte es vorkommen, dass aus der Analyse trotz korrekter Durchführung kein weiterer Handlungsbedarf resultierte, obschon die geplante Datenbearbeitung mindestens einen der oben aufgeführten Punkte erfüllt und gemäss dem kantonalen Datenschutzgesetz tatsächlich vor deren Beginn der FADS zur Vorabkontrolle unterbreitet werden muss. Daher wurde die Vorlage dahingehend angepasst, dass nun sowohl die Informationssicherheitsaspekte als auch diejenigen des Datenschutzes abgedeckt sind. Mit einer auf Basis der überarbeiteten Vorlage erstellten Schuban erhält ein Projekt eine zuverlässigere Aussage zu den weiteren notwendigen Schritten für ein korrektes Durchlaufen des ISDS-

Prozesses. Aufgrund dieser umfassenden Ermittlung des Schutzbedarfes werden im Projekt die Themen Datenschutz und Informationssicherheit zu einem frühen Zeitpunkt adressiert, und das weitere Vorgehen im Compliance Check Prozess kann bedarfsgerecht festgelegt werden.

Neue Schuban liefert zuverlässigere Resultate

Die Schuban wird durch die datenbearbeitende Behörde mit Unterstützung der ICT-Security ausgefüllt. Die FADS kann hierbei beratend beigezogen werden, insbesondere für ein Review der Schuban. Im Berichtsjahr führte die FADS gesamthaft 20 solcher Schuban Reviews durch und konnte so die Aspekte des Datenschutzes zu einem frühen Zeitpunkt einbringen. Auch hier zeigt sich die konstruktive Zusammenarbeit mit der ICT-Security. Aufgrund der Adressierung von relevanten Themen in dieser Projektphase können die Vorbereitungsarbeiten für eine allfällige Erstellung der ISDS-Dokumente durch die datenbearbeitende Behörde frühzeitig geplant und umgesetzt werden.

Selbstdeklaration Einhaltung Weisung Cloud Computing

Findet eine Personendatenbearbeitung in der Cloud statt, muss die datenbearbeitende Behörde resp. der Clouddienstleister zusätzlich und unabhängig vom Schutzbedarf den Nachweis der Erfüllung der Vorgaben aus der Weisung Cloud Computing der Stadt Bern (WCC) erbringen. Dazu verfasste die ICT-Security in Zusammenarbeit mit der FADS im Berichtsjahr eine Checkliste. Von zentraler Bedeutung ist hier die Schaffung von Transparenz in Bezug auf potenzielle Cloudanbieter. Damit keine cloudbasierte Applikation beschafft wird, die nicht den Vorgaben der Stadt Bern entspricht, wäre es auch wünschenswert, dass die Kriterien der WCC bereits als Kriterien in der Beschaffung miteinbezogen werden.

Neue Vorlage zur Erstellung einer Risikoanalyse

Die Risikoanalyse ist Teil des Risikomanagements und dient der Identifikation und Bewertung der Risiken, die mit einer geplanten Datenbearbeitung einhergehen. Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf für eine geplante Datenbearbeitung, ist zwingend eine Risikoanalyse dazu zu erstellen.

Die bisherige städtische Vorlage zum Erstellen einer Risikoanalyse fokussierte stark auf klassische Schutzziele, wie den Zugangs- und den Zutrittsschutz, und trug insbesondere technischen Entwicklungen, wie z.B. einer rein Cloud-basierten Datenbearbeitung, zu wenig Rechnung. Die aktualisierte Vorlage verlagert ihren Fokus weg von solchen allgemeinen, den Grundschutz betreffenden und damit allen Datenbearbeitungen inhärenten Risiken hin zu den effektiv anfallenden spezifischen Risiken. Bei geplanten Datenbearbeitungen in der Cloud werden die cloudspezifischen Risiken nun explizit behandelt.

In einer Risikoanalyse sind die bei einer Datenbearbeitung anfallenden Risiken zu eruieren, und für jedes erkannte Risiko müssen jeweils die Eintretenswahrscheinlichkeit und das Schadenspotential sorgfältig abgeschätzt werden. Auch hier wurde die Vorlage angepasst, so dass beim Schadenspotential nebst einem potenziellen Personen-, Reputations- oder finanziellen Schaden neu auch die möglichen Folgen einer Persönlichkeitsverletzung zu berücksichtigen sind.

Aus der Eintretenswahrscheinlichkeit verbunden mit dem Schadenspotential lässt sich in der Folge ableiten, wie hoch die jeweiligen Risiken sind und ob zusätzliche Massnahmen zu deren Senkung getroffen werden müssen. Ist ein Risiko nach dieser Methode als «hoch» oder «sehr hoch» zu bewerten, muss es mit geeigneten technischen und/oder organisatorischen Massnahmen auf ein tragbares Niveau gesenkt werden. Die nach Umsetzung der Massnahmen verbleibenden Risiken sind als Restrisiken transparent auszuweisen, und die verantwortliche Behörde (resp. ihre Leitung) hat explizit zu bestätigen, dass sie diese verstanden hat und die Restrisiken übernimmt.

Die bei der Einführung einer neuen Applikation ermittelten Risiken müssen von der datenbearbeitenden Behörde auch im laufenden Betrieb kontinuierlich neu bewertet werden. Gegebenenfalls müssen im Rahmen des Risikomanagements neue Massnahmen ergriffen werden, um die Restrisiken in einem akzeptablen Mass zu halten.

Neuer Vorlage zur Erstellung eines ISDS-Konzeptes

Bei erhöhtem Schutzbedarf ist das Erstellen eines Informationssicherheits- und Datenschutzkonzeptes (ISDS-Konzept) erforderlich. In diesem Konzept werden alle Aspekte im Bereich Informationssicherheit und Datenschutz dokumentiert. Die Vorlage dazu wurde im Berichtsjahr überarbeitet.

Zu einem ISDS-Konzept gehören insbesondere eine Systembeschreibung samt Darlegung der zu bearbeitenden Daten, die Sicherheitsarchitektur, ein Rollen- und Berechtigungskonzept, eine Kommunikationsmatrix sowie die nach Umsetzung der Sicherheitsmassnahmen verbleibenden Restrisiken. Die FADS hat an der Überarbeitung der dafür von der ICT-Security bereitgestellten Vorlage mitgewirkt. Die wichtigen Punkte der Informationssicherheit und des Datenschutzes sollen damit einfacher und systematisch ermittelt und dokumentiert werden können. Zudem wurden neu einzuhaltende Vorgaben darin eingearbeitet

Die aktualisierte Vorlage vereinfacht das Erstellen eines ISDS-Konzeptes in erster Linie dadurch, dass diverse, zuvor als Fliesstext zu erfassende Angaben neu in tabellarischer Form aufgeführt werden können. So wurden für die Beschreibung der bearbeiteten Daten (inkl. Datentyp, Bearbeitungszweck und gesetzliche Grundlage), für das Rollen- und Berechtigungskonzept (beschreibt, welche Rolle zu welchen Zwecken welche Zugriffsrechte erhält) sowie für die Kommunikationsmatrix (beschreibt, wie das System mit Umsystemen kommuniziert) Tabellen eingefügt. Damit können die relevanten Informationen rasch und für alle Beteiligten übersichtlicher erfasst werden.

Erhöhter Schutzbedarf macht ISDS-Konzept nötig

Im Weiteren wurde die bereits zusammen mit der Schuban auszufüllende Selbstdeklaration Einhaltung Weisung Cloud Computing in die Vorlage integriert. Der grösste Teil der darin anzugebenden Informationen ist auch in einem ISDS-Konzept relevant. Nun können sie aus den Arbeiten zur Schuban übernommen und in tabellarischer Form in das ISDS-Konzept eingefügt werden. Auch sieht die neue Vorlage die von der verantwortlichen Behörde abzugebende Erklärung zur Übernahme der Restrisiken nun explizit vor.

Erstellung von Merkblättern
Nebst der Mitarbeit bei der Aktualisierung von Vorlagen nahm die FADS im Berichtsjahr beratend Stellung zu Merkblättern der ICT-Security. Im Zentrum standen dabei die beiden Merkblätter zum einem Proof of Concept- (PoC) resp. eines Pilot-Vorhabens und zur Nutzung von personenbezogenen Daten zu Testzwecken.

Nebst der Klärung der beiden Begriffe «PoC» und «Pilot» werden im ausgearbeiteten Merkblatt Anforderungen an die jeweiligen Vorhaben definiert. Ein PoC dient dazu, die Machbarkeit einer bestimmten Idee, Technologie oder Lösung in einem kontrollierten Rahmen zu demonstrieren. Im Gegensatz dazu stellt ein Pilot eine vorläufige Implementierung einer Lösung in einem begrenzten Umfang dar, um die Effektivität und Praktikabilität einer Lösung unter realen Bedingungen zu testen. Für jedes PoC- resp. Pilot-Vorhaben ist zwingend der Schutzbedarf mittels Schuban zu ermitteln. Bei einem erhöhten Schutzbedarf sind ISDS-Dokumente zu erstellen und der ordentliche Compliance Check Prozess ist zu beschreiten.

Testbetrieb birgt erhöhte Risiken

Aus datenschutzrechtlicher Sicht ist darauf zu achten, für die Durchführung eines PoC bzw. Piloten Daten ohne Personenbezug (synthetische oder anonymisierte Daten) zu verwenden. Nur, wenn es zur Erreichung des Zieles zwingend notwendig ist, kann ausnahmsweise mit Personendaten gearbeitet werden.

Diese Nutzung von personenbezogenen Daten zu Testzwecken ist Thema eines weiteren Merkblattes. Im Austausch mit ICT-Security wurden die dabei aus datenschutzrechtlicher Sicht problematischen Aspekte behandelt: Die Bearbeitung von Personendaten für Testzwecke stellt in der Regel ein erhöhtes Risiko für die Rechte der betroffenen Personen dar. So besteht z.B. eine erhöhte Gefahr von Datenpannen bei noch nicht abschliessend entwickelten und daher fehleranfälligeren Systemen. Sollen trotzdem personenbezogene Daten zu Testzwecken verwendet werden, muss das erhöhte Risiko in den ISDS-Unterlagen dargelegt und dessen Inkaufnahme begründet werden. Insbesondere ist auszuführen, warum die Nutzung anonymisierter oder synthetischer Daten nicht möglich resp. mit einem unverhältnismässigen Aufwand verbunden wäre.

Die FADS empfiehlt, von einer Nutzung von besonders schützenswerter Personendaten für Testzwecke gänzlich abzusehen. Ein Datensatz mit besonders schützenswerten Personendaten ist vor der Nutzung für Testzwecke zu maskieren.

Die Zugriffsrechte sind im Weiteren so auszugestalten, dass die Berechtigungen zur Datenbearbeitung auf Personen beschränkt werden, die den Zugriff zur Erreichung des Testzweckes zwingend benötigen. Nach Beendigung einer Testphase sind die personenbezogenen Daten auf der Testumgebung zu löschen, und es ist sicherzustellen, dass in allfällig vorhandenen Testprotokollen keine personenbezogenen Daten enthalten sind.

Vorabkontrollen bei bereits betriebenen Applikationen
Bereits im letztjährigen Tätigkeitsbericht hat die FADS die Vorabkontrolle und den damit einhergehenden Lernprozess für die FADS und die Verwaltung in einem Schwerpunktthema behandelt (vgl. Tätigkeitsbericht 2023 S. 8). Auch im

Berichtsjahr hat sich die FADS mit einer steigenden Anzahl solcher Vorabkontrollen beschäftigt. Dabei hat sich folgendes Vorgehen etabliert: Sobald die FADS die ihr unterbreiteten Unterlagen geprüft hat, stellt sie den verantwortlichen Behörden das Resultat ihrer Prüfung in einem ersten Schritt in Form einer Befundliste zu. Bei Bedarf wird diese Liste besprochen, die FADS erläutert ihre Befunde und berät die verantwortlichen Behörden bei der Bereinigung der Befunde. Im Anschluss überarbeitet die verantwortliche Behörde ihre ISDS-Unterlagen im Sinne der Befundliste resp. der dazu geführten Beratungsgespräche oder begründet, warum eine von der FADS verlangte Anpassung nicht vorgenommen wird. Aufgrund der so überarbeiteten ISDS-Unterlagen erstellt die FADS ihren Vorabkontrollbericht und schliesst das Verfahren ab.

Der Zweck der Vorabkontrolle besteht in erster Linie darin, datenschutzrechtliche Mängel einer Datenbearbeitung bereits im Planungsstadium zu erkennen und zu beseitigen, was einerseits Aufwand sparen und andererseits verhindern kann, dass Applikationen, welche die Persönlichkeitsrechte der Betroffenen verletzen würden, überhaupt in Betrieb genommen werden. Die Vorabkontrolle stellt damit zwar ein Mittel der Aufsicht dar, kann aber durchaus auch als Dienstleistung für die verantwortliche Behörde verstanden werden. Dies gilt umso mehr, als die FADS, wie beschrieben, stark beratende Elemente in ihre Tätigkeit einfliessen lässt.

Dieser Bereinigungsprozess kann jedoch mehrere Runden umfassen und damit auch einige Zeit in Anspruch nehmen. Leider ist es wiederholt vorgekommen, dass der Abschluss des Vorabkontrollverfahrens nicht abgewartet und eine Applikation bereits in Betrieb genommen wurde, bevor die Befundliste bereinigt werden konnte. In gewissen Fällen wurden der FADS auch bereits im Betrieb genommene Applikationen zur Vorabkontrolle unterbreitet. Damit kann der mit der Vorabkontrolle verbundene Hauptzweck nicht mehr erreicht werden, da potenziell persönlichkeitsverletzende Datenbearbeitungen bereits stattfinden. Zum Teil wurden dabei auch Tatsachen geschaffen, die, falls überhaupt, nur noch mit grossem Aufwand geändert werden können. Die FADS machte in solchen Fällen auch die Erfahrung, dass sich das Projekt mit seiner Umsetzung so geändert hat, dass die nun tatsächlich durchgeführte Datenbearbeitung erheblich von der eingereichten Dokumentation abweicht.

Dies zeigt, 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. Vielmehr ist es hierfür angezeigt, den Ist-Zustand, d.h. die tatsächlich durchgeführte Datenbearbeitung, im Rahmen einer ordentlichen Kontrolle zu überprüfen.

Daher ist die FADS dazu übergegangen, bei bereits betriebenen Applikationen keine Vorabkontrolle mehr durchzuführen und, werden ihr solche Unterlagen unterbreitet, nur noch beratend Hinweise zur Verbesserung des Datenschutzniveaus zurückzumelden. Laufende Vorabkontrollen werden beendet, wenn eine Applikation vor deren Abschluss bereits in Betrieb genommen wird. In beiden Fällen werden die tatsächlich durchgeführten Datenbearbeitungen im Rahmen einer ordentlichen Kontrolle überprüft, falls Hinweise auf Mängel im Bereich Datenschutz vorliegen. Allenfalls bereits geleistete Vorarbeiten, wie z.B. Prüfberichte oder Befundlisten, können dabei als Grundlage für die ordentliche Kontrolle wiederverwendet werden.

3

Schwerpunktthema: Data-at-rest-Verschlüsselung für Daten in der Cloud

Werden Informationen der Stadtverwaltung in der Cloud bearbeitet, müssen sie durch eine Verschlüsselung vor unberechtigten Zugriffen geschützt werden. Im Berichtsjahr hat sich wiederholt gezeigt, dass diese Vorgabe nicht immer eingehalten werden kann.

In der Verwaltung der Stadt Bern werden vermehrt Cloud-Dienste eingesetzt, die nicht mehr auf der eigenen Infrastruktur betrieben werden, sondern auf den Servern von – meist privaten – Anbieter*innen. Bearbeitet die Stadtverwaltung Personendaten in der Cloud, ist eine ausreichende Verschlüsselung besonders wichtig, damit die datenschutzrechtlichen Vorgaben eingehalten werden können. Einerseits müsse die Daten abhörsicher zwischen der Stadtverwaltung und den Cloud-Anbieter*innen übermittelt werden (data-in-transport-Verschlüsselung), andererseits müssen aber auch die gespeicherten Daten vor unberechtigten Zugriffen geschützt werden (data-at-rest-Verschlüsselung). Die data-at-rest-Verschlüsselung soll sowohl vor unberechtigten Zugriffen von aussen, z.B. durch einen Hackerangriff, schützen, als auch verhindern, dass die Cloud-Anbieter*innen selbst auf den Inhalt der bei ihnen gespeicherten Informationen der Stadtverwaltung Zugriff nehmen. Daher muss entweder das Schlüsselmanagement bei der Stadtverwaltung selbst liegen oder die Anbieterin durch vertragliche Zusicherungen verpflichtet werden, die Daten nicht ohne Zustimmung der Stadt zu entschlüsseln.

Aktives Einfordern datenschutzfreundlicher Technologien

Wie die FADS im Berichtsjahr wiederholt feststellen musste, wird diese Vorgabe nicht in allen Bereichen eingehalten. Während die data-in-transport-Verschlüsselung bei Datenübermittlungen über öffentliche Netze ausreichend implementiert ist, werden ruhende Daten in

einigen Bereichen gar nicht verschlüsselt, oder eine Verschlüsselung findet nur auf Ebene Festplatte statt. Letzteres bietet zwar einen Schutz, wenn ein Datenträger gestohlen wird oder verloren geht, nicht aber im laufenden Betrieb, da die Daten dann lesbar im Klartext vorliegen. Damit bietet die Festplattenverschlüsselung keinen ausreichenden Schutz.

Dass eine data-at-rest-Verschlüsselung fehlt, kann unterschiedliche Gründe haben. Bei einigen Anwendungen ist das Fehlen technisch begründet, da die Verschlüsselung wichtige Funktionalitäten verunmöglichen würde. So müssen z.B. bei einer Volltextsuche die durchsuchten Informationen in der Regel in Klartext vorliegen. Anderenfalls wird der Rechenaufwand für das System so gross, dass Suchresultate nur mit Verzögerung angezeigt werden oder gar ein Systemabsturz provoziert wird. Kann eine data-at-rest-Verschlüsselung aus solchen technischen Gründen nicht umgesetzt werden, fordert die FADS, dass ein gleichwertiges Sicherheitsniveau mit Hilfe anderer Massnahmen hergestellt wird.

Anders ist die Situation zu beurteilen, wenn das Fehlen nicht technisch bedingt ist. Gerade bei Standardprodukten, welche als Gesamtpaket bei einer Dienstleisterin bezogen werden, ist es möglich, dass darin z.B. aus Kostengründen keine data-at-rest-Verschlüsselung enthalten ist, oder weil die Dienstleisterin diese Anforderung bei ihrer Produkteentwicklung nicht antizipiert hat. In diesen Fällen fordert die FADS, dass der Mangel zeitnah mit einer nachträglichen Implementierung behoben wird.

Im Berichtsjahr hat diese Forderung der FADS bereits in einigen Fällen dazu geführt, dass Anbieter*innen ihr Produkt in diesem Sinne überarbeitet oder eine baldige Überarbeitung zugesichert haben. Damit konnte die Sicherheit der damit bearbeiteten Daten erheblich verbessert werden. Dies zeigt, wie wichtig es ist, solche datenschutzfreundlichen Technologien bei den Anbieter*innen auch aktiv einzufordern. In der Pflicht sind hierbei insbesondere auch die für die Beschaffung Verantwortlichen, welche diesem Aspekt vor Abschluss eines Vertrages für ein neues Produkt Beachtung schenken müssen.

Bearbeitet die Stadtverwaltung Personendaten in der Cloud, ist eine ausreichende Verschlüsselung besonders wichtig.

4

Schwerpunktthema: Erste Anwendungen von KI in der Stadtverwaltung

Im Berichtsjahr beschäftigte sich die FADS mit ersten Anwendungen von maschinellem Lernen/KI in der Stadt Bern. Nebst der algorithmus-basierten Überwachung des Schwimmbeckens in der neuen Schwimmhalle Neufeld setzte sich die FADS mit der automatisierten Transkription von gesprochenem Text in Wortprotokolle an Kommissionsitzungen des Stadtrates sowie mit einem PoC-Betrieb von zwei ML-basierten Suchassistenten der Einwohnerdienste, Migration und Fremdenpolizei der Stadt Bern auseinander.

Beim Einsatz von KI/ML[1] muss grundsätzlich unterschieden werden zwischen KI-Komponenten, die innerhalb von Applikationen zum Einsatz kommen, und generativer KI. In Systeme integrierte KI-Komponenten können beispielsweise innerhalb der Microsoft 365-Produktpalette zum Einsatz kommen. Die sog. Connected Experiences etwa bieten u.a. die Möglichkeit, Dateninhalte zu analysieren oder Onlineinhalte zu suchen und herunterzuladen. Generative Modelle hingegen können aufgrund von erlernten Mustern Texte, Bilder, Musik und Videos selbst generieren. Durch das Training mit grossen Datenmengen werden Muster aus vorhandenen Daten erlernt.

Aus datenschutzrechtlicher Sicht ist der Einsatz von KI-Technologien aus mehreren Gründen von Bedeutung. In erster Linie ist hier die fehlende Vertraulichkeit der eingegebenen Daten zu erwähnen, da in KI-Anwendungen bearbeitete Daten oft für Training und Lernvorgang weiterverwendet werden. Aber auch die fehlende Reproduzierbarkeit und Erklärbarkeit von Resultaten und die mangelnde Transparenz der dahinterliegenden Algorithmen sowie die Re-Identifizierung von Personen aus anonymisierten Daten (z.B. durch Verknüpfung von Trainingsdaten aus verschiedenen Quellen) sind Themen, die für den Datenschutz immer relevanter werden.

Für die Beurteilung der Datenschutzkonformität ist die Bearbeitung von Personendaten über den gesamten Bearbeitungszyklus in einer KI-Anwendung

1 Der Einfachheit halber wird hier der Begriff «KI» verwendet, obwohl es keine allgemeingültige Definition davon gibt. In vorliegendem Bericht wird der Begriff benutzt, um den Vorgang zu beschreiben, in dem Algorithmen durch Wiederholung lernen, selbstständig eine Aufgabe zu erfüllen. Dies wird auch als maschinelles Lernen (ML) bezeichnet. Siehe dazu: https://cnai.swiss/dienstleistungen/terminologie-2/

zu betrachten: Von der Sammlung der Daten, über das Training der Modelle mit Trainingsdaten und die Nutzung von in Applikationen eingebundenen Komponenten oder von Chatbots durch Userinput (Prompting), bis hin zum Modell-Output durch Generierung von Text, Bildern oder Erteilen von Handlungsempfehlung.

Den mit dem Einsatz von KI-Technologien verbundenen Risiken muss mit geeigneten Gegenmassnahmen begegnet werden. Hierzu bietet es sich primär an, personenbezogene Daten vor einer Verwendung zu Trainingszwecken zu filtern oder zu anonymisieren. Ergänzt werden sollte dies durch die transparente Aufklärung über Nutzungsrisiken, durch Sensibilisierung der Nutzenden im Hinblick auf Fähigkeiten und Schwächen von KI-Technologien sowie durch die Sicherstellung der Erklärbarkeit der Entscheidungen und Funktionsweise der ML-Modelle, in dem diese für Menschen nachvollziehbar und verständlich gemacht werden.

Datenschutzkonformität muss über den gesamten Bearbeitungszyklus gegeben sein

Zu dieser Thematik hat Digital Stadt Bern im Berichtsjahr das «Merkblatt zur Verwendung von generativen KI-Werkzeugen in der Stadt Bern» veröffentlicht und die Arbeiten für eine übergeordnete städtische KI-Strategie in Angriff genommen. Die im Merkblatt grundsätzlich wiedergegebene Haltung, dass mit KI-Werkzeugen keine Personendaten bearbeitet werden dürfen, ist aus Sicht Datenschutz begrüssenswert. Die Normierung des Einsatzes von KI erachtet die FADS als ausserordentlich wichtig. Dabei gilt es jedoch, nebst den im erwähnten Merkblatt behandelten generativen KI-Werkzeugen auch KI-Komponenten innerhalb von Applikation allgemein zu behandeln sowie Qualitätsanforderungen an Systeme vorzugeben und, abhängig von der Klassifizierung resp. dem Schutzbedarf der Daten, Einsatzzwecke festzulegen.

Da der Einsatz von KI-Technologien mit besonderen Risiken für die betroffenen Personen verbunden ist, ist vor einem konkreten Einsatz in der Stadtverwaltung der Compliance Check Prozess inkl. anschliessender Vorabkontrolle durch die FADS zu durchlaufen, wobei die besonderen Aspekte der Nutzung von KI explizit zu adressieren sind. Im Berichtsjahr wurden der FADS denn auch erste Applikationen mit KI/ML-Komponenten zur Vorabkontrolle unterbreitet.

Technische Wasserüberwachung Schwimmhalle

Die Algorithmus-basierte Videoüberwachung des Schwimmbeckens in der neuen Schwimmhalle Neufeld detektiert mit Hilfe von KI-Technologie auffälliges Schwimmverhalten und alarmiert gegebenenfalls die Schwimmaufsicht via Smartwatch. Die Abklärungen zur Funktionsweise der dabei eingesetzten Algorithmen sowie der Datenbearbeitung durch die Herstellerfirma gestalteten sich aufwendig, haben jedoch zur unerlässlichen Transparenz beim Einsatz von KI geführt.

Im Berichtsjahr konnte die FADS die Vorabkontrolle zur technischen Wasserüberwachung in der Schwimmhalle Neufeld abschliessen. Zum Zeitpunkt der Eröffnung im Herbst 2023 war die Vorabkontrolle noch nicht abgeschlossen, und daher verzichtete das Sportamt auf die produktive Nutzung zum Eröffnungszeitpunkt.

Der erste Prüfbericht der FADS enthielt diverse Befunde mit hoher Gewichtung. So mussten insbesondere die Datenbearbeitung durch die Herstellerfirma detaillierter beschrieben und die Funktionsweise der KI-Komponenten transparenter dargelegt werden. Dazu gehörte auch die Frage, welche Daten aus dem Betrieb der Oberwasserkameras in der Schwimmhalle zum Training der KI verwendet werden und wo dieses Training stattfindet, lokal auf der Infrastruktur der Stadt Bern oder auf den Servern der Herstellerfirma im Ausland. Zur Klärung der offenen Fragen fanden mehrere bilaterale Besprechungen zwischen der FADS und dem Sportamt, aber auch ein Austausch mit Vertretern der Herstellerfirma, des Sportamtes und der FADS statt. Dabei hat sich gezeigt, dass die personenbezogenen Videobilder unmittelbar nach der Generierung von Bewegungsmustern gelöscht und die so im Betrieb gewonnen Daten lediglich zum Training der lokalen KI benutzt werden. In die globalen Trainingsdaten des Herstellers, die zur Verbesserung der allgemeinen Algorithmen genutzt werden, gelangen lediglich aggregierte Daten wie Statistiken über Systemleistung, Fehlalarme und Erkennungsgenauigkeit.

Transparente Beschreibung von KI-Komponenten

Das Sportamt hat die ISDS-Unterlagen gestützt auf diese Erkenntnisse aktualisiert und der FADS eingereicht. Die Prüfung dieser Unterlagen ergab keine Befunde, so dass die Vorabkontrolle im Frühling 2024 abgeschlossen werden konnte. Anschliessend reichte das Sportamt die notwendigen Unterlagen für das Rückspracheverfahren gemäss Art. 124 des Polizeigesetzes (PolG; BSG 551.1) der Kantonspolizei ein, die wiederum gestützt auf das Resultat der Vorabkontrolle der FADS bestätige, dass der Einsatz der Videoüberwachung in der Schwimmhalle den gesetzlichen Vorgaben entspricht.

Gemäss Videoreglement der Stadt Bern (SSSB Nr. 551.2) müssen Videoüberwachungen an öffentlichen Orten und zum Schutz öffentlicher Gebäude durch den Stadtrat angeordnet werden, worunter auch die technische Wasserüberwachung der neuen Schwimmhalle fällt. Dank den in der Vorabkontrolle geleisteten Vorarbeiten war es möglich, im entsprechenden Vortrag an den Stadtrat die notwendige Transparenz zu schaffen und die Funktionsweise des Systems ausreichend detailliert zu beschreiben, um das Vertrauen des Stadtrates zu gewinnen. So wurde das Geschäft «Wasserüberwachungssystem Schwimmhalle Neufeld; Genehmigung der Videoüberwachung» (2022.BSS.000089) ohne Gegenstimme an der Stadtratssitzung vom 15.08.2024 gutgeheissen[2], und im Herbst 2024 konnte die videobasierte Wasserüberwachung in Betrieb genommen werden.

Automatisierte Transkription von Kommissionssitzungen

Ebenfalls mit KI-Komponenten arbeitet die Applikation Kanparl, die zur Transkription von öffentlichen Sitzungen des Stadtrates bereits vor dem Berichtsjahr produktiv eingesetzt wurde. Das Ratssekretariat plante, den Einsatz auf Kommissionssitzungen des Stadtrates auszuweiten und kontaktierte hierzu die FADS. Die Erkenntnisse aus dem im Berichtsjahr durchgeführten Vorabkontrollverfahren führten zu Anpassungen der Applikation durch den Hersteller, so dass nun Kanparl

2 https://stadtrat.bern.ch/de/geschaefte/detail.php?obj_guid=59d400d321df4ee18c-7f0d21ac0bdb54

auch in Kommissionssitzungen datenschutzkonform genutzt werden kann.

Neue Funktion zum Schutz des Kommissionsgeheimnisses

Mit dem geplanten Einsatz von Kanparl in Kommissionssitzungen steigen die Anforderungen an die Vertraulichkeit der dabei bearbeiteten Informationen, da diese dem Kommissionsgeheimnis unterstehen. Ende 2023 wurden der FADS daher die ISDS-Dokumente zur Applikation Kanparl über das Compliance Check Tool zur Vorabkontrolle unterbreitet. Die Prüfung dieser Unterlagen ergab Informations- und Klärungsbedarf, welchen die FADS in einer Themenliste festhielt und dem Ratssekretariat zustellte. Am daraufhin stattfindenden Austausch wurden die offenen Fragen erörtert und dargelegt, dass erst nach deren Klärung und der darauffolgenden Aktualisierung der ISDS-Dokumente die Grundlagen für eine Vorabkontrolle gegeben sind. Die dabei zu klärenden Fragen bezogen sich auf die eingesetzte KI-Technologie, die notwendige Selbstdeklaration der Erfüllung der Anforderungen aus der Weisung Cloud Computing der Stadt Bern (WCC) durch die Cloudanbieter sowie das Ausweisen der Restrisiken.

Die vom Ratssekretariat für die Aufzeichnung von Sitzungen und für die Redaktion von Protokollen eingesetzte Applikation Kanparl Cloud sowie ein dazugehöriger Speicherdienst für Audiodateien werden auf der Infrastruktur bei zwei unterschiedlichen schweizerischen Cloudanbietern und der Herstellerfirma betrieben. Daher musste die Selbstdeklaration der WCC-Anforderungen ausgefüllt werden. So kam zu Tage, dass beide Clouddienstleister die aus datenschutzrechtlicher Sicht wichtigen Anforderungen der WCC nicht vollständig erfüllten.

Auf der Infrastruktur der Herstellerin wird zudem die automatische Spracherkennung mit Hilfe von KI-Komponenten betrieben. Nebst Spracherkennung und anschliessender Transkription findet dabei ein Lern-Feedback durch manuelle Korrekturen im generierten Wortprotokoll statt. Aus datenschutzrechtlicher Sicht stellt sich hier die Frage, inwiefern Daten als Trainingsmaterial in das KI-Modell des Herstellers einfliessen und damit den Einflussbereich des Ratssekretariats verlassen. Im Austausch mit den Beteiligten konnte geklärt werden, dass dies tatsächlich der Fall war, was mit Blick auf vom Kommissionsgeheimnis geschützte Informationen zu verbessern war. Um einen datenschutzkonformen Betrieb der Applikation für vertrauliche Daten zu gewährleisten, implementierte die Herstellerin daher eine neue Funktion, um Daten aus Kommissionssitzungen vom Training der KI ausschliessen zu können. Als organisatorische Massnahmen hat das Ratssekretariat die Weisung «Benutzung Kanparl für die Kommissionen» erlassen, in der die Vorgehensweise zur Aufnahme von Kommissionssitzungen verbindlich festgelegt wird.

Die im Prozess der Vorabkontrolle transparent herausgearbeitete Funktionsweise von Kanparl führte zu einer neuen Risikoanalyse und einer Neubewertung der Restrisiken. Bei der Darlegung der Restrisiken verwies die FADS, insb. mit Blick auf die noch nicht vollständig erfüllten WCC-Anforderungen, darauf, dass nur Massnahmen, die zum Zeitpunkt der Inbetriebnahme der Applikation umgesetzt sind, auch risikomindernd wirken können. Künftig geplante Umsetzungen haben keinen positiven Einfluss auf das Restrisiko, welches zum Zeitpunkt der Inbetrieb-

nahme besteht. Das Ratssekretariat hat in der Folge zugesichert, die Applikation erst für Kommissionssitzungen zu nutzen, wenn die noch offene Umsetzung der WCC-Anforderungen abgeschlossen ist.

ML-basierter Suchassistent EMF
Der Einsatz von generativer KI in der Stadt Bern wurde im Berichtsjahr anhand eines Proof of Concept-Vorhabens getestet und evaluiert. Dabei wurde ein virtueller Suchassistent der Einwohnerdienste, Migration und Fremdenpolizei (EMF) der Stadt Bern getestet. Die FADS wurde frühzeitig einbezogen, gemeinsam wurden die Art der Datenbearbeitung während der PoC-Phase und die rechtlichen Kriterien zum datenschutzkonformen Einsatz erörtert.

Ein virtueller Suchassistent soll den Mitarbeitenden im EMF auf fachliche Fragestellungen schnell und automatisiert Antworten zur Verfügung stellen. Nebst der erhofften kürzeren Dauer, die zur korrekten Informationssuche aufgewendet werden muss, soll auch die Qualität der Antworten erhöht werden. Im Rahmen des PoC-Vorhabens wurden ein kommerzielles Sprachmodell eines grossen Anbieters und ein Open Source-LLM evaluiert und in den Kriterien «Nutzenden-Akzeptanz», «Wirtschaftlichkeit», «Rechtliche Aspekte», «Technische Aspekte» und «Ethische Aspekte» bewertet. Im Austausch mit den Projektverantwortlichen riet die FADS dazu, für die Beurteilung der rechtlichen Aspekte die Anforderungen der Weisung Cloud Computing der Stadt Bern zu berücksichtigen. Beim kommerziellen Sprachmodell ist dies zwingend der Fall, das OSS-Modell könnte grundsätzlich auch im Rechenzentrum der Stadt Bern betrieben werden, wodurch die WCC-Anforderungen nicht anwendbar wären. Die Frage des Hostings der Lösung ist somit auch Bestandteil der Bewertung der rechtlichen Aspekte.

Im Austausch mit den Projektverantwortlichen konnte der FADS glaubhaft dargelegt werden, dass sich für die PoC-Phase keine personenbezogenen Daten aus der Stadt Bern in den Trainingsdaten des jeweiligen Sprachmodelles befinden. Als Basis der Resultatermittlung dienen Rechtstexte und interne Anleitungen, aus denen allfällige vorhandene Personendaten entfernt wurden. Auch ist nach der auf maximal sechs Monate befristeten PoC-Phase ein kompletter Rückbau der temporär genutzten Infrastrukturen und die Löschung aller dabei angefallenen Daten geplant.

Rückbau nach Abschluss des Tests geplant

Die FADS kam daher zum Schluss, dass mit diesem PoC-Vorhaben der Einsatz von generativer KI in der Stadt Bern datenschutzkonform getestet wird. Dass so allfällige Risiken bereits in der Evaluationsphase zu Tage treten und in die Gesamtbeurteilung einfliessen, begrüsst die FADS ausserordentlich. Der abschliessende Evaluationsbericht lag im Berichtsjahr noch nicht vor.

5

In eigener Sache: Neue Fallführungssoftware für OS und FADS

Die FADS und die Ombudsstelle der Stadt Bern (OS) konnte im Berichtsjahr die Vorbereitungsarbeiten zur angekündigten Einführung der neuen Fallführungssoftware abschliessen. Wie die Verwaltungsstellen der Stadt Bern haben sie dafür den ISDS-Prozess durchlaufen.

Für die beiden Dienststellen war bereits zu Beginn des Projekts klar, dass bei der neuen Fallführungssoftware auf eine Lösung mit einem externen Hoster gesetzt werden soll (vgl. dazu auch Tätigkeitsbericht OS/DSA 2022 S. 4 und Tätigkeitsbericht 2023 S. 7). Sowohl die OS, welche sich im Rahmen ihrer Ombudstätigkeit und als Wistleblowing-Meldestelle mit heiklen Fällen beschäftigt, als auch die FADS als Aufsichtsorgan über die städtischen Verwaltungsstellen, stuften es als wichtig ein, dass die von ihnen bearbeiteten Informationen zur Wahrung ihrer Unabhängigkeit nicht auf Servern der Stadtverwaltung gespeichert werden. Als Kleinststellen verfügen sie jedoch nicht über die Ressourcen, um die notwendigen Datenserver selbst auf sichere Weise zu betreiben. Entsprechend fiel die Wahl auf ein Schweizer Produkt, das auf der Infrastruktur einer Schweizer Anbieterin in der Schweiz betrieben wird.

Von der städtischen Infrastruktur unabhängige Lösung für die Fallführung

Wie jede Auslagerung von Datenbearbeitungen birgt aber auch diese Lösung eigene Risiken, welchen die OS und die FADS in den Vorbereitungsarbeiten besondere Beachtung schenken mussten. Aber auch unabhängig davon war es beiden Stellen ein Anliegen, das Vorhaben mit höchster Sorgfalt zu planen und umzusetzen. So zeigte auch die durchgeführte Schutzbedarfsanalyse klar, dass beide Stellen mit Daten mit erhöhtem Schutzbedarf arbeiten, wodurch zusätzliche Vorgaben an die Daten- und Informationssicherheit einzuhalten sind.

Daher haben die Stellen eine detaillierte Risikoanalyse durchgeführt und ein ISDS-Konzept erstellt. Ein Fokus lag hier bei der Einhaltung der Städtischen Weisung Cloud Computing. Zudem wurden die in der Risikoanalyse eruierten Restrisiken noch einmal eingehend separat diskutiert und durch die Leiterinnen der FADS und der OS explizit übernommen. Im Anschluss wurden die ISDS-Unterlagen der Datenschutzaufsichtsstelle des Kantons Bern (DSA) eingereicht, welche sich verdankenswerterweise dazu bereit erklärt hat, das Vorhaben einer Vorabkontrolle zu unterziehen.

Neuer Blickwinkel auf den ISDS-Prozess für die FADS

Einmal mehr hat sich gezeigt, dass die Vorabkontrolle einen wichtigen Beitrag zur Verbesserung von Informations- und Datenschutz leisten kann. So beinhaltete die erste Rückmeldung der DSA Befunde, welche von der OS und der FADS für einen sicheren Betrieb der neuen Fallführungssoftware dringend bereinigt werden mussten. Die beiden Stellen nahmen diese Arbeiten umgehend an die Hand und überarbeiteten die ISDS-Unterlagen dementsprechend. Die erneute Überprüfung der überarbeiteten Unterlagen ergab in der Folge keine wesentlichen Befunde mehr, so dass die Vorabkontrolle mit einem positiven Ergebnis abgeschlossen werden konnte.

Für die FADS war das Durchlaufen des ISDS-Prozesses in zweierlei Hinsicht gewinnbringend. Einerseits konnte mit der sorgfältigen Erarbeitung der ISDS-Unterlagen und der anschliessenden unabhängigen Prüfung durch die DSA das Sicherheitsniveau erhöht und sichergestellt werden, dass das Vorhaben auch mit Blick auf die besonderen Vorgaben zur Informations- und Datensicherheit korrekt geplant wurde. Andererseits gab dies der FADS die Gelegenheit, den Prozess aus dem Blickwinkel der für die geplante Datenbearbeitung verantwortlichen Behörde kennen zu lernen. Daraus konnte sie wesentliche Erkenntnisse für die Durchführung ihrer eigenen Vorabkontrollen gewinnen.

6

Statistik

Die Zahl der bearbeiteten Dossiers hat im Berichtsjahr zugenommen. So wurde insbesondere das Beratungsangebot der FADS durch die Stadtverwaltung vermehrt in Anspruch genommen. Dabei standen Anliegen in Zusammenhang mit der Einführung neuer Applikationen im Vordergrund.

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

Im Berichtsjahr hat die Zahl der bearbeiteten Dossiers zugenommen, es wurden insgesamt 120 bearbeitet (Vorjahr 88). Von 28 aus dem Vorjahr übertragenen und 92 neu eröffneten Fällen sowie 31 eröffneten Anfragen konnten 127 abgeschlossen werden. 24 Fälle wurden zur Weiterverarbeitung auf das Folgejahr übertragen.

Die Anzahl der bearbeiteten Fälle hat gegenüber dem Vorjahr um rund 35% zugenommen. Die stärkste Zunahme ist bei den verwaltungsinternen Beratungen zu verzeichnen, welche von 45 im Vorjahr auf 76 im Berichtsjahr gestiegen sind. Hier war für die FADS auch der bei der IBE im Berichtsjahr vorangetriebene Ausbau bei der ICT-Security spürbar. So führte die FADS einerseits kaum mehr ISDS-Workshops durch (2 Workshops im Berichtsjahr im Vergleich zu 32 im Vorjahr), da Projektverantwortliche im städtischen ISDS-Prozess nun stärker durch die ICT-Sicherheit begleitet werden können. Andererseits hat die FADS diverse Beratungen zu Fragen durchgeführt, die im Rahmen dieses Prozesses aufgetaucht sind, oder sie hat dort erstellte ISDS-Unterlagen einem Review unterzogen (so z.B. 20 Reviews im Berichtsjahr, im Vorjahr 10).

Auch zugenommen hat die Anzahl der Vorabkontrollen. Während die Datenschutz-Aufsichtsstelle im Jahr 2023 15 Vorabkontrollen bearbeitet hat, waren es im Berichtsjahr 18, wobei ein Teil davon bereits im Vorjahr gestartet worden ist. Die FADS hat im Berichtsjahr

zudem zum ersten Mal eine ordentliche Kontrolle (Audit) einer bereits in Betrieb genommenen Applikation an die Hand genommen. Die Arbeiten dazu werden im laufenden Jahr weitergeführt.

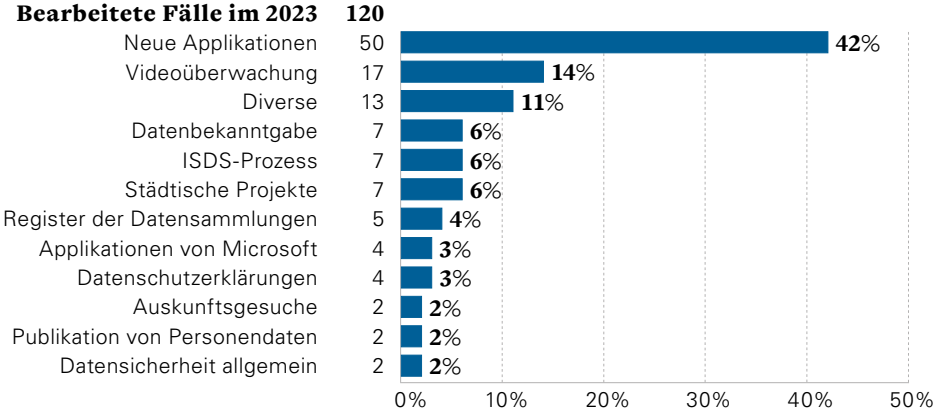
Abgenommen hat dagegen die Zahl der bearbeiteten Fälle von Privatpersonen, da im Berichtsjahr deutlich weniger aufsichtsrechtliche Anzeigen gegen die Stadtverwaltung eingegangen sind.

Kennzahlen Gesamtübersicht	2024	2023
Fälle	**120**	**88**
Fälle aus dem Vorjahr	28	18
Neu eröffnete Fälle	92	70
Anfragen	**31**	**46**
Total Fälle und Anfragen	**151**	**134**
Pendent per Ende Jahr	24	28

Kennzahlen bearbeitete Fälle	2024	2023
Bearbeitete Fälle von Privatpersonen	**12**	**14**
Beratung	8	7
Aufsichtsrechtliche Anzeigen	2	7
Auskunftsgesuche	2	0
Bearbeitete Fälle Verwaltung und Betriebe	**108**	**74**
Beratung	76	45
ISDS-Workshop	2	32
Review	20	10
Beratung im engeren Sinn	54	3
Nachträgliche Überprüfung	5	7
Vorabkontrolle	18	15
Audit	1	0
Formelle Stellungnahme	2	1
Führen Register der Datensammlung	5	1
Umsetzung Empfehlungen	1	1
Eigene Untersuchung	**0**	**4**

Einen Themenschwerpunkt bildeten im Berichtsjahr einmal mehr neue Applikationen. 42% der Fälle betrafen diesen Bereich; viele der dabei behandelten Applikationen befanden sich im Beratungszeitpunkt entweder im städtischen ISDS-Prozess oder in der Vorbereitung dazu. Separat erfasst wurden Beratungen in Zusammenhang mit Microsoft. Diese haben zwar im Vergleich zum Vorjahr abgenommen (4 im Berichtsjahr, im Vorjahr: 7), aber das Thema war noch immer aktuell. Ein Dauerbrenner bleibt das Thema Videoüberwachung, mit dem sich die FADS in 17 Fällen (Vorjahr: 15) beschäftigt hat. Sie hat dabei sowohl Vorabkontrollen als auch Beratungen durchgeführt.

Anteile der bearbeiteten Fälle pro Themenbereich



7

Einblick in die Praxis

Die FADS hat sich im Berichtsjahr mit einem bunten Strauss an Themen auseinandergesetzt. Der nachfolgende Einblick in die Praxis soll exemplarisch Fälle wiedergeben, in denen sich typische oder eben gerade aussergewöhnliche Fragen gestellt haben und damit einen Einblick in den Arbeitsalltag der FADS vermitteln. Er ist nach Themenbereichen geordnet.

Neue Applikationen

Pilotprojekt zur digitalen Mitwirkung bei Bauvorhaben

Mit der Applikation Konova soll die digitale Mitwirkung und Partizipation von Bürger*innen der Stadt Bern ermöglicht werden. Dabei wird unterschieden zwischen der informellen Mitwirkung und der gesetzlich verordneten, formellen Mitwirkung (z.B. öffentliche Auflage von Planungsvorhaben). Für den im Tiefbauamt geplanten Pilotbetrieb konnte im Berichtsjahr die Vorabkontrolle abgeschlossen werden.

Eine erste Fassung der ISDS-Dokumente zu Konova wurde der FADS vom Tiefbauamt (TAB) bereits im Spätsommer 2022 zur Vorabkontrolle zugestellt. Per Ende November stellte die FADS dem TAB einen Vorabkontrollbericht mit gesamthaft 61 Befunden zu. Davon wurden 45 mit hoher Wesentlichkeit gewichtet, was bedeutet, dass diese zwingend vor einer datenschutzkonformen Nutzung von Konova zu bereinigen sind. Inhaltliche Schwerpunkte waren dabei die potenzielle Bearbeitung von besonders schützenswerten Personendaten im Rahmen von Stellungnahmen zu Planungsvorhaben und, daraus folgend, die Einstufung des Schutzbedarfes durch das TAB. Weiter war für die FADS der Standort der Datenbearbeitung zu unklar beschrieben. Da es sich um eine SaaS-Lösung handelt und der Anbieter mit unterschiedlichen Subunternehmern zusammenarbeitet, musste Transparenz im ISDS-Konzept wie auch in den Verträgen geschafft werden zur Frage, wer zu welchem Zweck wo welche personenbezogenen Daten bearbeitet. Auch die Beschreibung des Registrationsprozesses für Teilnehmende an formellen Mitwirkungen war aus datenschutzrechtlicher Sicht ungenügend.

Die Befunde wurden in der Folge vom TAB bearbeitet, was zu offenen Fragen führte, welche FADS und TAB im Sommer 2023 miteinander besprachen. Dabei konnten einige Befunde erledigt resp. deren Erledigung vereinbart werden. So wurde beispielsweise mehr Transparenz in der Frage der Unterauftragsnehmer der Herstellerfirma geschaffen und vereinbart, auf zwei standardmässig in die Auftragsdatenverarbeitung involvierte US-Unternehmen zu verzichten.

Ferner wurde das TAB auch auf die per 15. August 2023 in Kraft getretene Weisung Cloud Computing (WCC) hingewiesen. Diese ist auf Konova anwendbar, und entsprechend sind die Sicherheitsanforderungen gemäss Anhang 2 WCC zu erfüllen. Die Deklaration der Anforderungen aus der WCC brachte zum Vorschein, dass die aus Sicht Datenschutz wichtigen Anforderungen der WCC durch die Herstellerin nicht vollständig erfüllt wurden. Das sich daraus ergebende Risiko wird zwar in der Risikoanalyse behandelt, die zur Risikosenkung ergriffenen alternativen Massnahmen sind aus Sicht der FADS jedoch nicht gleichwertig. Dies hat die FADS dazu veranlasst den Befund zwar auf «mittel» herabzustufen, aber das TAB darauf hinzuweisen, dass mittelfristig mit dem Hersteller der Applikation eine Lösung gesucht werden muss, um die WCC-Anforderung vollumfänglich zu erfüllen.

Verzicht auf US-amerikanische Unterauftragsbearbeiter

Nach zwei weiteren Besprechungen zu aktualisierten ISDS-Dokumenten und erledigten Befunden verblieben noch vier offene Befunde mit hoher Gewichtung. Zur Klärung dieser Punkte fand im Frühling 2024 ein Austausch zwischen dem TAB, der FADS und einem Vertreter der Herstellerfirma statt. Da in der Folge lediglich drei befunde mit mittlerer Wesentlichkeit verblieben, konnte die Vorabkontrolle abgeschlossen werden. Das TAB wurde jedoch dazu aufgefordert, die Behebung der noch offenen Befunde mit mittlerer Wesentlichkeit bei nächster Gelegenheit anzugehen.

Meldeplattform der Whistleblowing-Meldestelle

Die Ombudsfrau gelangte an die FADS, um die Pflicht zur Vorabkontrolle der beschafften Whistleblowing-Meldeplattform prüfen zu lassen. Da nicht ausgeschlossen werden kann, dass über die Plattform besonders schützenswerte Personendaten bearbeitet werden, entschied sich die FADS, die Applikation einer Vorabkontrolle zu unterziehen.

Die Meldeplattform besteht aus einem öffentlich zugänglichen Formular und einem Cockpit für die Mitarbeitenden der Whistleblowing-Meldestelle. Die meldende Person erhält beim Absenden des Online-Meldeformulars die Zugangsdaten für den Zugriff auf ein persönliches Postfach. Die Authentifizierung geschieht dabei zweistufig mit PIN und Passwort. Die Kontaktaufnahme der Whistleblowing-Meldestelle mit der meldenden Person geschieht über das persönliche Postfach, wobei es in der Verantwortung der meldenden Person ist, regelmässig zu prüfen, ob eine neue Nachricht eingegangen ist. Die meldende Person kann bei der Meldung des potenziellen Missstandes selbst entscheiden, ob sie anonym bleiben will oder Angaben zu ihrer Person im Freitextfeld machen möchte.

Nach Angaben des Herstellers ist aus technischer Sicht die Anonymität gewährleistet, da keine IP-Adressen und auch keine weiteren personenbezogenen Metadaten der meldenden Person gespeichert werden. Allerdings kann nicht ausgeschlossen werden, dass personenbezogene Informationen im Freitextfeld des Meldeformulars eingegeben werden und folglich eine Bearbeitung von sonders schützenswerten Personendaten stattfindet.

Bereits im Jahr 2023 führte die FADS mit der Ombudsfrau daher einen ISDS-Workshop mit Blick auf die zu erstellenden ISDS-Unterlagen durch. Im Anschluss daran waren verschiedene Fragen technischer und rechtlicher Art mit der Herstellerfirma zu klären. Die FADS unterstützte die Ombudsfrau dabei und stand bei der Erarbeitung der ISDS-Dokumentation beratend zur Seite. Zu Beginn des Berichtsjahres wurde der FADS eine erste Fassung der finalisierten ISDS-Dokumente zur Vorabkontrolle unterbreitet.

Verbesserte Sicherheit dank Zweifaktor-Authentifizierung

Darin waren in Bezug auf die Einhaltung der Anforderungen der städtischen Weisung Cloud Computing noch nicht sämtliche Punkte restlos geklärt. Daher fand nebst einer weiteren Besprechung mit der Ombudsfrau im März des Berichtsjahres ein Austausch zwischen Vertreter*innen der Herstellerfirma, der Ombudsfrau und der FADS statt, an der die offenen Fragen besprochen werden konnten. Dabei wurde vereinbart, den Zugriff der Mitarbeitenden der Whistleblowing-Meldestelle auf das Cockpit mit einem zweiten Faktor abzusichern und die Passwort-Komplexität für die Cockpit-Userinnen den Vorgaben der städtischen ICT-Sicherheit anzugleichen. Auch die Verschlüsselung von data-at-Rest und data-in-transit sowie die Sicherheit der Webapplikation konnten durch den Hersteller mit entsprechender Dokumentation glaubhaft belegt werden.

Mit diesen Informationen wurden die ISDS-Dokumente aktualisiert und der FADS erneut zur Vorabkontrolle eingereicht. Der abschliessende Prüfbericht beinhaltet keine Befunde mit hoher Wesentlichkeit, weshalb die FADS zum Schluss gelangte, dass die Meldeplattform grundsätzlich den datenschutzrechtlichen Anforderungen der Stadt Bern genügt.

Fachapplikation Friedhofsverwaltung

Die Fachapplikation mpsFIM wird seit mehreren Jahren im Bereich Friedhöfe von Stadtgrün Bern zur Bearbeitung der Todesfälle, der Kremationen und Bestattungen sowie dem Unterhalt und der Pflege der Grabstätten und deren Verwaltung eingesetzt.

Da darin besonders schützenswerte Personendaten bearbeitet werden und viele Nutzende darauf Zugriff haben resp. über Schnittstellen Personendaten mit der Einwohnerkontrolldatenbank und SAP (Rechnungswesen) ausgetauscht werden, hat die FADS zunächst entschieden, die Applikation FIM nachträglich zu überprüfen.

Nach einer ersten Kontaktaufnahme seitens Stadtgrün Bern wurde klar, dass ein grösserer Releasewechsel der Applikation geplant war und es wurde vereinbart, für diesen eine Vorabkontrolle durchzuführen. Mit dem neuen Release stand eine

wesentliche Änderung einer Datenbearbeitung bevor, womit die Durchführung einer Vorabkontrolle gestützt auf Art. 17a Abs. 2 KDSG gerechtfertigt war, obschon die Applikation bereits in Betrieb ist.

Releasewechsel rechtfertigt Vorabkontrolle

Nach einem ISDS-Workshop in Zusammenarbeit mit dem ICT-Sicherheitsbeauftragten der Stadt Bern und den Verantwortlichen von Stadtgrün Bern wurden die erforderlichen ISDS-Dokumente erarbeitet und der FADS zur Prüfung unterbreitet.

Gestützt darauf wurde eine erste Berichtsversion verfasst und der datenbearbeitenden Behörde zugestellt. In der dazugehörigen Befundliste lagen einige Befunde mit hoher Wesentlichkeit vor. Diese betrafen nicht in erster Linie die Applikation an sich, sondern die Dokumentation einzelner Aspekte wie die Beschreibung der bearbeiteten Personendaten, der anwendbaren Rechtsgrundlagen, der Datenflüsse, der Schnittstellen und Weiteres mehr. Die FADS kam deshalb zum Schluss, dass die ISDS-Unterlagen die geplante Datenbearbeitung noch nicht in genügender Weise dokumentieren und daher überarbeitet werden müssen.

Die offenen Befunde wurden von Stadtgrün Bern in der Folge bearbeitet. Zur Besprechung der Befundliste und zur Klärung offener Fragen erfolgten zwei Austausche zwischen Stadtgrün Bern, dem Informatikkoordinator der zuständigen Direktion und der FADS. In der Folge wurden der FADS die finalisierten ISDS-Dokumente eingereicht. Nach deren Prüfung verfasste die FADS die zweite Berichtsversion. Im Ergebnis lag noch ein Befund mit mittlerer Wesentlichkeit zu einem Aspekt der Informatikarchitektur vor. Die FADS konnte deshalb festhalten, dass der geprüfte Gegenstand den datenschutzrechtlichen Anforderungen der Stadt Bern im Grundsatz entspricht. Stadtgrün Bern wurde aufgefordert, die Behebung des noch offenen Befunds mit mittlerer Wesentlichkeit bei nächster Gelegenheit anzugehen.

Saas-Lösung zur Bewirtschaftung von Hypothekarkrediten

Die bisherige, im städtischen Rechenzentrum betriebene Applikation zur Bewirtschaftung der Hypothekarkredite der Personalvorsorgekasse der Stadt Bern (PVK) wurde nicht mehr weiterentwickelt und musste daher abgelöst werden. Das neu zu beschaffende System wurde von einer Kantonalbank entwickelt und wird als SaaS-Lösung in deren Rechenzentren betrieben.

Bei der PVK handelt es sich um eine öffentlich-rechtliche Anstalt der Stadt Bern; als solche untersteht sie der kantonalen Datenschutzgesetzgebung. Im Rahmen einer Vorbesprechung konnte sich die FADS bereits beratend zu den vertraglichen Vorgaben sowie zur Anwendung der städtischen Weisung Cloud Computing (WCC) äussern.

Der FADS wurden in der Folge die ISDS-Unterlagen über die ICT-Sicherheit zur Vorabkontrolle unterbreitet. Nach einer ersten Sichtung ergaben sich von Seiten FADS Fragen vorab in Bezug auf den Nachweis der Erfüllung der WCC sowie in Bezug auf die Risikoanalyse, welche durch den ISDS-Verantwortlichen des Projekts mit der Herstellerin geklärt werden mussten. Die offenen Fragen wurden dem

ISDS-Verantwortlichen des Projekts im Rahmen einer Themenliste unterbreitet.

Die Ergebnisse dieser Rücksprachen flossen in die neuen Fassungen der ISDS-Dokumente, welche der FADS eingereicht und anlässlich eines weiteren Austausches besprochen wurden.

Bis auf eine Ausnahme wurden die offenen Punkte in den finalen Fassungen der ISDS-Dokumente bereinigt. Einzig verbleibender Punkt war eine nichterfüllte Anforderung der WCC. Das sich daraus ergebende Risiko wurde in der Risikoanalyse behandelt. Als risikomindernde Massnahme wurde generell auf getroffene Massnahmen zum Schutz vor Cyber-Risiken verwiesen und das Risiko damit auf ein aus Sicht PVK vertretbares Mass gesenkt. Zusätzlicher Handlungsbedarf wurde dabei nicht ausgewiesen.

Anbieterin muss bei Einhaltung WCC nachbessern

Für die FADS war grundsätzlich nachvollziehbar, dass die Kantonalbank als Anbieterin von der Bankenaufsicht unterstellten Dienstleistungen erhöhten Anforderungen an die Informatiksicherheit unterstehen dürfte. Mangels näherer Kenntnis der entsprechenden technischen und organisatorischen Massnahmen konnte die FADS deren risikomindernde Wirkung aber nicht vollumfänglich nachvollziehen. Die FADS riet daher der PVK, bei der Kantonalbank auf die Erfüllung der nicht berücksichtigten Vorgabe der WCC hinzuwirken. Dieser Befund wurde mit mittlerer Wesentlichkeit gewichtet und stand der Produktivsetzung der Applikation daher nicht entgegen.

Städtische Projekte

Microsoft 365 und Neue Digitale Zusammenarbeit

Die FADS hat sich auch im Berichtsjahr mit Microsoft 365 beschäftigt. Sie konnte die Vorabkontrolle für dessen Einsatz in der Stadtverwaltung abschliessen und hat sich im Folgenden mit Fragen zur konkreten Nutzung auseinandergesetzt. Bei der weitergeführten Vorabkontrolle zu base4kids2 war die Implementierung von Microsoft 365 in der Schulinformatik ebenfalls ein Schwerpunktthema.

Am 5. Juli 2023 hat der Stadtrat beschlossen, dass die mit dem Betrieb von Microsoft 365 verbundenen Restrisiken getragen werden können und dass er dessen Nutzung in der Stadtverwaltung, unter Einhaltung gewisser Vorgaben, freigibt (vgl. Tätigkeitsbericht 2023 S. 11). In der anschliessend durchgeführten Vorabkontrolle hat die FADS am 19. Juli 2023 der verantwortlichen Behörde einen ersten Prüfbericht zugestellt. Darin hielt sie fest, dass ein datenschutzkonformer Betrieb von Microsoft 365 noch nicht sichergestellt ist, dass im Programm nachgebessert und die ISDS-Unterlagen überarbeitet werden müssen. Im daraufhin durchgeführten intensiven Austausch zwischen dem Programm, der ICT-Security und der FADS konnte ein grosser Teil der im Bericht aufgeführten Befunde bereinigt werden. Einige der von der FADS in ihrem Prüfbericht neu verorteten Restrisiken wurden zudem einem gemeinderätlichen Ausschuss zur Kenntnis gebracht. Am 31. Oktober 2023 wurden der FADS die überarbeiteten ISDS-Dokumente zur erneuten Vorabkontrolle unterbreitet. Aufgrund einer ersten informellen Rückmeldung sowie weiterer Besprechungen wurden diese noch einmal

angepasst resp. ergänzt und der FADS am 22. Januar 2024 eingereicht. Nach einer Prüfung dieser Unterlagen hat die FADS dem Programm am 1. Februar 2024 ihren finalen Vorabkontrollbericht zugestellt.

Die FADS verlangte im Vorabkontrollverfahren sowie bereits im Rahmen der vorgelagerten Beratungstätigkeit wiederholt einen angemessenen Umgang mit den mit dem Betrieb von Microsoft 365 verbundenen Risiken. Sie hat das Programm dazu aufgefordert, eine Risikoanalyse gemäss den Vorgaben der städtischen Informatiksicherheit durchzuführen, die daraus abzuleitenden Massnahmen zu prüfen und umzusetzen. In ihrem Abschlussbericht ist die FADS zum Schluss gekommen, dass das Programm seine Risikoanalyse grundlegend überarbeitet und diverse technische und organisatorische Massnahmen eingeführt hat, um die verorteten Risiken zu senken. So wurden z.B. mit der Umsetzung der sog. CIS-Benchmarks anerkannte Best Practices eingeführt, welche den Datenschutz und die Informationssicherheit deutlich verbessern. Mit dem Abschluss zusätzlicher vertraglicher Garantien wurde Microsoft hinsichtlich einer gesetzeskonformen Bearbeitung der städtischen Daten besser in die Pflicht genommen, und mit dem Erlass der Weisung Cloud Computing und der Klassifizierungsweisung verfügt die Stadt nun auch weit über das Programm Microsoft 365 (resp. dem darauf aufbauenden Programm NDZ) hinaus über Vorgaben für die städtischen Mitarbeitenden.

Die FADS hat aber auch festgestellt, dass trotz dieser Massnahmen diverse Restrisiken bestehen, für welche die zuständigen Gemeindeorgane die Verantwortung tragen, womit ein laufendes sorgfältiges Risikomanagement für einen datenschutzkonformen Betrieb essenziell ist. Zudem hat sie auf den dringenden Handlungsbedarf im Bereich Machine Learning (ML) und KI hingewiesen, und zwar nicht nur in Bezug auf Microsoft 365. Sie hat gefordert, dass eine Grundstrategie und daraus folgende Regulierungsmassnahmen (z.B. Weisungen) erlassen werden und die Nutzer*innen entsprechend geschult werden, um sicherzustellen, dass diese Technologie in der Stadt Bern datenschutzkonform eingesetzt wird. Beides wurde vom Programm zugesichert.

Dringender Handlungsbedarf bei KI und Machine Learning

Im Berichtsjahr hat sich gezeigt, dass die korrekte Nutzung der IT-Infrastruktur seit der Einführung von Microsoft 365 für die Mitarbeitenden der Stadtverwaltung anspruchsvoller geworden ist. Der vom Gemeinderat in seinem Risikoentscheid vom 5. Juli 2023 vorgegebene hybride Ansatz (Nutzung von Microsoft 365 nur für die Bürokommunikation, die systematische Bearbeitung besonders schützenswerter Personendaten oder geheimnisgeschützter Informationen dagegen in Fachapplikationen, welche höheren Sicherheitsanforderungen genügen müssen) wurde zwar umgesetzt und es besteht nach wie vor die Möglichkeit, Daten ausschliesslich lokal resp. in den dafür vorgesehenen Fachapplikationen zu bearbeiten. Ausserdem wurden mit Microsoft 365 auch diverse Schulungsangebote eingeführt, welche die Nutzer*innen zum korrekten Umgang mit den neuen Arbeitsmitteln befähigen sollen.

Die Nutzung der in Microsoft 365 enthaltenen Cloud-Komponenten ist für Informationen mit erhöhtem Schutzbedarf jedoch kaum durch technische

Massnahmen eingeschränkt, so dass es in erster Linie in der Verantwortung der Nutzer*innen liegt, die organisatorischen Vorgaben für einen datenschutzkonformen Betrieb einzuhalten. Dabei legt die Klassifizierungsweisung zwar verbindlich fest, dass und wie Informationen zu klassifizieren sind. Die Regelungen sind dabei aber naturgemäss sehr allgemein gehalten, und die sich daraus ergebenden Vorgaben für die Bearbeitung in der Microsoft 365-Welt weisen einen erheblichen Interpretationsspielraum auf. Der Umstand, dass Microsoft laufend und ohne Ankündigung für die Nutzenden neue Funktionen einführt, welche vermehrt ML/KI-Komponenten aufweisen, erschwert eine korrekte Nutzung und das Risikomanagement im laufenden Betrieb zusätzlich.

Die FADS beobachtet daher die Entwicklungen und ist auch nach Abschluss der Vorabkontrolle im Austausch mit den Programmverantwortlichen, um den datenschutzkonformen Umgang mit Personendaten auch im laufenden Betrieb einzufordern und allfälligen Anpassungsbedarf frühzeitig zu adressieren.

Vorabkontrolle der Schulinformatik-Plattform base4kids2

Digital Stadt Bern und das Schulamt kontaktierten die FADS zwecks Vorabkontrolle der Schulinformatik-Plattform base4kids2, bei der ein Grossteil der eingesetzten OpenSource-Komponenten abgebaut und mit Microsoft 365 Lösungen ersetzt werden. Auch wird ein Wechsel der Betriebsverantwortung vorgenommen.

Bereits im Jahr 2023 fand ein erster Austausch zwischen der Programmleitung Neue digitale Zusammenarbeit (NDZ), der IBE, der ICT-Security und der FADS mit Blick auf die Finalisierung der neu erarbeiteten ISDS-Dokumente statt. Die ISDS-Dokumente zu Microsoft 365 in der Stadtverwaltung konnten grundsätzlich als Basis für base4kids2 dienen. Die FADS verlangte jedoch, dass in den ISDS-Dokumenten zu base4kids2 die Unterschiede in der Datenbearbeitung und die daraus resultierenden neuen Risiken zur bereits eingeführten Datenbearbeitung mit Microsoft 365 in der Stadtverwaltung herauszuarbeiten und die zusätzlichen, in der Plattform eingesetzten Komponenten (wie bspw. Nextcloud und Apple School Manager) zu behandeln sind.

Im Mai 2023 wurde der FADS eine erste Version des ISDS-Konzeptes eingereicht. Nach erfolgter summarischer Prüfung stellte die FADS der Programmleitung NDZ per Ende Mai 2023 eine Befundliste mit gesamthaft 57 Befunden zu. An einer darauffolgenden Besprechung zwischen dem Schulamt, IBE und der ICT-Security wurden die offenen Punkte und das weitere Vorgehen im Hinblick auf die Vorabkontrolle besprochen. Gestützt darauf wurden vom Schulamt die ISDS-Dokumente überarbeitet und Anfangs September 2023 via Compliance Check Tool zur Vorabkontrolle unterbreitet.

Die Prüfung dieser Dokumente wurden im Oktober 2023 mit einem Vorabkontrollbericht abgeschlossen, in dem insgesamt 29 Befunde, davon 24 mit hoher Wesentlichkeit, festgestellt wurden. Die FADS hielt im Bericht fest, dass ein datenschutzkonformer Betrieb damit noch nicht gewährleistet sei und forderte das Schulamt auf, die in den Befunden festgehaltenen Folgeaktivitäten umzusetzen und die ISDS-Dokumente entsprechend nachzuführen. Hauptpunkte waren dabei die Abgrenzung zu Microsoft 365 in der Stadtverwaltung, die Zusammenarbeit mit externen Partnern und, damit einhergehend, allfällige Auftragsdatenverarbeitungen, die Bearbeitung von besonders schützens-

werten Personendaten sowie die Datenbearbeitung durch Apple (School Manager und iPads) innerhalb der Plattform.

Unterschiede zur Stadtverwaltung sind auszuweisen

Überarbeitete ISDS-Dokumente wurden der FADS anschliessend Ende März des Berichtsjahres eingereicht. Die Prüfung der aktualisierten Unterlagen ergab, dass einige Befunde erledigt werden konnten. Da jedoch nach wie vor offene Befunde mit hoher Gewichtung bestanden, und weil sich aus dem neu eingereichten Rollen- und Berechtigungskonzept zusätzliche Befunde ergaben, wurden die verbleibenden sowie die neuen Befunde mit dem Schulamt im Hinblick auf deren Erledigung nochmals besprochen. Daraufhin wurden der FADS ein neues Backup-Konzept Microsoft 365, überarbeitete Nutzungsbedingungen für die base4kids2-Services und die Nutzungsbedingungen für die Geräte sowie neue Versionen des ISDS-Konzepts, der Risikoanalyse und des Rollen- und Berechtigungskonzepts unterbreitet.

Damit konnten von den insgesamt 40 offenen Befunden deren 19 geschlossen werden. Zur Bereinigung der verbleibenden Befunde wurde dem Schulamt die entsprechend nachgeführte Befundliste zugestellt. Inhaltlich ging es dabei hauptsächlich um die innerhalb von Microsoft 365 eingesetzten Services und die Umsetzung der sog. CIS-Benchmarks zu Microsoft 365 und Apple. Die Umsetzung dieser Best Practices zur sicheren Konfiguration von IT-Systemen sollten, wie bereits bei der Einführung von Microsoft 365 in der Stadtverwaltung, auch für die Schulinformatik transparent dargelegt werden und in das Risikomanagement einfliessen. Dabei stand auch die Frage im Raum, inwiefern die in Bezug auf Microsoft 365 anfallenden Restrisiken bei b4k2 bereits im Beschluss vom 5. Juli 2023 des Gemeinderates enthalten waren[3]. Weiterhin offen und aus datenschutzrechtlicher Sicht von grosser Bedeutung war auch die Frage der Bearbeitung von besonders schützenswerten Personendaten innerhalb der Plattform.

Die nochmals aktualisierten ISDS-Unterlagen wurden der FADS Anfangs November 2024 über das Compliance Check Tool eingereicht. Die daran anschliessende Vorabkontrolle konnte im Berichtsjahr noch nicht abgeschlossen werden.

Videoüberwachung

Merkblatt Videomonitoring Verkehrsanalyse

Nachdem im Vorjahr die Einordnung von Videoaufnahmen zur Verkehrsanalyse in grundsätzlicher Hinsicht geklärt werden konnte, gelangte die Verkehrsplanung im Berichtsjahr mit einem Entwurf für ein Merkblatt Videomonitoring Verkehrsanalyse sowie einer ersten konkreten Anwendung an die FADS.

Im Tätigkeitsbericht 2023 wurde über den Einsatz von Videokameras für das Verkehrsmonitoring durch die Abteilung Verkehrsplanung der Direktion für Tiefbau, Verkehr und Stadtgrün in allgemeiner Hinsicht berichtet (S. 20). Es konnte geklärt werden, dass aufgrund des nicht personenbezogenen Bearbei-

3 Zur Diskussion des Beschlusses aus datenschutzrechtlicher Sicht siehe Tätigkeitsbericht 2023 (S. 11 f.).

tungszwecks keine Videoüberwachung im Sinne des kantonalen Polizeigesetzes und des städtischen Videoreglements vorliegt. Im Weiteren wurde vereinbart, ein Merkblatt zu erarbeiten und die Datenbearbeitung im Rahmen eines konkreten Monitoring-Vorhabens zu beurteilen.

Erkennbarkeit von Personen kann nicht ausgeschlossen werden

Die FADS prüfte das Merkblatt und konnte einige Vorschläge und Hinweise zur rechtlichen Einordnung anbringen. Im Kern stand dabei die Feststellung, dass trotz nicht personenbezogenem Bearbeitungszweck nicht ausgeschlossen werden konnte, dass in Einzelfällen bestimmte Personen oder Kontrollschilder von Fahrzeugen erkennbar sein könnten. Aus diesem Grund wurde im Merkblatt ausdrücklich auf das sog. Forschungsprivileg verwiesen. Demnach ist nach Art. 15 Abs. 1 KDSG die Datenbearbeitung zu einem nicht personenbezogenen Zweck wie Forschung, Statistik oder Planung zulässig, wenn sichergestellt ist, dass a) die Personendaten, sobald es der Bearbeitungszweck erlaubt, anonymisiert werden und b) die Ergebnisse der Bearbeitung nur so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind. Das Merkblatt richtet sich an die mit den jeweiligen Vorhaben beauftragten Ingenieurbüros und stellt Vorgaben und Auflagen technischer und organisatorischer Art für die Einhaltung der gesetzlichen Vorgaben auf. Es bildet zudem integrierenden Bestandteil der vertraglichen Vereinbarungen.

Das Merkblatt konnte beim Monitoring eines Pilotversuchs im Rahmen des Projektes «Velohauptroute Bern-Bethlehem-Brünnen» auf der Stöckackerstrasse erprobt werden. Die darin gewonnenen Erkenntnisse wurden bei der Weiterentwicklung des Dokuments berücksichtigt. Insbesondere wurde neu zur Einhaltung der Datenschutzauflagen und zur Dokumentation der technischen und organisatorischen Massnahmen auch eine unterschriftliche Bestätigung einverlangt.

Videomonitoring an einer öffentlich zugänglichen Liftanlage

Immobilien Stadt Bern erhielt von der Fachstelle für hindernisfreie Architektur eine Anfrage für ein Videomonitoring an einer öffentlich zugänglichen Liftanlage der Stadt Bern. Zweck des Videomonitorings bildete die Untersuchung der Türoffenhaltezeit, insbesondere für Menschen mit eingeschränkter Mobilität. Die FADS wurde um Beurteilung des Vorhabens aus Sicht Datenschutz ersucht.

Die FADS stellte fest, dass der Zweck der Datenbearbeitung nicht personenbezogen ist und auch nicht im polizeilichen Bereich liegt. Zudem war das Videomonitoring auf wenige Tage befristet. Damit lag keine nach kantonalem Polizeigesetz und städtischem Videoreglement bewilligungspflichtige Videoüberwachung vor.

Im Weiteren sollte das Vorhaben durch die Fachstelle hindernisfreie Architektur als privatrechtliche Behindertenorganisation durchgeführt werden. Diese stellt kein öffentliches Organ dar und ist keine Trägerin gesetzlicher Aufgaben. Ebenso wenig wurde das Vorhaben im Auftrag einer (städtischen) Behörde durchgeführt. Damit lag eine Datenbearbeitung durch eine private Verantwortliche vor, womit

das Datenschutzgesetz des Bundes (DSG) anwendbar und die Aufsichtszuständigkeit des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gegeben war.

Einhaltung des Datenschutzes durch private Akteure soll durch Stadt geprüft werden

Trotz dieser Rechtslage bestand ein Interesse der Stadt Bern, sich von der Einhaltung des Datenschutzes durch die Fachstelle zu überzeugen, bevor dem Vorhaben zugestimmt bzw. dieses geduldet wird. Die von der Fachstelle vorgelegte Selbstdeklaration gab Anlass zur Annahme, dass die allgemeinen Vorgaben des DSG sowie insbesondere auch diejenigen des sog. Forschungsprivilegs nach Art. 31 Abs. 2 Bst. e DSG (analoge Bestimmung zu derjenigen von Art. 15 KDSG) eingehalten werden. So war z.B. sicherzustellen, dass bei einer Publikation der Ergebnisse kein Personenbezug möglich ist; dass der Kameraperimeter auf den Zutrittsbereich der Liftanlage beschränkt ist; dass die Rohdaten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt; dass sämtliche Daten nach Projektende gelöscht werden; dass die Rechte der Betroffenen auf Einsicht, Berichtigung und Löschung gewährleistet werden; oder dass vor Ort innerhalb und ausserhalb des Kameraperimeters gut sichtbare Hinweisschilder angebracht werden. Die Fachstelle als Verantwortliche hatte überdies sicherzustellen, dass in Bezug auf die beauftragte Firma die Vorgaben für die Auftragsdatenbearbeitung nach Art. 9 DSG eingehalten werden.

Im Übrigen wurde zuhanden der Fachstelle auf die Webseite des EDÖB zur Videoüberwachung durch Private verwiesen.

Überwachung des öffentlichen Raums durch die Cuba Bar

Am 9. Februar 2024 entgleiste am Kornhausplatz in Bern ein Tram und kam vor der Cuba Bar zum Stehen. Der von einer privaten Videoüberwachungskamera aufgezeichnete Vorfall wurde auf der Facebook-Seite der Cuba Bar gepostet. In der Folge gingen bei der FADS aufsichtsrechtliche Anzeigen ein, welche die Frage nach der Zulässigkeit der (privaten) Videoüberwachung aufwarfen.

Zufolge der privaten Natur der Videoüberwachung lag die Aufsichtszuständigkeit beim EDÖB. Dies wurde den Anzeigenden mitgeteilt und sie gleichzeitig um eine Rückmeldung gebeten, ob die Anzeige durch die FADS an den EDÖB weitergeleitet werden soll. Davon machte lediglich eine der Anzeigenden Gebrauch.

Wie sich in der Folge zeigte, war die Überwachungskamera bereits am Tag nach der Tramentgleisung aufgrund einer Intervention des städtischen Bauinspektorats beim Betreiber der Cuba Bar entfernt worden. Auch dies wurde den Anzeigenden mitgeteilt. Für die FADS war die Angelegenheit damit erledigt.

Zum Thema Behandlung von privaten Videoüberwachungen im öffentlichen Raum als «Störung der öffentlichen Ordnung, die von sonst wie ordnungswidrigen Bauten und Anlagen ausgeht» im Sinne von Art. 45 Baugesetz (BauG; BSG 721.0) wurde im Tätigkeitsbericht OS/DSA 2020 ausführlich berichtet (S. 40 f.).

Datenbekanntgabe

Datenbekanntgabe bei Taggeldzahlungen

Taggeldzahlungen der SUVA und privater Unfallversicherer zuhanden städtischer Angestellter gingen bei der städtischen Finanzverwaltung zwecks Identifikation der Betroffenen jeweils unter Angabe der versicherten Person als Buchungstext ein. Bei Taggeldzahlungen der IV wird die betroffene Person jedoch nicht namentlich aufgeführt; zur Identifikation wird auf die AHV-Nummer abgestellt. Das Personalamt erkundigte sich bei der FADS, ob die Praxis bei den Unfalltaggeldzahlungen aus Sicht Datenschutz entsprechend anzupassen sei.

Die FADS konnte dazu Folgendes festhalten: Die Datenbekanntgabe durch die Unfallversicherer an die Arbeitgeberin richtet sich nach Art. 97 Bundesgesetz über die Unfallversicherung (UVG; SR 832.20). Nach dieser Bestimmung dürfen nur diejenigen Daten bekannt gegeben werden, welche für die Aufgabenerfüllung erforderlich sind. Die IV-Taggeldzahlungen der kantonalen Ausgleichskasse richten sich nach den einschlägigen Bestimmungen der Invaliden- bzw. Alters- und Hinterlassenengesetzgebung, welche inhaltlich identisch sind. Im Rahmen der Taggeldzahlungen an die Arbeitgeberin zugunsten der versicherten Person ist offensichtlich ein Merkmal erforderlich, welches die Zuordnung der Zahlung zur versicherten Person ermöglicht. Dazu stehen als Personendaten der Klarname der versicherten Person, die Versichertennummer (AHV-Nummer) oder allenfalls auch weitere Identifikatoren zur Verfügung. Bei der Überweisung der IV-Taggelder durch die Ausgleichskasse genügt offenbar die AHV-Nummer für die Zuordnung zur versicherten Person. Aus Gründen der Verhältnismässigkeit wäre auch bei den Taggeldzahlungen durch die Unfallversicherer ein nichtsprechendes Personendatum wie die AHV-Nummer dem Klarnamen vorzuziehen. Dabei handelt es sich um einen allgemeinen datenschutzrechtlichen Grundsatz. Art. 97 Abs. 7 UVG hält zudem nochmals ausdrücklich fest, dass nur diejenigen Daten übermittelt werden dürfen, welche für den in Frage stehenden Zweck erforderlich sind. Sofern eine analoge Behandlung wie bei den IV-Taggeldzahlungen möglich ist, sind die Abläufe entsprechend anzupassen, und es ist auch da die AHV-Nummer als Identifikator zu verwenden. Nur, wenn eine analoge Behandlung nachweislich ausgeschlossen und eine Verwendung des Klarnamens damit unumgänglich ist, wäre die aktuelle Praxis bei den Taggeldzahlungen durch die Unfallversicherer aus Sicht Datenschutz sowie nach den Bestimmungen des UVG rechtmässig.

Datenbekanntgabe an ausserkantonale Schulbehörde

Das Schulamt der Stadt Bern erhielt von einer Schulleitung eines anderen Kantons eine Anfrage für eine Datenbekanntgabe. Es ging um die Angaben über zwei neue Schülerinnen (Schwestern), welche bisher in der Stadt Bern zur Schule gegangen sind.

Das Schulamt schilderte, dass die Eltern sich weigern würden, der neuen Schule den bisherigen Schulstandort bekannt zu geben, obschon der Austausch zwischen der bisherigen und der neuen Lehrperson aus schulischen Gründen angezeigt war. Es wollte daher wissen, ob die Weitergabe der Angaben zu den Schülerinnen betreffend früherem Schulstandort und Lehrperson zulässig und damit

die Ermöglichung eines Austausches zwischen den Lehrpersonen zulässig sind.

Das kantonale Volksschulgesetz (VSG; BSG 432.210) regelt den Datenaustausch unter Schulbehörden im Anwendungsbereich des Gesetzes. Es ist damit nur auf Schulbehörden des Kantons anwendbar. Die FADS stellte daher fest, dass für eine Datenweitergabe an eine ausserkantonale Schulbehörde vorliegend keine Rechtsgrundlage besteht; insbesondere lag auch eine Zustimmung durch die Erziehungsberechtigten ausdrücklich nicht vor. Die ersuchende Behörde musste daher auf den Weg der Amtshilfe verwiesen werden.

Datenweitergabe Schulamt an Kantonspolizei

Im Nachgang zu einem öffentlich bekannt gewordenen Vorfall an einer Berner Schule «Mob aus Kindern umzingelte eine Pausenaufsicht und rief «Allahu Akbar»» gelangte das Schulamt an die FADS mit der Bitte um Prüfung einer Anfrage um Weitergabe der Namen der involvierten Schüler*innen an die Kantonspolizei. Die Datenbekanntgabe sollte nicht zum Zweck der Einleitung einer Strafuntersuchung erfolgen, sondern der Durchführung einer Gefahrenanalyse dienen.

Dem Schulamt konnte Folgendes zurückgemeldet werden: Die Kantonspolizei führt das kantonale Bedrohungsmanagement als Aufgabe des Staatsschutzes gestützt auf die Bestimmungen des Bundes und diejenigen des kantonalen Polizeigesetzes. Im Hinblick auf die Erfüllung von Aufgaben dieses Gesetzes sind kommunale Behörden ermächtigt, der Kantonspolizei Personendaten, einschliesslich besonders schützenswerter Personendaten zu melden. Vorbehalten bleiben dabei besondere Geheimhaltungspflichten wie z.B. das Berufsgeheimnis von Gesundheitsfachpersonen im Schulbereich. Die Frage, ob eine solche Meldung zu erfolgen hat, liegt im pflichtgemässen Ermessen der betreffenden Behörde. Allenfalls wäre auch eine Beratung bei der städtischen Fachstelle Radikalisierung und Gewaltprävention angezeigt, was im vorliegenden Fall erfolgte.

Datenweitergabe an Familien und Quartier Stadt Bern bei Rückstellungen Kindergartenbesuch

Das Schulamt ersuchte um Beurteilung der Weitergabe einer Liste der Kinder, welche von ihren Eltern für den Kindergartenbesuch um ein Jahr zurückgestellt worden sind, an Familien und Quartier Stadt Bern.

Familien und Quartier Stadt Bern benötigte Angaben zur Zurückstellung, um den Anspruch auf Kita-Betreuungsgutscheine zu prüfen (dieser Anspruch besteht nur für Kinder, welche nicht den Kindergarten besuchen). Allerdings enthielt die betreffende Liste die Angaben zu sämtlichen Rückstellungen, d.h. auch zu Kindern, welche die Kita nicht besuchen und daher für die Prüfung des Anspruchs auf Kita-Betreuungsgutscheine nicht erforderlich sind. Die Weitergabe der gesamten Liste wurde nach Angaben des Schulamts aus Ressourcengründen erbeten.

Die FADS hielt fest, dass die Datenweitergabe grundsätzlich nur im für die Aufgabenerfüllung erforderlichen Ausmass zulässig ist. Auf die Personendaten derjenigen zurückgestellten Kinder, welche keine Kita besuchen, trifft dies nicht zu. Es dürfen daher nur diejenigen Kinder an Familie und Quartier Stadt Bern gemeldet werden, welche tatsächlich eine Kita besuchen. Die Einsparung von Ressourcen kann für sich keinen Grund

für die Nichteinhaltung von Vorgaben des Datenschutzrechts darstellen. Die FADS empfahl dem Schulamt, die Information bezüglich Kita-Besuch im Rahmen der Meldung der Rückstellung direkt bei den Erziehungsberechtigten zu erheben.

Weitergabe Klassenlisten an Kindertreff

Ein als privatrechtlicher Verein organisierter Kindertreff fragte eine Schulleitung um die Weitergabe der Klassenlisten in digitaler Form an. Als Begründung wurde dargelegt, dass es dem Kindertreff wie auch den teilnehmenden Kindern ermöglicht werden sollte, bei Bedarf die Eltern erreichen zu können.

Die betreffende Schulleitung wandte sich mit dem Anliegen an das Schulamt, welches es der FADS unterbreitete. Das Schulamt äusserte bereits von sich aus Zweifel an der Zulässigkeit der Datenbekanntgabe. Zunächst hielt die FADS fest, dass es sich hier um eine Datenbekanntgabe an eine private (juristische) Person ausserhalb des Anwendungsbereichs der Datenschutzbestimmungen des Volkschulgesetzes handeln würde. Damit waren die allgemeinen Bestimmungen für die Datenbekanntgabe an Private nach Art. 11 KDSG zu beachten. Das Problem bestand hier darin, dass die Datenbekanntgabe an private Personen nach Art. 11 Abs. 1 KDSG immer nur eine Bekanntgabe im Einzelfall umfasst. Die generelle Bekanntgabe der Personendaten sämtlicher Schüler*innen gemäss Klassenliste wird von dieser Bestimmung nicht abgedeckt. Bereits aus diesem Grund wäre die Weitergabe der integralen Klassenlisten nicht zulässig.

Weiter wurde die Frage aufgeworfen, ob eine entsprechende Datenweitergabe allenfalls im Sinne von Art. 11 Abs. 1 Bst. b «im Interesse» der betroffenen Person liegen könne. Hierzu war festzuhalten, dass ein konkretes Interesse der betroffenen Personen im Zeitpunkt der Datenbekanntgabe nicht bzw. noch nicht vorliegt. Das Interesse der betroffenen Person muss unmittelbar und konkret vorliegen, um als Rechtsgrundlage für eine Datenbekanntgabe dienen zu können. Ein mögliches, sich allenfalls später bei einem Besuch des Kindertreffs ergebendes Interesse genügt den gesetzlichen Anforderungen nicht. Wie das Schulamt zu Recht festhielt, würden zudem ja auch Daten von Betroffenen bekannt gegeben, bei welchen sich die Frage einer Kontaktaufnahme gar nie stellen wird. Möglicherweise wäre dies gar die Mehrheit der auf den Klassenlisten verzeichneten Betroffenen. Auch aus diesem Grund würde sich die integrale Weitergabe der Klassenliste als unverhältnismässig erweisen.

Keine Rechtsgrundlage für die Übermittlung von Klassenlisten

Nach dem Gesagten erachtete die FADS eine Übermittlung von Klassenlisten an einen Kindertreff mangels Rechtsgrundlage als nicht zulässig. Den Kindertreff bzw. der Schulleitung wurde empfohlen, andere Massnahmen für den Einzelfall zu prüfen. Denkbar wäre aber auch, bei den betroffenen Eltern eine informierte und ausdrückliche Zustimmung für die Weitergabe der Kontaktdaten an den Kindertreff einzuholen.

Weitere Anfragen aus dem Schulbereich

Privater Podcast zum Schulbetrieb

Das städtische Schulamt erkundigte sich nach der Zulässigkeit von privaten Podcasts zum Schulbetrieb unter Nennung der Klarnamen von betroffenen Schüler*innen und Lehrpersonen.

Die FADS bestätigte zunächst, dass hier, wie vom Schulamt zu Recht festgehalten, Bundesdatenschutzrecht zur Anwendung kommt. Es wurde darauf hingewiesen, dass die Nennung von tatsächlichen Klassenkamerad*innen und Lehrpersonen, je nach Kontext, eine Persönlichkeitsverletzung darstellen könne. Die FADS riet daher, darauf hinzuwirken, dass solche Podcasts nur mit fiktiven Namen von Betroffenen, Schulen und Klassen veröffentlicht werden. Darauf wäre einleitend im jeweiligen Podcast ausdrücklich hinzuweisen.

Datenschutz bei der Verpflegung in den Tagesschulen

Beim Fachbereich Verpflegung des Schulamts stellten sich Fragen in Bezug auf den Datenschutz bei Kindern mit speziellen Ernährungsbedürfnissen (Allergien, Diäten). Betroffen waren die Frage der Zulässigkeit der Einsichtnahme in Arztzeugnisse und der namentlichen Beschriftung von Boxen mit Spezialmahlzeiten. Die FADS wurde um Beurteilung der Sach- und Rechtslage ersucht.

Für die Bearbeitung von Gesundheitsdaten, welche sog. besonders schützenswerte Personendaten darstellen, besteht in Art. 73 Abs. 2 Volksschulgesetz (VSG; BSG 432.210) eine Rechtsgrundlage. Voraussetzung ist, dass die betreffenden Personendaten für die Erfüllung der gesetzlichen Aufgabe zwingend erforderlich sind. Zudem müssen die Vorgaben des KDSG für die Bearbeitung von Personendaten erfüllt sein, insbesondere müssen die Personendaten und die Art des Bearbeitens für die Aufgabenerfüllung geeignet und notwendig sein (Art. 5 Abs. 3 KDSG).

Die FADS nahm Kenntnis davon, dass die Arztzeugnisse einverlangt werden, weil rein mündliche Angaben angesichts der Verantwortung für die (medizinische) Sicherheit und der sich aus der Lebensmittelgesetzgebung ergebenen Pflichten erfahrungsgemäss nicht ausreichend klar und verbindlich sind. Hinzu können auch sprachliche Probleme bzw. Verständnisschwierigkeiten treten. Gerade bei besonderen Allergien ist es für die Gesundheit der betroffenen Schülerinnen und Schüler entscheidend, dass die speziellen Mahlzeiten gestützt auf zuverlässige und dokumentierte medizinische Angaben hergestellt werden können. Vor diesem Hintergrund erschien es der FADS als verhältnismässig, bei den Erziehungsberechtigten jeweils ein Arztzeugnis einzuverlangen. Zudem werden die Arztzeugnisse zentral aufbewahrt; Zugang haben nur diejenigen Mitarbeitenden, welche die entsprechenden Angaben zur Aufgabenerfüllung benötigen. Bei Austritt aus der Tagesschule oder bei Änderung der Verhältnisse werden die Zeugnisse vernichtet.

Bezüglich namentlicher Beschriftung der Mahlzeitenboxen nahm die FADS Kenntnis davon, dass es sich um ein Massengeschäft (650 Mahlzeiten pro Tag) handelt. Die Komplexität der Logistik ist aufgrund einer gestaffelten Lieferung an 23 Standorte hoch. In Anbetracht der Risiken bei einer Verwechslung von Mahlzeitenboxen,

gerade bei besonderen Allergien, erschien es der FADS nachvollziehbar, dass eine namentliche Beschriftung der Boxen als zwingend erachtet wird. Einer Verwechslungsgefahr kann mit milderen Mitteln, wie z.B. der Beschriftung der Boxen mit einem Code oder lediglich einer Bezeichnung der Spezialmahlzeit, angesichts der möglichen Auswirkungen einer Verwechslung nicht ausreichend begegnet werden.

Allergien machen zuverlässige medizinische Angaben notwendig

Insgesamt erachtete die FADS gestützt auf den aktuellen Kenntnisstand die Praxis der Handhabung der Mahlzeiten für spezielle Ernährungsbedürfnisse (Allergien, Diäten) als datenschutzkonform.

Diverse Anfragen

Publikation von historischen Adressbüchern

Das Stadtarchiv wandte sich für eine Beratung zum Thema Online-Publikation historischer Adressbücher, verknüpft mit Geoinformationsdaten, an die FADS. Nach einer Medienberichterstattung stellte sich die Frage, ob eine solche zulässig ist.

Das Stadtarchiv wies zunächst auf eine Berichterstattung von SRF hin, wonach der kantonale Datenschutzbeauftragte gegen die Online-Publikation von archivierten Staatskalendern, welche jünger als 110 Jahre alt waren, interveniert hatte. Für das Stadtarchiv war gestützt darauf unklar, ob ein aktuelles Projekt aus Sicht Datenschutz zulässig sei. Dabei war geplant, Einträge der historischen Adressbücher der Stadt Bern aus den Jahren 1860 bis 1945 strukturiert und verknüpft mit städtischen Geoinformationsdaten im Internet zugänglich zu machen.

Die FADS prüfte die Sach- und Rechtslage. Sie stellte zunächst fest, dass das Vorhaben durch die gesetzlichen Grundlagen in den Aufgabenbestimmungen des Stadtarchivs abgedeckt wurde. Damit vermieden werden konnte, dass durch die Datenverknüpfung Adressdaten noch lebender Personen betroffen sind, empfahl die FADS eine analoge Anwendung der archivrechtlichen 110-jährigen Sperrfrist. Vor dem Hintergrund, dass Eintragungen in die damaligen Adressbücher ab dem 16. Altersjahr erfolgten, hatte dies zur Folge, dass lediglich Adressbücher bis und mit Jahrgang 1930 für die Datenverknüpfung verwendet werden konnten.

Listenauskunft für Masterarbeit

Die Einwohnerkontrolle erkundigte sich bei der FADS nach der Zulässigkeit einer Listenauskunft für eine Masterarbeit betreffend ehemaligen Bewohnenden einer bestimmten Liegenschaft. Insbesondere wollte sie wissen, ob auch Angaben zu nicht mehr aktiven Einwohnerdaten gemacht werden dürfen.

Die FADS hatte damit Gelegenheit, sich erstmals einlässlich mit der neuen Bestimmung von Art. 8 des am 1. Januar 2023 in Kraft getretenen städtischen Datenschutzreglements (DSR; SSSB 152.06) zu befassen. Art. 12 Abs. 3 KDSG hält fest, dass das Gemeindereglement die systematisch geordnete Bekanntgabe bestimmter Daten der Einwohnerkontrolle (sog. Listenauskunft) gestatten kann.

Wesentlich ist, dass mit der Listenauskunft nach Art. 8 DSR keine kommerziellen Zwecke verfolgt werden, was vorliegend gegeben war. Zur Frage der Datenbasis stellte die FADS fest, dass weder das KDSG noch das DSR die Listenauskunft auf aktive Einwohnerdaten einschränken; der Begriff «Daten der Einwohnerkontrolle» umfasst aus Sicht FADS sämtliche bei den Einwohnerdiensten vorhandenen Daten von (aktiven und ehemaligen) Einwohner*innen. Eine Einschränkung erfolgt in Bezug auf diejenigen Daten, welche bekannt gegeben werden dürfen (Name, Vorname, Beruf, Geschlecht, Adresse, Zivilstand, Heimatort, Datum Zu- und Wegzug, Jahrgang; Art. 12 Abs. 1 KDSG), sowie selbstverständlich in Bezug auf Personen, welche eine Adresssperre verlangt haben.

Auswertung Telefonverkehr beim IT-Servicedesk

Der Direktionspersonaldienst Finanzen Personal und Informatik ersuchte die FADS um eine grundsätzliche Einschätzung zur Zulässigkeit von personalisierten Auswertungen des Telefonverkehrs beim IT-Servicedesk. Die betreffenden Auswertungen sollten einerseits zum Zweck der verbesserten Einsatzplanung und andererseits zur Festlegung von Leistungszielen der Mitarbeitenden und deren Messung erfolgen.

Die FADS legte vorab die grundlegende rechtliche Einordnung von Überwachungsmassnahmen am Arbeitsplatz, insbesondere des Verbots der Überwachung des Verhaltens, dar.

Überwachungsmassnahmen am Arbeitsplatz stehen im Grundsatz in Konflikt mit der Pflicht der Arbeitgeberin zur Gewährleistung des Persönlichkeitsschutzes und der entsprechenden Fürsorgepflicht gegenüber den Angestellten (Art. 3 Abs. 4 und Art. 3a Abs. 2a Personalreglement der Stadt Bern, PRB; SSSB 153.01). Die auf die Stadt Bern anwendbare Bestimmung von Art. 26 Abs. 1 Verordnung 3 zum Arbeitsgesetz (ArGV 3; SR 822.113) verbietet Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer*innen am Arbeitsplatz überwachen sollen. Sofern solche Systeme aus anderen Gründen notwendig sind, müssen sie so ausgestaltet werden, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer*innen dadurch nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3). Grundsätzlich zulässig sind demnach Systeme, welche aus anderen Gründen, z. B. für die Kontrolle der Funktion, Qualität oder Leistung von Personen, Maschinen, Systemen, erforderlich sind. Allerdings ist die Abgrenzung von Verhaltung und Leistung in der Praxis nicht einfach. Zudem muss das gewählte Überwachungssystem nach der Rechtsprechung des Bundesgerichts in Anbetracht aller Umstände in einem angemessenen Verhältnis zum verfolgten Ziel stehen, und die betroffenen Angestellten müssen vorab über seine Verwendung informiert worden sein (BGE 130 II 425).

Zur Auswertung des Telefonverkehrs im Kundensupport wies die FADS auf die Vorgaben des Staatssekretariats für Wirtschaft seco gemäss der Checkliste zum Einsatz von technischen Überwachungssystemen hin[4]. Die Checkliste hält Konzeption und Rahmenbedingungen solcher Systeme fest und zeigt auf, welche Massnahmen zum Schutz der Betroffenen zu ergreifen sind. Die FADS empfahl, für den Zweck der Leistungs-

4 https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Merkblatter_und_Checklisten/checkliste-technische-ueberwachung.html

überwachung die Vorgaben der Checkliste, soweit anwendbar, umzusetzen. Zudem hielt sie fest, dass zum Zweck der Einsatzplanung ausschliesslich nicht personenbezogene Auswertungen vorzunehmen sind. Gleichzeitig bot die FADS an, die konkret geplante Überwachung sowie die getroffenen Schutzmassnahmen zu gegebener Zeit nochmals zu prüfen.

Pilot selbstfahrendes Lieferfahrzeug

Das Amt für Umwelt erkundigte sich nach der Bewilligungspflicht für einen Pilotversuch mit einem selbstfahrenden Lieferfahrzeug in der Stadt Bern. Im Vorfeld des Pilotbetriebs sei zum Training der Algorithmen für das autonome Fahren eine Befahrung des städtischen Strassennetzes mit Kameras und Lidar-Technologie vorgesehen.

Die FADS klärte zunächst die Rolle der Stadt Bern im Pilotversuch. Wie sich zeigte, war die Stadt Bern am Projekt nicht beteiligt. Verantwortlich für das Projekt sind ausschliesslich die beteiligten privaten Akteure. Damit liegt eine Datenbearbeitung durch Private vor, womit das Datenschutzgesetz des Bundes anwendbar und die Aufsichtszuständigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gegeben ist. Für den Pilotversuch an sich wurde durch die Projektverantwortlichen die erforderliche Ausnahmebewilligung des Bundesamts für Strassen beantragt. Bei der Stadt Bern musste zusätzlich eine Bewilligung zur Benutzung der öffentlichen Strassen eingeholt werden. Die FADS hielt fest, dass die Projektverantwortlichen in diesem Zusammenhang zur Einhaltung des Datenschutzes zu verpflichten sind.

Wie sich zeigte, führten die Projektverantwortlichen bereits Befahrungen von städtischen Strassen durch, ohne dass eine Information der Bevölkerung erfolgt war. Die FADS legte nahe, bei allfälligen Anfragen besorgter Bürger*innen darauf hinzuweisen, dass es sich um ein privates Vorhaben auf eigene Verantwortung handelt. Zusätzlich könnte dahingehend informiert werden, dass keine personenbezogene Bearbeitung der Daten (Zweck ist das Training des Algorithmus für automatisiertes Fahren) und keine Veröffentlichung von Kamerabildern erfolgen, dass die Daten nach erfolgter Bearbeitung gelöscht werden und dass der EDÖB für die Aufsicht zuständig ist.

Einhaltung des Datenschutzes als Bewilligungsvoraussetzung

Gemäss Medienmitteilung des Gemeinderats wurde die Bewilligung des Bundes erteilt und das Projekt im letzten Quartal 2024 gestartet. Verschiedentlich wurde auch in den Medien über das Projekt berichtet.

Antrag

Kenntnisnahme des Tätigkeitsberichts 2024 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.