Stadt Bern

daten
schutz

«Es ist wichtig und notwendig, diese Extrameile zu gehen, um das Vertrauen der Bevölkerung zu wahren und sie auf diese Reise in eine digitale Zukunft mitnehmen zu können.»

Sophie Haag,
Leiterin Fach- und Aufsichtsstelle
Datenschutz FADS

Tätigkeitsbericht 2023

Fach- und Aufsichtsstelle Datenschutz der Stadt Bern FADS

Leiterin Fach- und Aufsichtsstelle Datenschutz FADS:
Sophie Haag, Rechtsanwältin
Mirjam Graf, Rechtsanwältin und Mediatorin,
Datenschutzbeauftragte ad interim (bis Januar)

Mitarbeitende: Markus Hochuli, MA Governance, Techniker HF Elektrotechnik, wissenschaftlicher Mitarbeiter Informatik (60%)
Patrick Rohrbach, Fürsprecher, wissenschaftlicher Mitarbeiter Recht (bis Juli 70%, danach 60%)
Daniela Mäder, administrative Mitarbeiterin (30%)

Adresse: Effingerstrasse 4, 3011 Bern

Telefon: + 41 31 312 09 12

E-Mail: datenschutz@bern.ch

Öffnungszeiten: Mo bis Do, 8.00–12 Uhr und 13.30–16.30 Uhr

www.bern.ch/datenschutzaufsicht

Impressum
Herausgeberin: Fach- und Aufsichtsstelle Datenschutz der Stadt Bern
Layout: Büro Z, Bern

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 per 1. Januar 2023 in Kraft getretenen Datenschutzreglements der Stadt Bern (DSR; SSSB Nr. 152.06) mit Unterstützung meines Teams über die Tätigkeit im Jahr 2023 zu berichten.

Im Februar 2023 durfte ich meine Stelle als Leiterin der Fach- und Aufsichtsstelle Datenschutz FADS und Datenschutzbeauftragte der Stadt Bern antreten. Das Ankommen wurde mir durch mein Team, durch die Ombudsfrau und deren Team sehr leicht gemacht. Ich wurde freundlich empfangen, kompetent in die aktuellen Themen eingeführt und bei den diversen administrativen Arbeiten tatkräftig unterstützt.

Auch von der Stadtverwaltung wurde ich freundlich empfangen. Der Einstieg in die fachlichen Geschäfte der FADS war dabei steil: Die Stadt Bern steckt mitten in einer Digitalisierungswelle und hat sich eine vorbildliche Digital Governance auf die Fahne geschrieben. Während im Berichtsjahr übergeordnet rechtliche und organisatorische Rahmenbedingungen dafür geschaffen wurden, nahmen zeitgleich Projekte zur Einführung neuer Applikationen Fahrt auf. Der Bedarf an Unterstützung durch die neue Fachstelle war daher von Beginn weg gross, und auch eine Intensivierung der Aufsichtstätigkeit wurde notwendig. So warteten gleich mehrere Grossprojekte auf eine Begleitung und Kontrolle durch die FADS.

Es folgten intensive und spannende Arbeiten in den unterschiedlichen Projekten, wobei sich zeigte, wie wichtig die Lernbereitschaft aller Beteiligter ist. Gefreut hat mich dabei, dass sich in diversen Projekten eine konstruktive und äusserst zielführende Zusammenarbeit entwickelt hat, die zu einer deutlichen Verbesserung des Datenschutzes geführt hat. Klar ist jedoch, dass dieser Lernprozess weitergehen muss, wenn die Stadt Bern ihren eigenen Ansprüchen gerecht werden möchte. Digitalisierung unter Wahrung der Persönlichkeitsrechte der Bevölkerung ist nicht immer einfach und verlangt von den Verantwortlichen, genau hinzuschauen, wenn eine neue Applikation beschafft und in Betrieb genommen werden soll. Es ist wichtig und notwendig, diese Extrameile zu gehen, um das Vertrauen der Bevölkerung zu wahren und sie auf diese Reise in eine digitale Zukunft mitnehmen zu können.

Sophie Haag
Datenschutzbeauftragte der Stadt Bern

Bern, März 2024

1

Rückblick

Die neue Fach- und Aufsichtsstelle Datenschutz konnte im Berichtsjahr trotz der prägenden Trennung von der Ombudsstelle und dem Stellenantritt der neuen Leiterin den operativen Betrieb nahtlos weiterführen. Dabei beschäftigte sie insbesondere die Einführung neuer Applikationen.

Organisatorische Trennung Datenschutzaufsicht und Ombudsstelle und neue Leiterin FADS

Am 1. Januar 2023 ist das neue Datenschutzreglement der Stadt Bern in Kraft getreten. Die Datenschutzaufsicht wurde damit organisatorisch von der Ombudsstelle getrennt, als Fach- und Aufsichtsstelle Datenschutz einer eigenen Leitung unterstellt und personell aufgestockt. Daneben wurde mit dem Reglement eine Rechtsgrundlage für das Erteilen von Listenauskünften, für ein Abrufverfahren auf Daten der Einwohnerkontrolle sowie zur Publikation öffentlich zugänglicher Informationen mit Personendaten geschaffen.

Im September 2022 wurde die Juristin und Rechtsanwältin Sophie Haag vom Stadtrat zur Leiterin der neuen Fach- und Aufsichtsstelle Datenschutz (FADS) gewählt. Sie trat ihre Stelle am 1. Februar 2023 an. Bis dahin wurde die Leitung ad interim durch die Ombudsfrau und bisherige Datenschutzbeauftragte wahrgenommen. Das Berichtsjahr war denn auch geprägt durch die Trennung der FADS von der Ombudsstelle und den damit einhergehenden Leitungswechsel.

Eine Kombination von Aufsicht mit Elementen der Beratung ist notwendig, um effizient ans Ziel zu gelangen.

Zunächst war die Trennung technisch und organisatorisch umzusetzen. Viele Arbeiten dazu sind bereits im Vorjahr angefallen und durchgeführt worden, zogen sich aber weit in das Berichtsjahr hinein und waren insbesondere zu Beginn intensiv. Dank der umfassenden Vorbereitung durch die bisherige Datenschutzbeauftragte und ihr Team konnte die neue Leiterin im Februar jedoch eine gut organisierte, motivierte

und bereits voll operative FADS übernehmen. So konnte der Betrieb trotz dieser grossen Umstellung nahtlos weitergeführt und im Verlauf des Jahres weiter ausgebaut werden.

Gleichzeitig galt es für die neue Leiterin, sich mit der Stadt Bern, ihren Besonderheiten und ihren aktuellen Themen im Bereich Datenschutz auseinanderzusetzen. Sie konnte dabei von Beginn weg auf die volle Unterstützung durch ihr Team und die bisherige Leiterin zählen.

Themenschwerpunkte im Berichtsjahr

Gleich zu Beginn des Berichtsjahres erregten die nicht bewilligten Videoüberwachungen in diversen städtischen Velostationen die mediale Aufmerksamkeit. Der Gemeinderat ordnete daraufhin an, die Kameras abzuschalten und nachträglich zu legitimieren. Dies sowie weitere Videoüberwachungen bildeten einen Themenschwerpunkt im Berichtsjahr, wobei die Thematik in unterschiedlichen Facetten in Erscheinung trat. Im Vordergrund standen Videoüberwachungen zum Schutz öffentlicher Gebäude und deren Benutzenden nach dem kantonalen Polizeigesetz und dem städtischen Videoreglement. Die FADS befasste sich zudem mit Videoüberwachungen zu anderen als zu Zwecken nach Polizeigesetz. Solche Videoüberwachungen unterliegen in aller Regel nicht dem Verfahren nach Polizeigesetz und Videoreglement, jedoch grundsätzlich der datenschutzrechtlichen Vorabkontrolle. Nachdem die Thematik im Tätigkeitsbericht 2022 bereits als Schwerpunkt behandelt wurde, soll im vorliegenden Bericht unter Kapitel 6 Einblick in einzelne Fälle aus der Praxis gegeben werden.

Ein weiterer Schwerpunkt war die Prüfung neu geplanter Applikationen, und dabei insbesondere das Programm «Neue digitale Zusammenarbeit» und die damit einhergehende Einführung von Microsoft 365 in der Stadtverwaltung und der Schulinformatik. Microsoft 365 ist ein gutes Beispiel für die zunehmende Komplexität der an die FADS herangetragenen Projekte. Auch bei der Prüfung oder Beratung zu anderen, in der Stadt Bern geplanten Applikationen hat sich gezeigt, dass eine Kombination von Aufsicht mit Elementen der Beratung notwendig ist, um effizient ans Ziel zu gelangen, die Stadtverwaltung zu digitalisieren und dabei die Persönlichkeitsrechte der Bevölkerung zu wahren. So konnte sich eine gute Zusammenarbeit zwischen der FADS und den Projektverantwortlichen etablieren.

Vernetzung und Austausch innerhalb der Stadt Bern

Für die FADS ist eine gute Zusammenarbeit mit der Stadtverwaltung zentral. Können Digitalisierungsprojekte von Beginn weg datenschutzfreundlich geplant werden, trägt dies den Anliegen des Datenschutzes am besten Rechnung. Daher war es der neuen Leiterin wichtig, die für die Digitalisierung der Stadtverwaltung verantwortlichen Personen kennen zu lernen und einen Austausch zu etablieren.

Können Digitalisierungsprojekte von Beginn weg datenschutzfreundlich geplant werden, trägt dies den Anliegen des Datenschutzes am besten Rechnung.

Bereits kurz nach ihrem Stellenantritt wurden daher die bereits vorher durchgeführten Austauschgespräche mit der ICT-Sicherheit der Informatikdienste wieder aufgenommen.

Trotz diverser personeller Veränderungen bei der ICT-Sicherheit konnten diese Gespräche über das Berichtsjahr hinweg aufrechterhalten werden. Sie erwiesen sich für die FADS als enorm wertvoll, da beide Bereiche ähnliche Themen bearbeiten, ihre Arbeiten so koordinieren und ihren Anliegen damit besser zum Durchbruch verhelfen konnten.

Ebenfalls kurz nach Stellenantritt begann ein wiederkehrender Austausch mit Digital Stadt Bern. Auch dies hat sich als sehr gewinnbringend erwiesen, konnten auf diese Weise doch Grossprojekte, wie die Einführung von Microsoft 365 in der Stadtverwaltung oder der Schulinformatik, besprochen und koordiniert werden, was die Arbeiten in diesen Projekten deutlich erleichterte.

Bei Antrittsbesuchen bei den Mitgliedern der KDSB und der Stadtkanzlei konnte die Leiterin FADS die Tätigkeit der Fachstelle vorstellen, Bedürfnisse abholen und sich über gemeinsame Themen austauschen. Es zeigte sich, dass das Bedürfnis nach Beratung zu Datenschutzthemen in der Verwaltung gross ist. Die FADS hat ihre Tätigkeit in der Folge denn auch stark auf dieses beratende Element hin ausgerichtet und mit Blick auf den Bedarf in der Verwaltung auch in ihre Aufsichtstätigkeit einfliessen lassen (vgl. Schwerpunktthema «Die Vorabkontrolle», Seite 8 im vorliegenden Bericht).

Im Rahmen von Austauschgesprächen mit der GPK resp. mit einem Ausschuss der GPK konnte die Leiterin FADS ihre personellen und organisatorischen Anliegen besprechen und übergeordnete Datenschutzthemen präsentieren. Der Rückhalt und die Unterstützung durch ihre vorgesetzte Stelle wurden von ihr sehr geschätzt.

Wiederkehrende Austauschgespräche zu organisatorischen Themen fanden auch mit den weiteren Legislativstellen Ratssekretariat und Ombudsstelle statt.

Vernetzung und Austausch mit anderen Datenschutzaufsichtsstellen und weiteren Behörden

Die zunehmende Komplexität im Datenschutz macht auch den Austausch mit anderen Datenschutzaufsichtsstellen immer wichtiger. Daher vernetzt sich die FADS mit anderen Datenschutzaufsichtsstellen in der Schweiz z. B. im Rahmen der Plenarversammlung von Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Darüber hinaus nahm sie aber auch regelmässig an den Treffen der Privatim Arbeitsgruppe ICT teil, in denen die technischen Aspekte des Datenschutzes besprochen und untereinander koordiniert werden. Auch zu spezifischen Projekten wie Microsoft 365 oder Citysoftnet fanden Austauschgespräche mit den ebenfalls betroffenen Datenschutzaufsichtsstellen statt. Wichtig war zudem ein Austausch mit der Kantonspolizei Bern, in dem die künftige Zusammenarbeit bei geplanten, unter das kantonale Polizeigesetz fallenden Videoüberwachungen besprochen wurde.

Digitale Fallführung für FADS und OS

Im Projekt digitale Fallführung wurden die Arbeiten zusammen mit der OS weitergeführt. Der Entscheid für die Beschaffung wurde definitiv gefällt. Wie unter der früheren Datenschutzbeauftragen geplant, soll die Fallführung basierend auf zwei getrennten Mandanten bei einem Drittanbieter betrieben werden (s. dazu Tätigkeitsbericht OS/DSA 2022, Seite 4). Ein Grobkonzept wurde erstellt und mit dem Anbieter der Einführungstermin infolge dessen hoher terminlicher Auslastung auf das erste Quartal 2024 festgelegt.

2

Schwerpunktthema: Die Vorabkontrolle – Ein Lernprozess für die FADS und die städtische Verwaltung

Während die Anzahl der im Berichtsjahr zur Vorabkontrolle eingereichten IT-Projekte stark angestiegen ist, hat die FADS bei in den Dienststellen der Stadtverwaltung vorhandenen Knowhow und Ressourcen für den Bereich Datenschutz und Datensicherheit Verbesserungsbedarf verortet. Die dazu angestossenen Arbeiten müssen zwingend weitergeführt werden, um mit der wachsenden Digitalisierung Schritt halten zu können.

Beabsichtigt eine Behörde, Personendaten einer grösseren Anzahl von Personen elektronisch zu bearbeiten, unterbreitet sie die beabsichtigte Datenbearbeitung vor deren Beginn der Datenschutzaufsichtsstelle zur Stellungnahme, wenn zweifelhaft ist, ob eine genügende Rechtsgrundlage besteht, besonders schützenswerte Personendaten bearbeitet werden, eine besondere Geheimhaltungspflicht besteht oder technische Mittel mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen eingesetzt werden (Art. 17a des Datenschutzgesetzes des Kantons Bern, KDSG). Damit soll verhindert werden, dass Applikationen, welche die Anforderungen des Datenschutzes nicht erfüllen, überhaupt in Betrieb genommen werden.

Obschon die Vorabkontrolle im kantonalen Gesetz bereits 2008 eingeführt worden ist, wurden in der Stadt Bern kaum Vorabkontrollen durchgeführt. Die personellen Ressourcen bei der Datenschutz-Aufsicht liessen es nicht zu, solche in der Regel sehr aufwändigen Projekte an die Hand zu nehmen. Dies änderte sich mit dem Ausbau der personellen Ressourcen der Datenschutz-Aufsichtsstelle im Jahr 2020. Der Kontrollprozess wurde definiert sowie eine Musterdokumentation in Zusammenarbeit mit der ICT-Sicherheit der Informatik Stadt Bern erstellt und zusammen mit entsprechenden Merkblättern im Inter- und im Intranet aufgeschaltet. In der Folge wurden erste IT-Projekte zur Vorabkontrolle eingereicht und der Kontrollprozess bei der Datenschutz-Aufsichtsstelle gestartet.

Im Berichtsjahr kam Bewegung in die Sache. Die FADS hat sich mit insgesamt 15 Vorabkontrollprojekten befasst, darunter Grossprojekte wie M365 in der Stadtverwaltung und der Schulinformatik oder Citysoftnet, mittelgrosse Projekte wie die Technische Unterstützung der Wasseraufsicht in der neuen Schwimmhalle oder kleine einfache Videoüberwachungen an diversen Standorten. So erhielt nicht nur die FADS die Möglichkeit, auf breiter Basis Erfahrungen zu sammeln und den Kontrollprozess laufend zu verbessern. Auch in der Stadtverwaltung ist ein Lernprozess im Gang, der auch in den folgenden Jahren weitergeführt werden muss. So stellt die FADS fest, dass der Wille

für eine vorbildliche Digitalisierung in der Stadt Bern gross ist, das Knowhow und die eingesetzten Ressourcen für Datenschutz und Datensicherheit aber noch verbessert werden müssen, um mit der fortschreitenden Digitalisierung Schritt halten zu können.

Dies beginnt damit, dass der in der Stadt Bern einzuhaltende ISDS-Prozess inkl. einer allfällig daran anschliessenden Vorabkontrolle noch zu wenig bekannt ist. So wurden in Unkenntnis dieser Prozesse Applikationen in Betrieb genommen, ohne dass das Projekt vorgängig verwaltungsintern auf die Einhaltung der Informatiksicherheit überprüft oder bei der FADS zur Vorabkontrolle eingereicht wurde. Dementsprechend müssen sowohl die FADS als auch die mit der Thematik befassten Einheiten der Stadtverwaltung künftig noch besser darauf hinwirken, dass diese Prozesse in der gesamten Verwaltung bekannt sind. Erste Vorbereitungen dazu wurden denn auch bereits von beiden Seiten an die Hand genommen.

Als grösste Herausforderung verortet die FADS jedoch das fehlende Knowhow beim Erstellen der ISDS-Dokumentation. Diese soll die geplante Applikation beschreiben und stellt die Basis für die interne Überprüfung der Informatiksicherheit wie auch für die Vorabkontrolle dar. Im Wesentlichen ist darin darzulegen, welche Datenbearbeitungen mit welchen Daten zu welchen Zwecken und auf welcher Grundlage durchgeführt werden, und wer dafür verantwortlich ist. Dazu wird ein ISDS-Konzept mit den im Einzelfall notwendigen Anhängen (z. B. Risikoanalyse, Rollen- und Berechtigungskonzept, Verträge mit Auftragsbearbeitern) erstellt. Die ISDS-Dokumentation dient dabei jedoch nicht nur den kontrollierenden Stellen. In erster Linie dient sie dem Projekt selbst, in dem damit dokumentiert wird, dass die Projektverantwortlichen wissen, was für eine Applikation sie einführen wollen, was die damit verbundenen Risiken sind und welche Massnahmen zu deren Senkung getroffen werden. So wird einerseits nachgewiesen, dass bei der Planung mit der notwendigen Sorgfalt vorgegangen wurde, andererseits wird nur so ein angemessenes Risikomanagement im laufenden Betrieb möglich.

Bei den im Berichtsjahr durchgeführten Vorabkontrollen stellte die FADS fest, dass der grösste Teil ihrer Beanstandungen nicht die geplante Applikation selbst betraf, sondern deren Dokumentation und, daraus folgend, das Risikomanagement für den laufenden Betrieb. So wurden die geplanten Applikationen (oder Teile davon) oft unzureichend beschrieben, es fehlten wichtige Beilagen wie ein Berechtigungs- oder ein Löschkonzept, oder die mit den Lieferanten abgeschlossenen Verträge regelten die Einhaltung der datenschutzrechtlichen Vorgaben nicht ausreichend. Auch bei den Risikoanalysen konnte immer wieder festgestellt werden, dass Risiken offensichtlich unvollständig oder unrealistisch eingeschätzt wurden, so dass notwendige Sicherheitsmassnahmen in der Planung fehlen. Es wurde klar, dass das Wissen um die korrekte Erstellung einer ISDS-Dokumentation in der Verwaltung kaum vorhanden ist.

In der Stadtverwaltung ist ein Lernprozess im Gang, der auch in den folgenden Jahren weitergeführt werden muss.

Im Bewusstsein, dass zum Thema Vorabkontrolle nicht nur die FADS selbst, sondern alle Beteiligten einen Lernprozess durchlaufen müssen, ist die FADS im Berichtsjahr dazu über gegangen, anstelle eines Vorabkontrollberichtes mit umfangreicher Befundliste mit den Beteiligten einen Beratungsprozess anzustossen, in dessen Verlauf sie die nötige Hilfestellung dazu gibt, dass die Verantwortlichen die ISDS-Dokumente gezielt bereinigen können. Die FADS erachtete dieses Vorgehen als effiziente Variante, da so gleichzeitig das Knowhow der Beteiligten verbessert und ein ausufernder Schriftenwechsel verhindert werden konnte.

Allerdings war dies mit einem erheblichen Mehraufwand für die FADS verbunden. Dieser Mehraufwand erscheint aktuell als gerechtfertigt, da viele Beteiligte zum ersten Mal mit dem ISDS-Prozess und der Vorabkontrolle bei der FADS konfrontiert sind. Es war für die FADS denn auch bereits feststellbar, dass sich das Wissen und das Verständnis dazu verbessert hat.

Die für den Datenschutz und die Datensicherheit wesentlichen Parameter sollten bereits bei der Beschaffung einer Applikation berücksichtigt werden.

Es wird jedoch unumgänglich sein, das Know-how der gesamten Verwaltung in diesem Bereich zu verbessern. Einerseits kann nur so sichergestellt werden, dass die Vielzahl von IT-Projekten in der Stadt im Bereich Datensicherheit und Datenschutz gut aufgestellt ist, andererseits ist eine Entlastung der FADS notwendig, damit diese allen ihren Aufgaben gerecht werden kann. Bereits im Berichtsjahr hat sie die ICT-Sicherheit dabei unterstützt, die der Verwaltung zur Verfügung gestellten Vorlagen zur Erstellung einer ISDS-Dokumentation zu überarbeiten und so benutzerfreundlicher zu machen. Zudem hat sie ihre Beteiligung an verwaltungsinternen Schulungen zugesagt.

Für alle Beteiligten kann der Aufwand zudem massgeblich gesenkt werden, indem bereits bei der Beschaffung einer neuen Applikation die für den Datenschutz und die Datensicherheit wesentlichen Parameter festgelegt, beim Hersteller die diesbezüglichen Informationen eingeholt und der Vergabeentscheid gestützt auf diese Informationen gefällt wird. In den Projekten selbst muss vermehrt darauf geachtet werden, dass die notwendigen Ressourcen zur Planung angemessener Massnahmen zu Datenschutz und Datensicherheit sowie zum Erstellen der ISDS-Dokumentation und das Durchlaufen der beiden Prüfprozesse eingeplant werden. Die zur Digitalisierung der Stadtverwaltung aufgestockten Ressourcen müssen zwingend auch in diesem Bereich eingesetzt werden. Nur so ist sichergestellt, dass die Stadt Bern ihr selbst gestecktes Ziel, bei ihrer Digitalisierung vorbildlich vorzugehen, erreichen kann. Diverse, in jüngster Zeit bekannt gewordene Datenschutzvorfälle bei öffentlichen Verwaltungen zeigen, wie wichtig es ist, dieses Ziel ernst zu nehmen und die Themen Datenschutz und Datensicherheit mit der nötigen Sorgfalt zu behandeln.

3

Schwerpunktthema: Microsoft als Auftragsdatenbearbeiterin der Stadt Bern

Der Gemeinderat hat die Nutzung von Microsoft 365 in der Stadt Bern freigegeben, wobei er den Forderungen der FADS weitgehend gefolgt ist. Die Datenschutzkonformität der konkreten Implementierung in der Stadtverwaltung und in der Schulinformatik wird durch die FADS im Rahmen zweier Vorabkontrollen geprüft. Diese waren Ende Berichtsjahr noch nicht abgeschlossen.

Auch bereits in Betrieb genommene Applikationen von Microsoft beschäftigten die FADS. So untersuchte sie, ob die Stadt Bern von einem im Berichtsjahr bekannt gewordenen Datensicherheitsvorfall betroffen war.

Microsoft 365 in der Stadtverwaltung und der Schulinformatik

Wie viele andere Gemeinden hat sich auch die Stadt Bern dazu entschlossen, künftig auf Microsoft 365 (M365) zu setzen. Der Gemeinderat hat mit Beschluss vom 5. Juli 2023 dessen Nutzung für die Bürokommunikation freigegeben. Er hat sich mit den damit verbundenen grundsätzlichen Risiken auseinandergesetzt und ist zum Schluss gelangt, dass diese für die Stadt Bern tragbar seien. Dem Gemeinderatsbeschluss voraus gegangen ist ein intensiver Austausch zwischen der FADS und den für das Programm M365 Verantwortlichen in der Präsidialdirektion und den Informatikdiensten der Stadt Bern, in dem Nutzen und Risiken beim Betrieb von M365 vertieft behandelt wurden.

Die Nutzung von M365 in öffentlichen Verwaltungen ist umstritten und wird in der Schweiz und im europäischen Ausland bereits seit einiger Zeit viel diskutiert. Microsoft verfolgt mit dem Produkt die Strategie, dass Kund*innen bei der Nutzung von M365 ihre Daten nicht mehr lokal auf der eigenen Infrastruktur, sondern auf Cloud-Servern von Microsoft bearbeiten. Damit wird ermöglicht, dass die Nutzer*innen einfach und ortsunabhängig zusammenarbeiten können, womit ein dringendes Bedürfnis der modernen Arbeitswelt bedient wird. Zudem bringt dieser Ansatz den Kunde*innen wirtschaftliche Vorteile, und durch die Nutzung zentral verwalteter Applikationen auf zentral verwalteter Infrastruktur soll es einfacher werden, die Systeme insbesondere auch sicherheitstechnisch auf dem neuesten Stand zu halten. Microsoft wirbt dabei mit einem breiten Know-How auf dem Gebiet der Informatiksicherheit.

Aus dem Blickwinkel des Datenschutzes ist M365 jedoch mit namhaften Risiken verbunden. Durch die Bearbeitung auf fremden Servern verlieren Kund*innen die Kontrolle über ihre Daten. Sie wissen nicht mehr genau, wo sich welche Daten befinden und ob diese nur für die vorgesehenen Zwecke verwendet werden. Bekannt wurde zudem die Problematik, dass durch die Verwendung von M365 möglicherweise ausländische Behörden Zugriff auf über M365 bearbeitete Daten erhalten, ohne dass die davon betroffenen Personen sich in einem

rechtsstaatlichen Verfahren dagegen oder gegen deren Weiterverwendung wehren könnten. Zwar sichert Microsoft vertraglich zu, dass Personendaten nur zu den vorgesehenen Zwecken und unter Einhaltung aller gesetzlicher Bestimmungen in der Schweiz bearbeitet werden. Dies lässt sich durch die Kund*innen jedoch nicht wirksam überprüfen, zumal Microsoft nicht in allen Bereich transparent über das Produkt und die damit einhergehenden Datenbearbeitungen durch die Anbieterin selbst informiert.

Sind diese Kund*innen Behörden von Bund, Kantonen oder Gemeinden, können sie so nicht mehr ohne Weiteres sicherstellen, dass die Persönlichkeitsrechte der davon betroffenen Bevölkerung gewahrt bleiben. Ausserdem könnte sich auch die Einhaltung gesetzlicher Geheimhaltungspflichten (z. B. Amtsgeheimnis) als schwierig erweisen. Dabei befinden sich die Behörden aufgrund der Marktmacht von Microsoft und des bekannten Lock-In-Effekts in einem Abhängigkeitsverhältnis. So können sie sich nicht mehr frei für das passendste und datenschutzfreundlichste Produkt entscheiden.

Im Rahmen des eingangs erwähnten Austauschs hat die FADS daher darauf hingewirkt, dass sich die Verantwortlichen vertieft und mit der nötigen Sorgfalt mit diesen Risiken auseinandersetzen und geeignete Massnahmen ergriffen werden, um die Risiken auf ein vertretbares Mass zu senken. Sie führte zu diesem Zweck während mehreren Monaten regelmässige Gespräche und legte darüber hinaus ihren Standpunkt in mehreren formellen Stellungnahmen ausführlich dar und machte Verbesserungsvorschläge. Die Stellungnahmen wurden dem Gemeinderat zur Vorbereitung seines Beschlusses vorgelegt.

Die FADS zielte dabei in erster Linie in folgende Richtungen:

– Sie forderte, dass die Beurteilungen sämtlicher Risiken nachvollziehbar und realistisch erfolgt.
– Darüber hinaus forderte sie, dass beim Einsatz von M365 ein hybrider Betrieb aufrechterhalten werden muss, der es erlaubt, besonders schützenswerte Personendaten oder durch ein gesetzliches Geheimnis geschützte Informationen weiterhin lokal zu bearbeiten sowie
– dass eine umsetzbare Exit-Strategie vorliegt, welche es der Stadt ermöglicht, aus M365 und der MS-Cloud auszusteigen, falls es sich zeigen solle, dass eine rechtskonforme Datenbearbeitung damit nicht (mehr) möglich ist.

Der Gemeinderat hat die Nutzung von M365 in der Folge nicht ohne Weiteres freigegeben. Vielmehr erfolgte der Beschluss im Lichte folgender zusätzlicher Massnahmen:

– Im Juni des Berichtsjahres wurde die Weisung Cloud Computing der Stadt Bern erlassen. Diese legt über M365 hinaus für sämtliche städtischen Applikationen fest, welche Anforderungen diese erfüllen müssen, wenn sie in der Cloud betrieben werden.
– Daraus folgend wurde festgelegt, dass M365 nur für die Bürokommunikation genutzt werden darf. Systematische Bearbeitungen besonders schützenswerter Personendaten oder geheimnisgeschützter Informationen müssen dagegen in Fach-Applikationen erfolgen, welche höheren Sicherheitsanforderungen genügen müssen.
– Mit Hilfe der im Februar des Berichtsjahres erlassenen und ebenfalls übergeordnet geltenden Klassifizierungsweisung sind sämtliche Dokumente zu klassifizieren und demzufolge ausschliesslich an dafür freigegebenen Ort zu bearbeiten.

In diesem Sinne folgte der Gemeinderat der Forderung der FADS nach Aufrechterhaltung eines hybriden Ansatzes. Darüber hinaus forderte er ein den Risiken angemessenes Risikomanagement auch während des Betriebes von M365 und folgte damit weitgehend den übrigen Forderungen der FADS auf grundsätzlicher Ebene.

Inwiefern diese auf grundsätzlicher Ebene beschlossenen Massnahmen tatsächlich zu einem datenschutzkonformen Betrieb von M365 führen, zeigt sich in der konkreten Implementierung der Applikation in der Stadt Bern. Die FADS setzt sich in erster Linie im Rahmen von Vorabkontrollen damit auseinander und

überprüft dabei die geplante Einführung der einzelnen Komponenten von M365 im Detail.

Die Vorbereitungsarbeiten dazu wurden zeitgleich mit der Vorbereitung des gemeinderätlichen Beschlusses in Angriff genommen und durch die FADS ebenfalls eng begleitet. Sie erhielt für die Einführung von M365 in der Stadtverwaltung und der Schulinformatik je ein ISDS-Konzept inkl. weitere Dokumente und unterstützte die Verantwortlichen in der Folge bei den Verbesserungsarbeiten, indem sie die Dokumente laufend auf die Erfüllung der formellen Anforderungen im Vorabkontrollverfahren überprüfte und Verbesserungsvorschläge machte. Zudem wirkte sie darauf hin, dass auch in materieller Hinsicht die für einen datenschutzkonformen Betrieb wichtigen Weichen frühzeitig richtig gestellt werden.

In den anschliessend eröffneten Vorabkontrollen zeigte sich, dass die Arbeiten dazu sowie insbesondere diejenigen zur Verbesserung diverser, von der FADS in jeweiligen Zwischenberichten festgehaltener Mängel aufwändig und komplex sind. Die beiden Vorabkontrollverfahren konnten daher im Berichtsjahr noch nicht abgeschlossen werden.

Auswirkungen Diebstahl MS-Kontosignaturschlüssel auf die Stadt Bern

Im Mai des Berichtsjahres war mutmasslich von der chinesischen Gruppe «Storm-0558» ein Kontosignaturschlüssel von Microsoft entwendet worden, welcher für die Anmeldung von Endnutzern bei Microsoft Diensten wie Outlook-Online verwendet werden konnte. Der Diebstahl wurde nicht von Microsoft selbst bemerkt, sondern von einem Kunden, bei dem Intrusion-Detection-Mechanismen aufgrund von auffälligen Einträgen in Cloud-Logdateien Alarm geschlagen hatten. Die FADS hat über diesen Vorfall via Medienberichterstattung erfahren und die ICT-Sicherheit angefragt, ob in der MS-Infrastruktur der Stadt Bern ein unberechtigter Zugriff auf Daten mit Hilfe des gestohlenen Signaturschlüssels stattgefunden habe.

Die ICT-Sicherheit meldete der FADS zurück, dass die zur Klärung dieser Frage notwendigen Logdateien im zum Zeitpunkt des Vorfalls genutzten Lizenzmodell der Stadt Bern nicht enthalten waren. So konnte nachträglich nicht festgestellt werden, ob ein unberechtigter Zugriff auf die MS-Ressourcen der Stadt Bern mit dem gestohlenen Signaturschlüssel stattgefunden hatte. Konkret bedeutete dies für die Stadt Bern, dass sie sich auf die Mitteilung von Microsoft verlassen musste, wonach betroffene Kunden durch Microsoft eigenständig kontaktiert wurden. Da die Stadt Bern keine entsprechende Benachrichtigung erhalten hatte, wurde davon ausgegangen, dass sie von dieser Problematik nicht betroffen war und keine unberechtigten Zugriffe auf Daten der Stadt Bern stattgefunden hatten. Die FADS teilte daraufhin der ICT-Sicherheit mit, dass sich die Stadt Bern so organisieren sollte, dass sie bei künftigen Sicherheitsvorfällen in der Lage ist, eigenständig Untersuchungen anzustellen. Dies ist aus Sicht der FADS zwingend notwendig, um dem Kontrollverlust begegnen zu können, der mit der Nutzung von Cloud-Lösungen einhergeht.

Eigene Untersuchungen anstellen zu können ist aus Sicht der FADS zwingend notwendig, um dem Kontrollverlust begegnen zu können, der mit der Nutzung von Cloud-Lösung einhergeht.

4

Erfahrungsaustausche, Vernetzung, Weiterbildung und Öffentlichkeitsarbeit

Erfahrungsaustausche

- Regelmässige Austauschgespräche mit der ICT-Sicherheit der Stadt Bern
- Wiederkehrende Austauschgespräche mit Digital Stadt Bern
- Wiederkehrende Austauschgespräche mit Legislativstellen der Stadt Bern
- Austauschgespräche mit GPK und einem Ausschuss der GPK zu personellen, organisatorischen und fachlichen Themen
- Austauschgespräch mit DSA Stadt Zürich und Kanton BS betreffend CSN und Datenhaltung OIZ, wiederkehrend telefonisch sowie einmalig vor Ort, Zürich, 23.02.2023
- Austausch mit den DSA Basel-Stadt und der Städte Winterthur und St. Gallen zum Pilotbetrieb einer digitalen Wohnsitzbestätigung, 07.03.2023
- Austausch mit Vertreter*innen der Direktionen der Stadt Bern betreffend Vorgehen für Bewilligungen Videoüberwachung, Bern, 23.03.2023
- Austauschgespräch mit DSA Kanton Bern zu M365, 16.05.2023
- Austauschgespräch mit dem Rechtsdienst der Kantonspolizei Bern betreffend Koordination Bewilligungsverfahren Videoüberwachung, Bern, 05.12.2023

Vernetzung

- Kennenlerngespräche mit der Stadtkanzlei, Bern, 09.03.2023
- Antrittsbesuch beim Ratssekretariat der Stadt Bern, Bern, 13.03.2023
- Kennenlerngespräche mit den Mitgliedern KDSB Stadt Bern, Bern, 09.03.–23.03.2023
- Kennenlerngespräch mit DSA Kanton Bern, Bern, 31.03.2023
- Privatim Frühjahrsplenum 2023, Brunnen, 03.–04.05.2023
- Privatim Arbeitsgruppe ICT, Luzern, 22.03.2023
- Privatim Arbeitsgruppe ICT, Bern, 05.07.2023
- Privatim Arbeitsgruppe ICT, Basel, 13.09.2023
- Privatim Arbeitsgruppe ICT, Aarau, 15.11.2023
- Präsentation FADS bei der Direktion BSS, Bern, 22.06.2023

Weiterbildungen

- Div. Einführungsmodule für neue Führungskräfte des Personalamtes der Stadt Bern
- 27. Symposium on Privacy and Security, Stiftung für Datenschutz und Informationssicherheit, online-Teilnahme, 14.06.2023
- E-Government Event «Cloud & Behörden», Inside-IT, FIFA-Museum Zürich, 25.10.2023
- Kurs IT für Juristinnen und Juristen, privatim, Olten, 07.12.2023

Öffentlichkeitsarbeit

- Video-Beitrag zur Ausstellung Anti-Surveillance Fashion, Kornhausforum Bern, 15.09.–22.10.2023
- Teilnahme an Podiumsdiskussion «Gesichtserkennung und Datenschutz im öffentlichen Raum: Wie weiter?», Polit-Forum Bern, 17.10.2023

5

Statistik

Wie die Statistik für das Jahr 2023 zeigt: Das Instrument der Vorabkontrolle ist in der Stadtverwaltung angekommen. Die FADS hat im Berichtsjahr eine deutlich höhere Zahl solcher Kontrollen durchgeführt. Die Anzahl der Beratungen ist dagegen zurückgegangen, die Geschäfte sind dabei aber komplexer geworden. Die Themenschwerpunkte lagen bei Kontrollen oder Beratungen zu neuen Applikationen und zu Videoüberwachungen.

Mit der Trennung von der Ombudsstelle hat die Fach- und Aufsichtsstelle Datenschutz ihre Statistik umgestellt. Zwar unterscheidet sie wie bisher zwischen Fällen und Anfragen. Fälle benötigen eine vertiefte Abklärung und intensivere Beratung. Als Anfragen werden Anliegen erfasst, welche mit geringem Aufwand beantwortet werden können. Neu werden jedoch nicht mehr nur die im Berichtsjahr erledigten, sondern alle in dieser Periode bearbeiteten Fälle ausgewiesen. Dies drängte sich aus folgenden Gründen auf:

In erster Linie hat sich die Art der Geschäfte, welche der FADS im Berichtsjahr unterbreitet wurden, auffällig verändert. Die Fälle wurden komplexer und aufwändiger. So wurden z. B. diverse Projekte, welche in den vorangehenden Jahren vorbereitet wurden und dort eine Vielzahl einzelner, einfacherer Beratungsanfragen generiert haben, im Berichtsjahr der FADS zur Vorabkontrolle eingereicht. Wie im Kapitel 2 beschrieben, hat die FADS bei Vorabkontrollen, in welchen Befunde mit hoher Wesentlichkeit zutage getreten sind, auf eine beratende Zusammenarbeit mit den Verantwortlichen gesetzt, um das Projekt auf einen datenschutzkonformen Stand zu bringen. Es erreichten die FADS auch komplexere Beratungsanfragen, welche sie ebenfalls in einem iterativen Vorgehen zusammen mit den Verantwortlichen bearbeitet hat. Da auf diese Weise nur ein einzelnes Geschäft und nicht mehr eine Vielzahl, voneinander losgelöster Fälle ausgelöst wurden, erscheinen in der Statistik weniger, dafür umfassendere Geschäfte.

Solche Geschäfte konnten jedoch oft nicht mehr innerhalb des Berichtsjahres abgeschlossen werden. Da die Hauptarbeiten dazu aber im Berichtsjahr angefallen sind, ist die FADS dazu übergegangen, in der Statistik nicht mehr nur die im Berichtsjahr erledigten, sondern alle in der Zeit bearbeiteten Geschäfte abzubilden, um ein korrektes Bild ihrer Tätigkeit zu vermitteln. Um einen Vergleich mit dem Vorjahr zu ermöglichen, wurden vorliegend die Fallzahlen des Jahres 2022 auf das neue System umgerechnet und neben den Zahlen des Berichtsjahres aufgeführt. Diese Zahlen unterscheiden sich in der Folge von denjenigen, die nach

dem alten System berechnet im Tätigkeitsbericht 2022 aufgeführt wurden.

Daraus ergibt sich folgendes Bild: Im Berichtsjahr wurden insgesamt 88 Fälle bearbeitet (Vorjahr 119). Von 70 neu eröffneten und 18 aus dem Vorjahr übertragenen Fällen konnten 60 abgeschlossen werden. 28 Fälle wurden zur Weiterverarbeitung auf das Folgejahr übertragen.

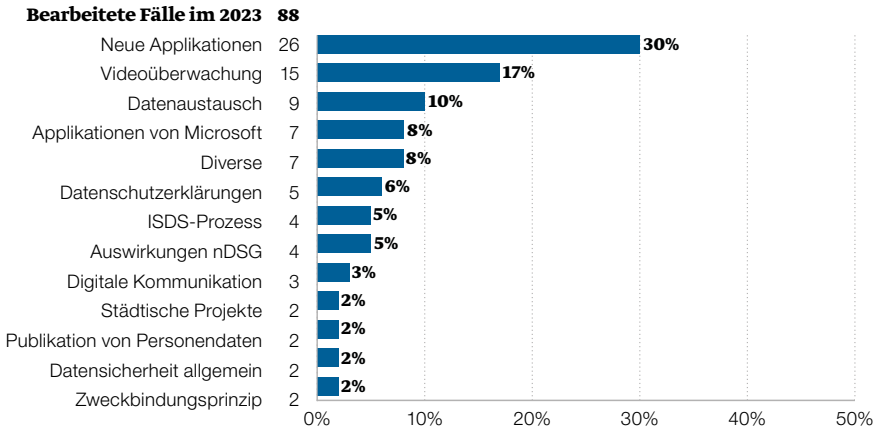
Die Anzahl der bearbeiteten Fälle hat gegenüber dem Vorjahr um rund 25% abgenommen, wobei die Abnahme aus den erwähnten Gründen bei den verwaltungsinternen Fällen zu verzeichnen ist, welche von 107 im Vorjahr auf 74 gesunken sind. Innerhalb dieser Fälle sind es vorab Beratungsgeschäfte, die zu dieser Abnahme geführt haben (im Berichtsjahr 45 Beratungen, im Vorjahr 83).

Zugenommen hat hingegen die Anzahl der Vorabkontrollen. Während die Datenschutz-Aufsichtsstelle im Jahr 2022 9 Vorabkontrollen bearbeitet hat, waren es im Berichtsjahr bereits 15, darunter sehr komplexe Fälle wie z. B. Microsoft 365.

Kennzahlen Gesamtübersicht	2023	2022
Fälle	**88**	**119**
Fälle aus dem Vorjahr	18	18
Neu eröffnete Fälle	70	101
Anfragen	**46**	**62**
Total Fälle und Anfragen	**60**	**101**
Pendent per Ende Jahr	28	18

Kennzahlen bearbeitete Fälle	2023	2022
bearbeitete Fälle von Privatpersonen	**14**	**12**
Beratung	7	8
Aufsichtsrechtliche Anzeigen	7	4
bearbeitete Fälle Verwaltung und Betriebe	**74**	**107**
Beratung	45	83
ISDS-Workshop	32	
Review	10	
Beratung im engeren Sinn	3	
Nachträgliche Überprüfung	7	6
Vorabkontrolle	15	9
Audit	0	0
Formelle Stellungnahme	1	1
Führen Register der Datensammlung	1	0
Umsetzung Empfehlungen	1	4
Eigene Untersuchung	**4**	**4**

Anteile der bearbeiteten Fälle pro Verwaltungsbereich



Werden die Dossiers pro Themenbereich betrachtet, ergibt sich folgendes Bild: Knapp ein Drittel der Fälle (30%) betrafen geplante oder in der Stadtverwaltung neu eingeführte Applikationen. In diese Kategorie fallen sowohl Vorabkontrollen, in denen geplante Applikationen durch die FADS geprüft wurden, als auch Beratungen, welche oftmals der Vorbereitung einer künftigen Vorabkontrolle gedient haben. Im Bereich Videoüberwachung (17%) hat die FADS Vorabkontrollen, Beratungen und eine aufsichtsrechtliche Anzeige behandelt. Zum Thema Datenaustausch war die FADS beratend tätig, wohingegen die Applikationen von Microsoft schwerpunktmässig im Rahmen der aufsichtsrechtlichen Tätigkeit und damit einhergehenden Beratungen behandelt wurden.

Eine Besonderheit war im Berichtsjahr das Inkrafttreten des neuen Datenschutzgesetzes des Bundes per 1. September 2023 (nDSG). In diesem Zusammenhang erhielt die FADS einige Anfragen von Seiten der Stadtverwaltung (2%). Im Vordergrund stand dabei die Frage, ob städtische Behörden in den Anwendungsbereich des neuen Gesetzes fallen, wozu die FADS jeweils eine Einschätzung abgegeben hat. Hinsichtlich inhaltlicher Frage zur Anwendung und Auslegung des nDSG wurde jeweils auf die Zuständigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hingewiesen.

6

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.

Videoüberwachung

Velostationen Milchgässli, Postparc, Schanzenbrücke, Welle 7 und Bollwerk

Zu den in den städtischen Velostationen betriebenen Videoüberwachungen wurden im Berichtsjahr die Vorabkontrolle bei der FADS und das Rückspracheverfahren bei der Kantonspolizei durchgeführt. Die Anlagen durchlaufen damit nachträglich die im kantonalen Polizeigesetz und im städtischen Videoreglement vorgesehenen Bewilligungsprozesse.

In den städtischen Velostationen wurden jahrelang Videoüberwachungsanlagen betrieben, ohne dass das Verfahren nach Polizeigesetz und Videoreglement durchgeführt und die erforderliche Bewilligung des Stadtrats eingeholt wurde. Aufgrund entsprechender Medienberichterstattungen reagierte der Gemeinderat und ordnete mit Beschluss vom 1. Februar 2023 die sofortige Einstellung der Videoüberwachungen und die Einleitung der dafür vorgesehenen Bewilligungsverfahren an. In einem ersten Schritt wurde der FADS die ISDS-Dokumentation für die Velostation Postparc eingereicht.

Die FADS hat diese in einer ersten Prüfung beurteilt und eine Befundliste i. S. eines Reviews zugestellt. Nach einer Besprechung der Befunde wurden die ISDS-Dokumente von TVS überarbeitet. Wie in der Besprechung vereinbart wurde dabei für die Velostationen Postparc, Schanzenbrücke, Welle 7 und Bollwerk ein gemeinsames ISDS-Konzept erstellt, da die datenschutzrechtlich relevanten Punkte bei diesen Stationen identisch sind. Für die Velostation Milchgässli wurde demgegenüber ein separates Konzept erstellt, weil diese sich im Bahnhofareal befindet und die betreffende Videoüberwachung in Teilen ebenfalls der Transportpolizei der SBB zu bahnpolizeilichen Zwecken dient. Die FADS hat die Dokumente geprüft. Zur Klärung der noch offenen Fragen wurde eine Besprechung mit Besichtigung vor Ort durchgeführt. Nachdem alle offenen Fragen bei dieser Gelegenheit bereinigt werden konn-

ten, hat die FADS in ihrem Schlussbericht zur Vorabkontrolle festgehalten, dass die Videoüberwachung in den Velostationen datenschutzkonform betrieben werden kann. Die Kantonspolizei Bern hat sich in ihrem Rückspracheverfahren der Beurteilung durch die FADS angeschlossen. Der gemäss Videoreglement notwendige Beschluss des Stadtrates war im Zeitpunkt der Berichtsredaktion noch ausstehend.

Neue 50m-Schwimmhalle Neufeld

Ebenfalls als Videoüberwachung zum Schutz öffentlicher Gebäude und deren Benutzenden im Sinne des Polizeigesetzes wurde die für die neue 50m-Schwimmhalle Neufeld geplante Anlage zur technischen Wasserüberwachung behandelt. Bei der Vorabkontrolle legte die FADS ihren Fokus auf die eingesetzten KI-Komponenten.

Die Anlage besteht aus einem Algorithmus-basierten Überwachungssystem (KI) mit Oberwasserkameras, deren Echtzeitbilder durch maschinelle Bildverarbeitung in Bewegungsmuster umgewandelt und anschliessend gelöscht werden. Mittels künstlicher Intelligenz werden daraus auffällige Bewegungsmuster von sich mutmasslich in Not befindlichen Badegästen detektiert, und es erfolgt eine Alarmierung auf Smart-Watches der Badeaufsicht. Zusätzlich werden Echtzeitbilder der Schwimmbecken auf einen Bildschirm in die Loge der Badeaufsicht übertragen; eine Speicherung erfolgt hier nicht. Ferner nimmt das System statistische Auswertungen ohne Personenbezug über die Belegung und Auslastung der Schwimmbecken vor. Nach Vorbesprechungen im Jahre 2022 unterbreitete das Sportamt der FADS im Frühling 2023 ISDS-Unterlagen zur Vorabkontrolle. Nach einer summarischen Prüfung gab die FADS eine erste Einschätzung mit den zunächst wesentlichsten Befunden ab. Im Rahmen eines Austausches mit dem Sportamt konnten diese Befunde besprochen werden. Gestützt darauf wurden der FADS überarbeitete ISDS-Dokumente zur Prüfung eingereicht, worauf die FADS einen ersten Prüfbericht erstattete. Da ein datenschutzkonformer Betrieb der Anlage zu diesem Zeitpunkt noch nicht möglich war, erfolgte die Eröffnung der Schwimmhalle Neufeld im Herbst 2023, ohne dass die Wasserüberwachungsanlage in Betrieb genommen wurde. Zur Klärung der offenen Fragen waren weitere Besprechungen, unter anderem auch mit dem Hersteller des Systems, erforderlich. In der Folge wurden der FADS gegen Ende 2023 finale ISDS-Dokumente eingereicht. Vor der Redaktion des vorliegenden Berichts konnte die hängige Vorabkontrolle abgeschlossen und das weitere Verfahren zur Bewilligung der Anlage durch den Stadtrat eingeleitet werden.

Für die FADS war hier von besonderer Bedeutung, dass allfälligen Risiken für die Persönlichkeitsrechte der Betroffenen durch den Einsatz von künstlicher Intelligenz mit angemessenen Massnahmen begegnet wurde. So konnte im Dialog mit dem Sportamt und dem Hersteller geklärt werden, dass die im Betrieb gewonnenen Bewegungsmuster lediglich zur Verbesserung des lokalen Algorithmus verwendet werden. Nebst dem lokalen existiert zwar auch ein globaler Trainingsdatensatz, der mit Trainingsdaten von allen Standorten erweitert wird, welche das Produkt einsetzen. Die Synchronisation der Trainingsdaten vom lokalen Server in der Schwimmhalle Neufeld in den globalen Algorithmus des Herstellers geschieht laufend. Dabei werden jedoch nach Angaben des Herstellers nur anonymisierte und aggregierte Daten übermittelt, welche Statistiken über Systemleistung, Fehlalarme und Erkennungsgenauigkeit beinhalten. Somit werden durch den Hersteller keine personenbezogenen Daten zu eigenen Zwecken verarbeitet, und dem Grundsatz der Zweckbindung wird entsprochen.

Die im Betrieb gewonnenen Bewegungsmuster werden lediglich zur Verbesserung des lokalen Algorithmus verwendet.

Videoüberwachung beim Amt für Erwachsenen- und Kindesschutz

Ein weiteres Verfahren nach Polizeigesetz wurde vom Amt für Erwachsenen- und Kindesschutz (EKS) eingeleitet, welches für die Echtzeitüberwachung des Eingangs- und Empfangsbereichs eine Videoanlage benötigt. Die Anlage bezweckt den Schutz der Mitarbeitenden und anderen Anwesenden vor gefährlichen Situationen.

Hier wurde durch die verantwortliche Behörde direkt das Rückspracheverfahren bei der Kantonspolizei angestossen. Diese leitete die ISDS-Unterlagen an die FADS zwecks Durchführung der Vorabkontrolle weiter. Die Datenschutzbeauftragte der Stadt Bern nahm dieses Geschäft zum Anlass, sich mit der Kantonspolizei zwecks Koordination künftiger Verfahren auszutauschen. In der Folge verfasste die FADS den Prüfbericht zur Vorabkontrolle. Darin wurde festgehalten, dass die Videoüberwachungsanlage datenschutzkonform betrieben werden kann. Die Kantonspolizei teilte diese Auffassung in ihrer zustimmenden Stellungnahme. Auch dieses Geschäft wird dem Stadtrat vorgelegt werden.

Wärmebild und Videokameras an Lichtsignalanlagen

Das Tiefbauamt gelangte an die FADS mit der Bitte um Beurteilung, ob die Wärmebild- und Videokameras an Lichtsignalanlagen der Bewilligungspflicht nach Polizeigesetz und Videoreglement unterliegen.

Die FADS führte hier zwecks Beurteilung der Datenbearbeitung und des Schutzbedarfs einen ISDS-Workshop durch. Wie sich zeigte, bezwecken die Videokameras ausschliesslich die Identifikation von Fehlerverhalten und Behebung von Störungen an den Lichtsignalanlagen; der Bearbeitungszweck ist damit nicht personenbezogen. Zudem werden die Videokameras nur punktuell eingesetzt, und es erfolgen keine Aufzeichnungen. Die FADS konnte sich anhand von Beispielbildern davon überzeugen, dass die Bildauflösung so tief ist, dass ein Personenbezug mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen ist. Bei den Wärmebildkameras, welche der Ampelsteuerung dienen, ist ein Personenbezug von vornherein nicht möglich. Vor diesem Hintergrund hat die FADS auf die Durchführung einer Vorabkontrolle verzichtet. Eine Bewilligungspflicht nach Polizeigesetz konnte aufgrund des spezifischen Einsatzzweckes der Anlage ausgeschlossen werden.

Einsatz von Videokameras für das Verkehrsmonitoring

Die Abteilung Verkehrsplanung (VP) der Direktion für Tiefbau, Verkehr und Stadtgrün gelangte an die FADS zur Klärung der Frage, ob das Verkehrsmonitoring mit Videokameras der Pflicht zur Vorabkontrolle sowie der Bewilligungspflicht nach Polizeigesetz bzw. Videoreglement untersteht. Dabei ging es nicht um die Beurteilung eines konkreten Vorhabens, sondern um die Klärung des Vorgehens in allgemeiner Hinsicht.

Wie sich zeigte, dienen die Videoaufnahmen ausschliesslich der numerischen Quantifizierung der Verkehrsabläufe und werden nach erfolgter Auswertung gelöscht. Aufgrund der Darlegungen des nicht personenbezogenen Zwecks der Datenbearbeitung konnte zunächst darauf geschlossen werden, dass damit keine Videoüberwachung im Sinne des Polizeigesetzes vorliegt. Dafür sprach auch der Umstand, dass in der Vergangenheit die Durchführung der Monitorings jeweils der Kapo gemeldet wurde, ohne dass diese interveniert und eine Bewilligungspflicht nach Polizeigesetz geltend gemacht hätte. Offen blieb aber die Frage der Vorabkontrollpflicht; jedenfalls so lange die FADS keine nähere Kenntnis der konkreten Datenbearbeitung hat und die Möglichkeit eines Personenbezugs mit genügender Wahrscheinlichkeit ausschliessen kann. Hinzu kommt, dass die Abteilung VP die Monitorings nicht selbst durchführt, sondern dafür externe Firmen beauftragt. Für eine allfällige Datenbearbeitung durch den Auftragsbearbeiter hat die Behörde die Verantwortung zu übernehmen. Es wurde vereinbart, diese Fragen anhand eines konkre-

ten Monitoring-Vorhabens näher zu prüfen. Im Vorfeld wird VP ein Merkblatt analog zu demjenigen des Kantons Zürich ausarbeiten und der FADS zur Prüfung vorlegen. Das Merkblatt soll Bestandteil des jeweiligen Vertrages mit der beauftragten Firma bilden.

Videoüberwachung mit Gesichtserkennung durch städtische Behörden

Die FADS hat sich im Berichtsjahr wiederholt mit dem Thema Videoüberwachung mit Gesichtserkennung auseinandergesetzt. Der Fokus lag dabei auf den hierzu geltenden oder zu erlassenden rechtlichen Rahmenbedingungen in der Stadt Bern.

Ein im Berichtsjahr wiederholt an die FADS herangetragenes Thema betrifft die Überwachung des öffentlichen Grundes mittels Videokameras und Gesichtserkennung. Das Thema wird in der Schweiz aktuell breit diskutiert, und auch in der Stadt Bern bewegt es Bevölkerung und Politik. Die Anfragenden interessierte insbesondere, ob solche Überwachungen durch städtische Behörden bereits durchgeführt werden, unter welchen Bedingungen dies zulässig wäre und ob die Stadt Bern in diesem Bereich eigene Regelungen erlassen könnte.

Gemäss dem Kenntnisstand der FADS setzen die Behörden der Stadt Bern zurzeit keine Videoüberwachungen mit Gesichtserkennung ein. Damit sie dies dürften, müssten folgende Voraussetzungen erfüllt sein:

- Beim Einsatz derartiger Technologien werden Personendaten auf eine Art bearbeitet, die für die betroffenen Personen mit besonderen Risiken verbunden ist. Daher muss ein solches Projekt vor Inbetriebnahme der Überwachungsanlage durch die FADS auf die Einhaltung des Datenschutzes hin überprüft werden. Die FADS würde dabei der im Rahmen der Gesichtserkennung erfolgenden Bearbeitung biometrischer Daten besondere Aufmerksamkeit schenken. Biometrische Daten sind untrennbar mit einer Person verbunden, und deren missbräuchliche Verwendung kann für die Betroffenen schwerwiegende Folgen haben. Aus diesem Grund rechtfertigen sich strenge Anforderungen an solche Datenbearbeitungen. Im Entwurf zum revidierten Kantonalen Datenschutzgesetz werden sie denn auch explizit als besonders schützenswerte Personendaten aufgeführt.
- Die Videoüberwachung muss gestützt auf das kantonale Polizeigesetz durch die Kantonspolizei bewilligt werden.
- Gemäss den Bestimmungen des städtischen Videoreglements muss die Videoüberwachung durch den Stadtrat angeordnet werden.

Biometrische Daten sind untrennbar mit einer Person verbunden, und deren missbräuchliche Verwendung kann für die Betroffenen schwerwiegende Folgen haben.

Die Stadt Bern kann den Einsatz solcher Technologien (sowohl die Videoüberwachung als auch die Gesichtserkennung) durch ihre eigenen Behörden regeln, soweit sie damit nicht übergeordnetes Recht verletzt. So wäre es z. B. denkbar, dass sie ihren Behörden generell untersagt, beim Vollzug des städtischen Rechts derartige Mittel einzusetzen, dass sie den Einsatz durch ihre Behörden einer Bewilligungspflicht unterstellt (was aufgrund des geltenden städtischen Videoreglements heute de facto bereits der Fall ist) oder anderweitig einschränkt. Nicht möglich wäre es hingegen beispielsweise, die für den Einsatz geltenden Regeln so zu erleichtern, dass die Persönlichkeitsrechte der Betroffenen nach Massgabe des KDSG verletzt würden. Es ist zudem denkbar, den Einsatz solcher Technologien durch Private auf öffentlichem städtischem Grund einer Bewilligungspflicht zu unterstellen.

Schwieriger wäre eine Regelung von solchen Überwachungen im öffentlichen Raum durch Private (mit oder ohne Gesichtserkennung). Eine Bewilligungspflicht rechtfertigen könnte der Umstand, dass die betroffenen Personen dadurch in ihrer Nutzung des öffentlichen Grundes eingeschränkt werden und die Situation damit z. B. vergleichbar ist mit derjenigen bei Restaurantbestuhlungen auf Trottoirs oder Veranstaltungen auf öffentlichem Grund.

Vermeintliche Videoüberwachung im Infopavillon zur Baustelle Hirschengraben

Im Infopavillon zur Baustelle Hirschengraben haben Piktogramme auf eine Videoüberwachung hingewiesen, obschon keine durchgeführt wurde. Die FADS hat sich mit der Frage auseinandergesetzt, ob dies beim von einer städtischen Behörde betriebenen Pavillon zulässig ist.

Die FADS wurde durch eine Bürgermeldung darauf aufmerksam gemacht, dass im kurz zuvor errichteten Infopavillon zur Baustelle am Hirschengraben Piktogramme auf eine Videoüberwachung hinweisen, obschon keine Kameras ersichtlich seien. Daher stelle sich die Frage, ob im Bereich des Infopavillons überhaupt eine Videoüberwachung durchgeführt wird und falls ja, ob diese bewilligt wurde. Falls keine Videoüberwachung durchgeführt werde, stelle sich dagegen die Frage, ob die Betreiber des Infopavillons mittels Piktogramme den falschen Anschein erwecken dürfen, dass der fragliche Bereich überwacht wird.

Da sich gezeigt hat, dass der Infopavillon zur Baustelle am Hirschengraben durch die Stadt Bern betrieben wird, hat die FADS bei der zuständigen Behörde nachgefragt, ob der Ort videoüberwacht wird. Aus der Antwort ging hervor, dass keine Videoüberwachung durchgeführt wird. Der Baucontainer, welcher Teil des Pavillons ist, würde jedoch von einer privaten Firma gemietet, welche die Aufkleber mit den Piktogrammen standardmässig an ihren Containern angebracht hätte.

Damit lag zwar keine durch die FADS zu beurteilende Videoüberwachung vor. Allerdings kann bereits die Verwendung von auf eine Überwachung hinweisenden Piktogrammen eine Wirkung auf das Verhalten der Betroffenen haben. So kann sie vor deliktischem Verhalten abschrecken, was an sich positiv zu beurteilen wäre. Andererseits entstehen so aber auch ein Beobachtungsdruck oder ein falsches Sicherheitsgefühl. Erweckt eine öffentliche Behörde durch Piktogramme den falschen Eindruck, dass ein bestimmtes Gebiet videoüberwacht wird, steht dies aber auch im Widerspruch zu ihrer Pflicht, sich gegenüber der Bevölkerung nach Treu und Glauben und damit transparent und wahrheitsgemäss zu verhalten.

Die FADS hat die verantwortliche Behörde auf diesen Widerspruch aufmerksam gemacht. Diese hat zugesichert, künftig zu prüfen, ob an den von ihr gemieteten Baucontainers Piktogramme angebracht sind und diese, falls nötig, abzudecken.

Koordination der Verfahren bei der Kantonspolizei und der FADS

Die Kantonspolizei Bern und die FADS haben sich bei geplanten städtischen Videoüberwachungen nach Polizeigesetz auf ein koordiniertes Vorgehen geeinigt. Damit wird das Verfahren zum Erlangen der vorgeschriebenen Bewilligungen übersichtlicher und unnötiger Aufwand durch Doppelspurigkeit vermieden.

Möchte eine Behörde der Stadt Bern zur Verhinderung und Ahndung von Straftaten auf öffentlichem Grund eine Videoüberwachung durchführen, braucht sie dazu die Bewilligung der Kantonspolizei. Zudem muss sie das Vorhaben der FADS zur Vorabkontrolle unterbreiten und anschliessend durch den Stadtrat bewilligen lassen. Vergleichbar ist die Situation bei städtischen Videoüberwachungen zum Schutz öffentlicher Gebäude und derer Nutzer*innen. Für Projektverantwortliche ist diese Situation unübersichtlich, zumal nicht ohne Weiteres klar ist, welcher Behörde in welchem Zeitpunkt welche Unterlagen einzureichen sind.

Die FADS hat sich daher mit dem Rechtsdient der Kantonspolizei Bern zur Frage ausgetauscht, wie das Bewilligungsverfahren nach Polizeigesetz und die datenschutzrechtliche Vorabkontrolle miteinander koordiniert werden können. Den Beteiligten ging es dabei nicht nur darum, das Vorgehen für die Projektverantwortlichen übersichtlicher zu gestalten. Vielmehr soll auch vermieden werden, dass dieselbe Kontrolle durch die Behörden wiederholt wird, wodurch zwar der doppelte Aufwand, aber kein wirklicher Mehrwert daraus resultieren würde. Zwar sollen die Behörden die vorgelegten Projekte unabhängig voneinander beurteilen können, aber in Kenntnis der relevanten Punkte aus der Prüfung der jeweils anderen Behörde. Die Beteiligten einigten sich dabei darauf, dass Verantwortliche ihr Gesuch einmalig bei der Kantonspolizei einreichen können. Diese leitet das Gesuch der FADS zur Vorabkontrolle weiter. Die FADS führt daraufhin die Vorabkontrolle gestützt auf das KDSG selbständig und unabhängig von der Kantonspolizei durch. Sie erstattet der für die Videoüberwachung verantwortlichen städtischen Behörden direkt ihren Vorabkontrollbericht und stellt der Kantonspolizei eine Berichtskopie zu. Anschliessend führt die Kantonspolizei in Kenntnis der datenschutzrechtlichen Einschätzung der FADS das Bewilligungs- resp. das Rückspracheverfahren nach Polizeigesetz durch. Sie stellt ihren Prüfbericht ebenfalls der verantwortlichen Behörde und, in Kopie, der FADS zu.

ISDS-Prozesse

Reviews von ISDS-Entwürfen und Vertragsvorlagen im Rahmen des Projektes SAP Go2HANA

Die FADS wurde Ende März des Berichtsjahres vom städtischen Projektleiter informiert, dass für die Erstellung der ISDS-Dokumente im Projekt SAP Go2HANA externe Unterstützung beschafft worden sei und bat um einen Austausch zur Klärung der Anforderungen seitens FADS zur Erstellung der ISDS-Dokumente.

Nebst Inhalt und Struktur des ISDS-Konzeptes wurde auch über die korrekte Ausweisung des Restrisikos diskutiert.

Die externen Mitarbeitenden stellten das geplante Vorgehen vor, pro SAP-Modul (bspw. HCM, Logistik, Immobilienmanagement) den Schutzbedarf der Daten zu ermitteln und die Verantwortlichkeiten zu definieren. Aufgrund der Grösse des Projektes wurde vereinbart, in einem regelmässigen Austausch zwischen der FADS, der IBE und den externen Mitarbeitenden den Fortschritt des Projektes darzulegen und sich über aktuelle datenschutzrechtliche Fragestellungen auszutauschen. Im Berichtsjahr fanden insgesamt fünf solcher Online-Meetings statt. Dabei wurde vorab über die in der Vorabkontrolle zentralen Prüfobjekte ISDS-Konzept und Risikoanalyse diskutiert. Grundlage dazu bildeten die Rückmeldungen der FADS zu den Entwürfen einzelner Kapitel des ISDS-Konzeptes und dem Entwurf der Risikoanalyse im Rahmen Ihrer beratenden Tätigkeit. Themen waren dabei die Dokumentation der gesetzlichen Grundlagen, die Zwecke der Datenbearbeitung in SAP, die Modellierung der Datenflüsse innerhalb der SAP-Module und zu Drittapplikationen sowie die dabei sicherzustellende Wahrung der Vertraulichkeit, die Integrität und Verfügbarkeit der Daten. Nebst Inhalt und Struktur des ISDS-Konzeptes wurde auch über die korrekte Ausweisung des Restrisikos diskutiert, welches nach der Umsetzung der in der Risikoanalyse dokumentierten, technischen und organisatorischen Massnahmen zum Zeitpunkt der Inbetriebnahme der Applikation besteht. Die FADS legte dar, dass gemäss Art. 8 KDSG die Risikoübernahme nicht durch ein Projektgremium, sondern durch die Funktionsträger der jeweiligen Verwaltungseinheiten zu erfolgen hat. Der Ent-

scheid darüber, auf welcher Stufe (Amt, Direktion) die Risikoübernahme bzw. Übernahme der Restrisiken erfolgt, obliegt jedoch den verantwortlichen Behörden. Auch die vom Projekt zugestellten Verträge wurden von der FADS einem Review unterzogen. Dabei wurde ersichtlich, dass aus dem Data Processing Agreement (DPA) nicht genügend klar hervorgeht, welche Personendaten SAP als Auftragsverarbeiter zu welchen Zwecken wie bearbeitet. Dieser Punkt muss von der verantwortlichen Behörde geklärt werden; entweder im Vertrag oder als vertraglich ausdrücklich vorgesehene nachträgliche Weisungen. Als weiterer offener Punkt im Vertragswerk wurde die Frage identifiziert, ob nebst den Gruppengesellschaften von SAP weitere Unterauftragsverarbeiter in die Datenbearbeitung involviert sind und inwieweit die Daten der Stadt Bern durch SAP für das Training von KI- und ML-Komponenten genutzt werden. Nach einer letzten Besprechung Ende Oktober 2023 endete das Mandat der externen Mitarbeitenden. Finale und freigegebene Versionen der ISDS-Dokumente zur ordentlichen Vorabkontrolle nach Art. 17a KDSG wurden der FADS bis zum Berichtszeitpunkt keine eingereicht.

Optimierung Compliance Check Prozess

Der ICT-Sicherheitsbeauftragte kontaktierte die FADS, um allfällige Optimierungen im Compliance Check Prozess bei einem Proof of Concept-Vorhaben (PoC) zu besprechen. Damit soll es für die verantwortliche Behörde einfacher werden, die grundsätzliche Durchführbarkeit einer geplanten Datenbearbeitung zu testen.

Der städtische Compliance Check Prozess dient zur Sicherstellung der Einhaltung der regulatorischen Vorgaben bei der Einführung einer neuen Applikation in der Stadt Bern und regelt u. a. die Zusammenarbeit zwischen der ICT-Sicherheit und der FADS in diesem Bereich. Wird anlässlich einer Schutzbedarfsanalyse ein erhöhter Schutzbedarf bei einem geplanten Vorhaben festgestellt, so sind ISDS-Dokumente zu erstellen, die aufzeigen, wie gesetzliche Vorgaben und Anforderungen des Datenschutzes und der Informationssicherheit eingehalten werden sollen und welche Restrisiken mit dem Betrieb der geplanten Applikation einhergehen. Nebst der Erstellung der ISDS-Dokumente hat die datenbearbeitende Behörde gemäss Art. 17a KDSG das geplante Vorhaben der FADS zur Vorabkontrolle vor Inbetriebnahme vorzulegen.

Im vorliegenden Fall gelangte der ICT-Sicherheitsbeauftragte an die FADS, um den Compliance Check Prozess für so genannte Proof of Concept-Vorhaben (PoC) zu vereinfachen. Falls das Ziel lediglich die Feststellung der prinzipiellen Durchführbarkeit eines Vorhabens ist, soll es der datenbearbeitenden Behörde ermöglicht werden, ein vereinfachtes ISDS-Konzept zu erstellen, welches nicht vorgängig von der FADS einer Vorabkontrolle unterzogen werden muss. Jedoch soll das ISDS-Konzept wie auch der zu erstellende Abschlussbericht der PoC-Phase durch die ICT-Sicherheit geprüft werden. Ist die grundsätzliche Durchführbarkeit des Vorhabens festgestellt und besteht die Absicht, die Applikation produktiv einzuführen, muss der ordentliche Compliance Check Prozess samt allfälliger Vorabkontrolle der FADS beschritten werden.

Der Idee eines vereinfachten PoC-Prozesses stand die FADS grundsätzlich offen gegenüber, und es wurde in mehreren Online-Meetings über Kriterien aus Sicht ICT-Sicherheit und Datenschutz diskutiert, die erfüllt sein müssen, damit es sich um einem PoC handelt. Demzufolge sollten PoCs, wenn immer möglich, mit Testdaten durchgeführt werden. Kann der Zweck des PoC nur durch die Bearbeitung personenbezogener Echtdaten erreicht werden, dürfen diese Echtdaten keine besonders schützenswerte Personendaten enthalten. Bei einer Bearbeitung von Personendaten mittels einer SaaS-Lösung muss zwingend ein Auftragsdatenverarbeitungsvertrag vorliegen, in dem die Datenbearbeitung des Anbieters geregelt ist und der sicherstellt, dass der Anbieter die Daten nur so bearbeitet, wie es dem öffentlichen Organ aufgrund der relevanten gesetzlichen Grundlagen ebenfalls gestattet ist. Die Einhaltung der Weisung Cloud Computing der Stadt Bern ist dabei durch die datenbearbeitende Behörde sicherzustellen.

Review ISDS POC Call Center Luware

Der Projektleiter für die Call Center-Lösung Luware gelangte mit einer Beratungsanfrage zum Vorgehen bei deren PoC-Betrieb (Proof-of-Concept) und der späteren produktiven Einführung an die FADS. Der PoC sollte mit personenbezogene Echtdaten durchgeführt werden.

Anlässlich eines ersten Austausches wurde der geplante PoC-Betrieb der Call Center-Lösung besprochen. Die Applikation setzt auf MS Teams auf, und der Betrieb wurde auf dem MS-Tenant der Schulinformatik geplant. Nach Information des Projektleiters werden alle Personendaten im MS-Teams geführt, in der neuen Applikation würden ausschliesslich Metadaten anfallen (wer telefoniert mit wem wie lange). Zeitlich war ein temporärer PoC-Betrieb von drei Monaten geplant, und der Kreis der Nutzenden wurde auf das Service Center der IBE eingeschränkt. Nach diesem Zeitraum sollte ein Entscheid gefällt werden, ob die Applikation für die Schul- sowie die Verwaltungsinformatik und möglicherweise auch in weiteren städtischen Call Center eingesetzt werden soll. Für den PoC-Betrieb existierte auch bereits ein ISDS-Konzept, welches anschliessend an die Besprechung der FADS zugestellt wurde.

Nach Sichtung dieses Konzeptes gelangte die FADS zur Ansicht, dass es sich beim geplanten Vorhaben nicht um einen PoC-Betrieb handelte, da die in Zusammenarbeit mit der ICT-Sicherheit erarbeiteten Kriterien für eine solchen Betrieb nicht erfüllt waren. Einerseits war geplant, die Applikation im produktiven MS-Tenant der Schulinformatik mit produktiven Daten (also keine Testumgebung und keine Testdaten) zu betreiben, und andererseits konnte die Bearbeitung von besonders schützenswerten Personendaten aufgrund von aufgezeichneten Sprachnachrichten aus Sicht Datenschutz nicht ausgeschlossen werden. Die FADS hatte jedoch Verständnis für das Anliegen, die Funktionalitäten des Contact Center vor der effektiven Beschaffung zu testen und stellte daher in Aussicht, für die Testphase auf eine ordentliche Vorabkontrolle zu verzichten.

Eine Überwachung von Mitarbeitenden durch die Funktionalitäten der Applikation (Reporting, Analysen etc.) muss ausgeschlossen werden.

Da es sich jedoch um einen produktiven Betrieb mit produktiven Echtdaten handelte, stellte die FADS folgende Bedingungen für den rechtskonformen Betrieb: Mit dem Auftragsdatenverarbeiter (Luware AG) ist ein Auftragsdatenverarbeitungsvertrag abzuschliessen, durch den sichergestellt wird, das Luware die Daten nur so bearbeitet, wie das öffentliche Organ dies darf (Art. 16 KDSG) und mittels technischer oder organisatorischer Massnahmen sichergestellt ist, dass eine Überwachung von Mitarbeitenden durch die Funktionalitäten der Applikation (Reporting, Analysen etc.) ausgeschlossen werden kann. Ferner ist nach Ende der Testphase und vor Inbetriebnahme des produktiven Betriebes zwingend der ordentliche Compliance Check Prozess in Zusammenarbeit mit der ICT-Sicherheit zu initiieren und die ISDS-Dokumente sind der FADS zur ordentlichen Vorabkontrolle gemäss Art. 17a KDSG einzureichen.

Im Anschluss an die Rückmeldungen zu den Bedingungen der FADS wurde von der datenbearbeitenden Behörde ein Entwurf zu einem Auftragsdatenverarbeitungsvertrag mit der Bitte um ein Review eingereicht. Dabei wurden von der FADS einige mit dem Auftragsdatenverarbeiter zu klärende Punkte identifiziert und der städtischen Projektleitung zurückgemeldet (fehlende Transparenz der bearbeiteten Daten, eingesetzte Subunternehmer). Daraufhin gelangten die Verantwortlichen der Stadt Bern an die FADS mit der Bitte um eine Aussprache dieser Punkte in direktem Austausch mit dem Auftragsdatenverarbeiter. An diesem Austausch konnten einerseits die vom Auftragsdatenver-

arbeiter bearbeiteten Daten geklärt werden. Andererseits wurde vereinbart, dass die Aufzeichnungsfunktion in der Stadt Bern nicht eingesetzt wird und damit eine Datenbearbeitung durch einen amerikanischen Subunternehmer entfällt.

Neue Applikationen

Vorabkontrolle Citysoftnet

Die Einführung der Applikation Citysoftnet (CSN) beschäftige die FADS auch in diesem Berichtsjahr. Wie im letztjährigen Tätigkeitsbericht aufgezeigt, wurde die Vorabkontrolle von CSN in die Beurteilung der Datenschutzkonformität der Test- und Migrationsphase sowie der Betriebsphase aufgeteilt. Im Berichtsjahr beschäftigte sich die FADS mit den ISDS-Dokumenten zur Betriebsphase der Applikation.

Ein erster provisorischer Vorabkontrollbericht wurde der datenbearbeitenden Behörde Ende Dezember 2022 zugestellt. Dieser beinhaltete insgesamt 50 Befunde, wovon 34 mit hoher Wesentlichkeit beurteilt wurden. Für einen datenschutzkonformen Betrieb von CSN in der Stadt Bern müssen diese Befunde zwingend bereinigt werden (siehe auch Tätigkeitsbericht 2022). Fast zeitgleich wurde der FADS die bis anhin fehlende und für eine Vorabkontrolle zwingend notwendige Risikoanalyse eingereicht. Darauf basierend erstattete die FADS per 12.01.2023 eine zweite Fassung des Prüfberichtsentwurfes mit insgesamt 64 Befunden, wovon 42 mit hoher Gewichtung beurteilt wurden. Per 10.02.2023 reichte die Gesamtprojektleitung die aktualisierten ISDS-Dokumente mitsamt einer Liste zum Stand der Umsetzung der Befunde ein. Nach der Prüfung der Dokumente wurde den verantwortlichen Behörden ein finaler Vorabkontrollbericht per 08.03.2023 zugestellt. Von den ursprünglich 64 Befunden konnten darin deren 47 (davon 32 mit hoher Wesentlichkeit) als erledigt betrachtet werden. Offen bzw. noch nicht umgesetzt blieben insgesamt 18 Befunde, davon 9 mit hoher Wesentlichkeit.

Nebst der Prüfung der ISDS-Dokumente wurde im Berichtsjahr zwecks Koordination der Prüfarbeiten und Informationsaustausch zwischen der FADS und den ebenfalls involvierten Datenschutzaufsichtsbehörden des Kantons Basel-Stadt und der Stadt Zürich mehrere Austausche organisiert. So fand beispielsweise am 23.02.2023 ein gemeinsamer Besuch der involvierten Datenschutzaufsichtsbehörden vor Ort in Zürich beim städtischen Amt für Organisation und Informatik (OIZ) statt, welches die für Betrieb und Datenhaltung von CSN notwendige Infrastruktur zur Verfügung stellt. Ziel des Austausches war es, offene Fragen bezüglich Hosting und Betrieb im OIZ direkt mit sachverständigen Personen vor Ort besprechen zu können. Die weiterführenden Informationen zu den Themen Zertifizierung, beim OIZ betriebene Komponenten und Schnittstellen sowie zur technischen und vertraglichen Situation in Bezug auf die Standleitung zwischen der Stadt Bern und OIZ führten zu Klärungen bezüglich gewisser Befunde und wurden, soweit relevant, direkt in die Befundliste der FADS eingearbeitet.

Am 14.04.2023 wurden dann wiederum aktualisierte ISDS-Dokumente von der Gesamtprojektleitung der FADS zur Vorabkontrolle eingereicht. Nach Prüfung der Dokumente stellte die FADS fest, dass von den noch offenen Befunden mit den aktualisierten Unterlagen lediglich drei umgesetzt waren und als erledigt beurteilt werden konnten. Anstatt nochmals einen Prüfbericht mit Befundliste an die Gesamtprojektleitung CSN zu richten, entschied sich die FADS zur mündlichen Besprechung der noch offenen Punkte direkt mit den Verantwortlichen der Stadt Bern. Zu diesem Zweck nahm die FADS Mitte Mai 2023 Kontakt auf mit der städtischen Projektleitung, was zu einer Besprechung der noch offenen Befunde Ende Juni 2023 führte. Dabei konnten einige Punkte im direkten Austausch geklärt werden und eine Neufassung der ISDS-Dokumente mit Behandlung der offenen Punkte vereinbart werden.

Mit den der FADS per 21.08.2023 eingereichten Dokumente konnten, mit einer Ausnahme, alle Befunde mit hoher Gewichtung als erledigt geführt werden. Bezüglich des noch offenen

Befundes wurde dessen Bereinigung zwar in Aussicht gestellt, gleichzeitig aber betont, dass die Aufrechterhaltung des ordentlichen Betriebs von CSN momentan oberste Priorität habe. Möglich wäre allenfalls eine Umsetzung zusammen mit dem auf Sommer 2024 geplanten neuen Release von CSN. Bis Redaktionsschluss wurde dies vom Projekt noch nicht definitiv bestätigt.

Workshop Confluence Cloud

Der ICT-Sicherheitsbeauftrage fragte die FADS für einen ISDS-Workshop an, um das Vorhaben zur Umstellung der Applikation Confluence von On-Premises in die Cloud zu besprechen und das weitere Vorgehen aus Sicht Datenschutz zu vereinbaren.

Am Workshop wurde geschildert, dass aktuell für das Konfigurations- und Wissensmanagement im Bereich IT-Betrieb die Lösung Confluence des Herstellers Atlassian als persönliches Arbeitsmittel eingesetzt werde. Der Betrieb dieses Systems laufe auf der städtischen ICT-Infrastruktur und Rechenzentren (On-Premises; On-Prem). Der Hersteller werde diese Betriebsform per Februar 2024 abkündigen und biete nur noch die Lösung aus der Cloud an. Daher gelangte der ICT-Sicherheitsbeauftragte zusammen mit dem Applikationsverantwortlichen an die FADS, um über die zur Migration in die Cloud notwendigen Schritte aus Sicht Datenschutz zu diskutieren.

Da die mit dieser Applikation in der Cloud bearbeiteten Personendaten lediglich Name, Vorname und Arbeitsort der IBE-Mitarbeiten-

Die Anforderungen der Informationssicherheit bezüglich sensibler Geschäftsinformationen sind zu berücksichtigen.

den betreffen und insbesondere keine Daten von Bürger*innen betroffen sind, erachtete die FADS dieses Vorhaben als nicht vorabkontrollpflichtig gemäss Art. 17 a KDSG. Jedoch wies die FADS darauf hin, dass die Anforderungen der Informationssicherheit bezüglich sensibler Geschäftsinformationen zu berücksichtigen sind. Im Workshop wurde ein Merkblatt in Aussicht gestellt, durch welches die Nutzenden auf Punkte des Datenschutzes und der Datensicherheit aufmerksam gemacht werden sollen. Die FADS stellte sich für ein Review des Merkblattes aus Sicht Datenschutz zur Verfügung.

Städtische Projekte

City Card Bern

Im Projekt einer digitalen City Card Bern stellen sich diverse, teilweise komplexe Fragen in Zusammenhang mit dem Datenschutz. Die FADS hat den Projektverantwortlichen den daraus folgenden Handlungsbedarf in mehreren Sitzungen sowie in einer schriftlichen Stellungnahme aufgezeigt.

Mit Entscheid des Gemeinderates im Juli 2022 wurde das Erstellen eines Konzeptes für eine City Card Bern in Auftrag gegeben. Die digitale City Card soll als Wohnortsbeleg, eigenständiger Identitätsbeleg oder als Altersbeleg in diversen Anwendungsbereichen dienen und so z. B. für den Zugang zu städtischen Dienstleistungen wie dem DeutschBon oder zu Vergünstigungen bei städtischen Eis- und Wasseranlagen oder bei den Entsorgungshöfen eingesetzt werden können. Darüber hinaus ist eine Reihe weiterer Einsatzmöglichkeiten geplant oder angedacht.

Die im Projekt federführende Fachstelle für Migrations- und Rassismusfragen hat im Berichtsjahr die FADS kontaktiert, um mit ihr die datenschutzrechtlichen Aspekte des Vorhabens zu besprechen.

In den der FADS eingereichten Unterlagen sowie im Rahmen mehrerer daraufhin durchgeführter Besprechungen wurde klar, dass sich

aus dem Projekt diverse, teilweise komplexe Fragen in Zusammenhang mit dem Datenschutz stellen. So werden für die City Card unterschiedliche Akteure, sowohl städtische als auch private, zusammenarbeiten und daher auch Personendaten austauschen können, welche teilweise aus städtischen Informationssystemen stammen und damit zu in den bisherigen gesetzlichen Grundlagen nicht vorgesehenen Aufgaben und Zwecken bearbeitet werden. Ausserdem könnten die geplanten Einsatzmöglichkeiten auch übergeordnetes Recht tangieren.

Die FADS hat darauf hingewiesen, dass zunächst eine angemessene Rechtsgrundlage geschaffen werden muss, welche auch die notwendigen Schnittstellen regelt. Da in gewissen Bereichen auch übergeordnetes Recht tangiert sein kann, muss dies dabei beachtet werden. Die Rollen der verschiedenen Akteure müssen genau geklärt werden. Hierbei interessiert insbesondere, wer für die City Card datenschutzrechtlich verantwortlich ist und wer als Auftragsbearbeiter tätig ist. Gegebenenfalls sind entsprechende Verträge aufzusetzen. Bei der technischen Ausgestaltung der digitalen City Card ist darauf zu achten, dass die datenschutzrechtlichen Bearbeitungsgrundsätze eingehalten werden, also z. B. nur so viele Daten bearbeitet werden, wie für die vorgesehenen Einsatzmöglichkeiten benötigt werden. Je nachdem, welche Daten über die City Card erhoben werden und in welchen Bereichen sie zum Einsatz gelangt, kann zudem nicht ausgeschlossen werden, dass auch besonders schützenswerte Personendaten bearbeitet werden, womit dem erhöhten Schutzbedarf sowohl auf technischer als auch auf rechtlicher Ebene entsprochen werden muss.

Zum in der Folge erstellten Umsetzungskonzept City Card hat die FADS zudem im Rahmen einer Direktionsvernehmlassung Stellung genommen und noch einmal auf die für den Datenschutz wesentlichsten Punkte hingewiesen.

Die FADS geht davon aus, dass das geplante Projekt der Vorabkontrollpflicht nach kantonalem Datenschutzgesetz untersteht. Sie hat die Projektverantwortlichen deshalb darauf hingewiesen, dass das Erstellen der dazu notwendigen Dokumentation seitens Projekt Zeit und Ressourcen in Anspruch nehmen wird und die Prüfung bei der FADS ebenfalls einige Wochen dauert. Sie hat ihnen nahegelegt, die notwendigen Arbeiten frühzeitig zu planen, damit es dadurch nicht zu unnötigen Verzögerungen kommt.

Mobility as a Service (MaaS): Städtekooperation zwischen Zürich, Bern und Basel

Im Projekt Mobility as a Service (MaaS) wurde das Thema Datenschutz frühzeitig und vorbildlich behandelt. Es fällt jedoch voraussichtlich nicht in den Zuständigkeitsbereich der FADS und unterliegt nicht der Vorabkontrollpflicht nach kantonalem Datenschutzgesetz.

Die drei Städte Zürich, Bern und Basel planen, eine gemeinsame Plattform zur Vermittlung, Buchung und Bezahlung diverser Mobilitätsdienstleistungen aufzubauen. Über eine einzige App sollen in den drei Städten künftig ÖV, Bikesharing, Carsharing, E-Scooter und weitere Mobilitätsangebote einfach gebucht und bezahlt werden können. Damit soll der Bevölkerung der Umstieg auf nachhaltige Verkehrsmittel so einfach wie möglich gemacht werden können.

Nachdem die drei Städte Ende 2022 eine entsprechende Kooperationsvereinbarung abgeschlossen haben, wurden die Arbeiten dazu unter der Federführung der Stadt Zürich in Angriff genommen. Die in der Stadt Bern mit dem Projekt betraute Fachstelle öffentlicher Verkehr hat die FADS im Berichtsjahr kontaktiert, um sich zu den datenschutzrechtlichen Fragen des Projekts beraten zu lassen. Sie hat der FADS die von der Stadt Zürich dazu erstellten umfangreichen Dokumente zugestellt, deren Inhalt im Rahmen von zwei Sitzungen besprochen wurden.

Die FADS hat einleitend darauf hingewiesen, dass eine App, welche das Mobilitätsverhalten einer grossen Anzahl von Personen und über ein breites Angebot an Verkehrsmitteln hinweg erfasst und analysiert, hohen datenschutzrechtlichen Anforderungen genügen muss. Sie konnte bei der Prüfung der Unter-

lagen jedoch feststellen, dass dies dem Projekt bewusst ist und es das Thema Datenschutz vorbildlich behandelt. So soll bereits im Vergabeverfahren sichergestellt werden, dass nur Anbieter berücksichtigt werden, welche die bei der Nutzung der App anfallenden Personendaten unter Einhaltung der in der Schweiz geltenden rechtlichen Vorgaben bearbeiten. Dazu wurden diese sowie die sich daraus ergebenden Anforderungen an die Applikation und den dahinterstehenden Anbieter zunächst evaluiert und festgehalten. Daraus abgeleitet wurde ein ausführlicher und detaillierter Fragekatalog erstellt, der durch die Bewerber im Vergabeverfahren auszufüllen ist. Nach der Prüfung dieses Katalogs und der weiteren Projektunterlagen geht die FADS davon aus, dass eine App eines so ausgewählten Anbieters datenschutzkonform betrieben werden kann. Dies zeigt, wie wichtig es ist, das Thema Datenschutz bei Digitalprojekten bereits in einem frühen Stadium anzugehen. Dadurch, dass bereits bei der Beschaffung die richtigen Fragen gestellt und damit die relevanten Informationen erhältlich gemacht werden, wird vermieden, dass das beschaffte Produkt am Ende nicht oder nur mit erheblichen Einschränkungen datenschutzkonform genutzt werden kann.

Im weiteren Verlauf der Arbeiten hat sich gezeigt, dass das Projekt, so wie es aktuell geplant ist, schwerpunktmässig unter dem Regime des Personenbeförderungsgesetzes des Bundes oder im Privatrecht einzuordnen ist. Damit liegt die datenschutzrechtliche Aufsichtskompetenz nicht bei der FADS, und es besteht keine Vorabkontrollpflicht nach kantonalem Datenschutzgesetz. Die FADS hat der Fachstelle Öffentlicher Verkehr aber mitgeteilt, dass dies neu geprüft werden muss, sollten im Projekt wesentliche Änderungen vorgenommen werden. Die Fachstelle Öffentlicher Verkehr hat der FADS zugesichert, sie über die Projektentwicklungen auf dem Laufenden zu halten.

Digitale Kommunikation

Datenschutzkonformität von Klapp im Schulbereich

Die FADS wurde durch Bürgeranfragen darauf aufmerksam gemacht, dass bei der für die Elternkommunikation in Stadtberner Schulen eingesetzten Applikation Klapp möglicherweise die Vorgaben des kantonalen Datenschutzgesetzes nicht eingehalten werden. Insbesondere wurde bemängelt, dass die App aufgrund des Fehlens einer end-to-end-Verschlüsselung nicht für den Versand besonders schützenswerter Personendaten oder geheimnisgeschützter Informationen geeignet sei und dass der Registrierungsprozess nicht sicher sei, so dass sich auch unberechtigte Dritte registrieren könnten.

Eigene Abklärungen haben ergeben, dass Klapp tatsächlich nicht über eine end-to-end Verschlüsselung verfügt und daher nicht für den Versand von besonders schützenswerten Personendaten eingesetzt werden soll. Rückfragen bei der Schulinformatik und dem Schulamt haben ergeben, dass zwar vom Schulamt die Vorgabe gemacht wurde, Klapp nicht für den Versand von besonders schützenswerten Personendaten zu nutzen, jedoch im Bereich Information der Lehrkräfte und der Erziehungsberechtigten noch Verbesserungsbedarf besteht.

Klapp verfügt nicht über eine end-to-end-Verschlüsselung und soll daher nicht für den Versand von besonders schützenswerten Personendaten eingesetzt werden.

So wird die Einschränkung auf nicht besonders schützenswerte Inhalte nicht von allen Schulleitungen aktiv kommuniziert, und die Eltern werden, je nach Schule, nur unzureichend darauf aufmerksam gemacht, dass Alternativen für die Elternkommunikation genutzt werden können (bswp. Klassentelefon für Krankmeldungen).

Da der einem Kind zugeordnete Registrierungscode mehrfach verwendet werden kann und nicht pro Erziehungsberechtigten neu generiert wird, kann eine Registrierung Unberechtigter tatsächlich nicht vollständig ausgeschlossen werden. Allerdings ist für die Lehrpersonen sichtbar, wer sich unter einem bestimmten Kind registriert hat. Zudem werden ein bestimmtes Kind betreffende Informationen nur an die bekannten Kontaktpersonen des Kindes gesendet, der Versand an grössere Adressatengruppen erfolgt nur bei allgemeinen Informationen, wie z. B. beim Mittagsmenü der Tagesschule. Daher bestand für die FADS in diesem Zusammenhang kein unmittelbarer Handlungsbedarf.

Da zu Klapp noch keine ISDS-Dokumentation erstellt wurde, hat die FADS die Schulinformatik jedoch dazu aufgefordert, dies nachzuholen und die Dokumente der FADS zur Prüfung einzureichen. Bei dieser Gelegenheit wird die FADS auch diese Fragen noch einmal vertieft prüfen können.

Mögliche Datenschutzverletzung bei Mails in Quarantäne

Der Vorgesetzte eines Mitarbeiters der Stadtverwaltung wandte sich wegen einer möglichen Datenschutzverletzung bei der Behandlung von Quarantänemails durch Informatik Stadt Bern IBE an die FADS. Es wurde beanstandet, dass eine eingehende Mail, welche zufolge Absenderadresse und Betreffzeile in Quarantäne genommen wurde, ohne Rücksprache mit dem Empfänger durch den Service Desk der IBE gelesen wurde.

Die FADS behandelte die Anfrage als aufsichtsrechtliche Anzeige und holte in der Folge eine Stellungnahme von IBE ein. Wie sich dabei zeigte, bestand bei IBE noch kein datenschutzkonformer Prozess zu Behandlung von Quarantänemails. Ein solcher wurde als Folge der Anzeige neu aufgesetzt und der FADS unterbreitet. Dabei wurde festgelegt, dass eine vollständige Einsicht in Quarantänemails (inklusive Anhänge und Links) künftig nur nach erfolgter Einholung der Zustimmung der Betroffenen und nur durch einen beschränkten Personenkreis bei der ICT-Sicherheit erfolgt. Der Einsicht nach erfolgter Zustimmung vorgelagert ist als erste Stufe die Möglichkeit einer Selbstfreigabe durch den User und als zweite Stufe die Plausibilisierung aufgrund des Absenders und/oder der Betreffzeile. Nur wenn die Plausibilisierung aufgrund dieser beiden Schritte noch nicht möglich ist, erfolgt gestützt auf die eingeholte Zustimmung eine inhaltliche Prüfung durch die ICT-Sicherheit. Dem Anzeiger wurde die Einrichtung des betreffenden Prozesses mitgeteilt.

Bestellbestätigung per Mail bei der elektronischen Wohnsitzbescheinigung

Der Anzeiger beanstandete bei den Einwohnerdiensten (EMF), dass ihm im Rahmen der online-Bestellung einer Wohnsitzbestätigung ungefragt eine Bestellbestätigung per Mail zugeschickt wurde. Er machte geltend, dass die Übermittlung per Mail ohnehin unsicher sei; zudem enthalte die Bestellbestätigung aus seiner Sicht mehr Personendaten als erforderlich. Die Einwohnerdienste gelangten ihrerseits mit der Fragestellung an die FADS.

Zur Klärung des Sachverhalts hat die FADS von EMF eine Stellungnahme eingeholt. Gestützt darauf und aufgrund der erfolgten Abklärungen stellte die FADS fest, dass aus Gründen der Datensparsamkeit der Versand einer Bestellbestätigung als optional ausgestaltet werden sollte. Im Sinne einer datenschutzfreundlichen Voreinstellung wäre «per default» keine Bestellbestätigung zu versenden.

Im Weiteren stellte die FADS fest, dass eine (optionale) Bestellbestätigung ebenfalls aus Gründen der Datensparsamkeit nur die dafür erforderlichen Angaben enthalten sollte. Dabei ist zunächst zu klären, was genau bestätigt

werden soll. Für die Kontrolle der von den Benutzenden eingegebenen Angaben steht die Möglichkeit des Drucks am Ende des Bestellprozesses zur Verfügung. Sofern nur die getätigte Bezahlung bestätigt werden soll, wären die entsprechenden Angaben ausreichend. Allenfalls könnte auch eine generische Bestätigung geprüft werden, z. B. «Wir bestätigen den Erhalt Ihrer Bestellung. Die Wohnsitzbestätigung wird Ihnen in den nächsten Tagen zugestellt werden». Auf jeden Fall zu vermeiden ist ein ungeschützter Versand der AHV-Nummer auf der Bestellbestätigung, wie dies im Falle des Betroffenen erfolgte. Diese Erkenntnisse wurden EMF mitgeteilt und deren Umsetzung empfohlen. Gleichzeitig wurden die Einwohnerdienste auf die bundesrechtlichen Vorgaben für die systematische Verwendung der AHV-Nummer hingewiesen. Der Anzeiger wurde über das Ergebnis informiert.

Publikation von Personendaten

Datenschutz auf Webseite zum Tag der Nachbarschaft

Das Kompetenzzentrum Alter organisiert jeweils den Tag der Nachbarschaft, an dem Private einen Nachbarschaftsevent veranstalten und auf der Webseite zum Tag der Nachbarschaft publizieren lassen können. Diese Webseite soll neugestaltet werden, wobei die Idee aufgekommen ist, die Events auf dem online-Stadtplan zu publizieren, so dass gezielt nach Events in einem bestimmten Quartier gesucht werden kann. Falls dies gemacht würde, stellt sich die Frage, welche Daten dabei veröffentlicht werden können, ob z. B. die Kontaktangaben der Veranstalter direkt veröffentlicht werden, oder ob solche Angaben nur auf Anfrage hin mitgeteilt würden.

Die Publikation im Internet ist mit bestimmten Risiken für die Betroffenen verbunden. So können die Daten, je nach technischer Implementierung, leicht abgegriffen und zweckentfremdet werden. Zudem besteht die Gefahr, dass nicht mehr kontrolliert werden kann, wer zu so einem Event erscheint. Fraglich ist für die FADS auch, ob eine solche Publikation zielgruppengerecht wäre. Die FADS rät daher dazu, die Daten nicht ohne weitere Schutzmassnahmen zu publizieren (min. Schutz vor Massenabfragen, z. B. durch robo.txt o. ä.) und nur nach vorgängiger zielgruppengerechter und vollständiger Information der Betroffenen auf freiwilliger Basis. Aus Sicht Datenschutz wäre es allerdings zu bevorzugen, dass die Daten nur auf Anfrage hin weitergegeben würden. Es muss abgewogen werden zwischen einer angemessenen Reichweite und dem Schutz der Privatsphäre der Veranstaltenden. Das Kompetenzzentrum Alter wird die Möglichkeiten prüfen und eine möglichst die Privatsphäre schonende Variante wählen.

Publikation von Wahllisten und -resultaten auf der Website der Stadt Bern

Die zeitlich unbegrenzte Publikation von Wahllisten und Resultaten städtischer Wahlen auf der Webseite der Stadt Bern wurde von der FADS als unverhältnismässig beurteilt. In Zusammenarbeit zwischen der Stadtkanzlei und der FADS konnte eine datenschutzfreundlichere Lösung gefunden werden.

Die FADS wurde durch eine Bürgermeldung darauf aufmerksam gemacht, dass die Stadt Bern Wahllisten und -resultate städtischer Wahlen zeitlich unbeschränkt auf ihrer Webseite publiziert. So waren Angaben zu den Wahlen aus dem Jahr 2008 auf der Webseite aufgeschaltet. Wurde in den gängigen Internetsuchmaschinen nach in diesen Unterlagen aufgeführten Personen gesucht, wurden die Informationen in den Suchresultaten an prominenter Stelle angezeigt. Die Stadtkanzlei vertrat zunächst die Auffassung, dass die der Publikation zugrunde liegende Rechtsgrundlage keine zeitliche Beschränkung enthalte und die Angaben daher, in Übereinstimmung mit der Praxis bei Bund und Kanton, zeitlich unbeschränkt veröffentlicht werden können.

Obschon die Rechtsgrundlage keine zeitliche Beschränkung enthält, ist die Publikation von Wahllisten und Resultaten städtischer Wahlen

Während das Interesse an einer Publikation bei Informationen zu aktuellen Wahlen und noch immer aktiven Amtsträgern den Schutz der Privatsphäre überwiegt, wird dies weniger der Fall sein, je länger die betreffende Wahl zurückliegt.»

jedoch nicht ohne Weiteres zulässig. Vielmehr muss sie den datenschutzrechtlichen Bearbeitungsgrundsätzen entsprechen. Daher galt es im vorliegenden Fall abzuwägen, welche Publikationsdauer als verhältnismässig gelten kann resp. wie lange ein überwiegendes Interesse an der Publikation besteht.

Bei den publizierten Informationen handelt es sich um Angaben zu Wahlen in ein öffentliches Amt, womit ein legitimes Interesse an deren öffentlichen Verfügbarkeit grundsätzlich gegeben ist. Während dieses Interesse bei Informationen zu aktuellen Wahlen und noch immer aktiven Amtsträgern den Schutz der Privatsphäre überwiegt, wird dies weniger der Fall sein, je länger die betreffende Wahl zurückliegt. Im der FADS angezeigten Fall betrafen die Wahllisten und -Resultate eine Wahl, welche bereits 15 Jahre zurück lag. Die damals gewählten Stadträt*innen sind aufgrund der in der Gemeindeordnung der Stadt Bern festgeschriebenen Amtszeitbeschränkung nicht mehr im Amt, und das Interesse der breiten Öffentlichkeit an diesen Informationen dürfte nicht mehr gross sein. Trotzdem waren sie ohne weitere Schutzmassnahmen (z. B. von Suchresultaten gängiger Suchmaschinen ausgenommen) weltweit abrufbar. Die FADS erachtete dies insgesamt als unverhältnismässig, zumal die Informationen interessierten Kreisen (z. B. Journalist*innen oder Historiker*innen) auch nach Massgabe der Archivgesetzgebung im Stadtarchiv zugänglich gemacht werden können. Dies hat sie der verantwortlichen Behörde mitgeteilt.

Die Stadtkanzlei hat sich daraufhin gegenüber der FADS dazu bereit erklärt, ihre Praxis noch einmal zu überdenken. Im Rahmen einer gemeinsamen Besprechung konnte daraufhin eine die Privatsphäre der Betroffenen besser wahrende Lösung gefunden werden. Dieser zufolge beschränkt die Stadtkanzlei ihre online-Publikation auf Informationen zu den letzten drei Gemeindewahlen. Die daraus resultierende Publikationsdauer von 12 Jahre entspricht der maximalen Amtsdauer für Stadträt*innen gemäss Gemeindeordnung, für die das öffentliche Interesse an dieser Publikation in einem massgeblichen Umfang zu bejahen ist. Sie stützt sich damit auf ein objektives und sachgerechtes Kriterium und erscheint so verhältnismässig.

Die Stadtkanzlei hat ihre Webseite umgehend in diesem Sinne bereinigt und die Daten aus dem Jahr 2008 vom Netz genommen. Damit wurde auch dem Anliegen der meldenden Person entsprochen, und die sie betreffenden Daten sind nun nicht mehr online abrufbar.

Bekanntgabe von Personendaten

Datenaustausch zwischen Einwohnerdiensten und Sozialdienst betreffend Institutionen und Anstalten

Die Einwohnerdienste gelangten an die FADS zur Beurteilung einer geplanten Datenweitergabe auf Antrag durch das Sozialamt. Dabei ging es um die Bekanntgabe von Personen, welche sich «im Strafvollzug oder in anderen Institutionen aufhalten».

Die Einwohnerdienste sind regelmässig mit Personen konfrontiert, welche ihrer Meldepflicht nicht nachkommen, d. h. sie erhalten Kenntnis

davon, dass eine Person nicht mehr an der gemeldeten Adresse wohnhaft ist, haben aber keine neue Adresse, und die Person ist nicht auffindbar. In einigen dieser Fälle habe der Sozialdienst Kenntnis davon, dass sich diese Personen in Strafanstalten oder anderen Institutionen aufhalten. Bei diesen Personen müssen die Einwohnerdienste diese Institutionen und Anstalten als Zustelladresse erfassen. Daher waren die Einwohnerdienste der Ansicht, dass das Sozialamt die Information bezüglich Aufenthalt in einer Strafanstalt oder Institution gestützt auf Art. 10 Abs. 1 Bst. b KDSG bekannt geben darf.

Die FADS prüfte die Sach- und Rechtslage und kam zum Schluss, dass das Sozialhilfegeheimnis als besondere Geheimhaltungspflicht einer Datenweitergabe durch das Sozialamt entgegensteht. Zwar besteht eine ältere bundesgerichtliche Rechtsprechung , wonach die besondere Geheimhaltungspflicht durch die Betroffenen dann nicht angerufen werden kann, wenn Letztere eine gesetzliche Auskunftspflicht trifft. Eine solche liegt zwar in Form der Meldepflicht für die Betroffenen grundsätzlich vor; aufgrund der Unterschiede im Sachverhalt lässt es sich jedoch aus heutiger Sicht nicht ausreichend sicher feststellen, ob die zuständigen Gerichte den aktuellen Fall analog zu dieser Rechtsprechung beurteilen würden. Dementsprechend riet die FADS davon ab, eine Datenweitergabe auf diese Rechtsprechung abzustützen. Die beste Lösung wäre eine klare Rechtsgrundlage in der Liste der Behörden für eine zulässige Datenweitergabe in Art. 57c Sozialhilfegesetz. Für die Einwohnerdienste war die rechtliche Beurteilung der FADS nachvollziehbar. Sie würden sich mit dem Sozialamt darüber austauschen, ob dieses eine Datenweitergabe gestützt auf die bundesgerichtliche Rechtsprechung vornehmen wird. Falls nicht, würden die Einwohnerdienste die betreffenden Fälle von Amtes wegen als mit unbekanntem Aufenthalt abmelden.

In der Folge wurde ebenfalls das Sozialamt bei der FADS vorstellig. Es konnte die Stellungnahme der FADS inhaltlich zwar nachvollziehen, hätte sich aber einen klaren Befund gewünscht. Insbesondere wollte die Amtsleitung eine Vorgabe, ob die Datenweitergabe gemäss der Rechtsprechung des Bundesgerichts zulässig sei oder nicht. Die FADS hielt dazu fest, dass die Rechtslage vorliegend eben gerade nicht vollumfänglich klar sei. Im Übrigen sei es Sache der datenbearbeitenden Behörde, die Zulässigkeit einer Datenweitergabe im konkreten Einzelfall zu beurteilen. Entsprechend trage sie dafür auch die Verantwortung (Art. 8 KDSG). Die FADS könne lediglich die Rechtslage erörtern und das Sozialamt bei der Rechtsanwendung beraten. Dies wurde gegenüber dem Sozialamt nochmals ausdrücklich bestätigt.

Datenaustausch zwischen den Einwohnerdiensten, Statistik Stadt Bern, Immobilien Stadt Bern und der kantonalen Steuerverwaltung

Die Abteilung Aussenbeziehungen und Statistik hatte Fragen zur Zulässigkeit eines Datenaustauschs zwischen städtischen Behörden und der kantonalen Steuerverwaltung in Zusammenhang mit der Vergabe vergünstigter Mietwohnungen. Die FADS hat die geplanten Datenflüsse und die Rechtsgrundlagen geprüft und die anfragende Behörde beraten.

Es stellte sich die Frage der Zulässigkeit eines Datenaustausches zwischen den Einwohnerdiensten, Statistik Stadt Bern, Immobilien Stadt Bern und der kantonalen Steuerverwaltung zwecks Festlegung der Einkommensobergrenzen für vergünstigte Neubauwohnungen in den Quartieren der Stadt Bern.

Dabei sollte zunächst eine Weitergabe von Einwohnerdaten inklusive AHV-Nummer an Statistik Stadt Bern erfolgen. Diese wird den Datensatz zwecks Ergänzung mit Einkommensdaten der Haushalte, aggregiert auf Quartiere, an die kantonale Steuerverwaltung weiterleiten. Der ergänzte Datensatz geht wiederum an Statistik Stadt Bern zurück, welche überdies sehr kleine Quartiere bezüglich Einkommensangaben schwärzt, um die Reidentifikation von Personen zusätzlich auszuschliessen. Der endgültige Datensatz, der keinen Personenbezug aufweist, wird Immobilien Stadt Bern unterbreitet.

Nach Prüfung und Besprechung der Datenflüsse konnte festgestellt werden, dass die betreffenden Datenweitergaben und -bearbeitungen durch die anwendbaren Bestimmungen (Art. 15 KDSG; Art. 11 und 12 Statistikverordnung, STAV; SSSB 422.1) abgedeckt werden. Insbesondere nahm die FADS davon Kenntnis, dass beim finalen Datensatz kein Personenbezug mehr vorhanden ist, dessen Bearbeitung zu nicht personenbezogenen Zwecken erfolgt und daher auf das Forschungsprivileg gestützt werden kann. Die FADS wies zudem auf die bundesrechtlichen Vorgaben bei der systematischen Verwendung der AHV-Nummer hin.

Zustellung von Strafanzeigen wegen Schulversäumnis

Das Schulamt fragte an, ob bei Strafanzeigen wegen Schulversäumnis, welche durch das Schulamt eingereicht werden, den Schulleitungen und Schulkommissionen jeweils eine Kopie zugestellt werden darf oder nicht.

Das Vorgehen bei Schulversäumnis wird in der Volksschulgesetzgebung (VSG; BSG 432.210) geregelt. Gemäss Art. 32 Abs. 2 VSG hat die Schulkommission nach Anhörung der Betroffenen Anzeige zu erstatten. In Art. 23d Abs. 2 Bst. c des städtischen Schulreglements (SR; SSSB 430.101) wird diese Zuständigkeit dem Schulamt zugewiesen; es kontrolliert ebenfalls in Zusammenarbeit mit den (Kreis-) Schulkommissionen die Einhaltung der Schulpflicht.

Dass im Vorfeld einer Strafanzeige Schulleitungen, Schulkommissionen und Schulamt zusammenarbeiten und daher Kenntnis über den Sachverhalt erhalten, wird von den Rechtsgrundlagen abgedeckt. Demgegenüber stellt die Strafanzeige an sich aus Sicht Datenschutz ein Dokument mit erhöhter Sensitivität dar, welches besonders schützenswerte Personendaten enthält. Die Zustellung der Anzeige an die Schulleitung und an die Schulkommission stellt eine Bekanntgabe von besonders schützenswerten Personendaten unter Schulorganen dar; sie richtet sich nach Art. 73 VSG und ist nur zulässig, wenn sie zur Erfüllung der gesetzlichen Aufgabe zwingend erforderlich ist.

Eine systematische Zustellung von Strafanzeigen wegen Schulversäumnis an Schulleitungen und Schulkommissionen wird als unverhältnismässig beurteilt.

Das Schulamt wurde daher darauf hingewiesen, dass es zu prüfen hat, ob diese zwingende Erforderlichkeit für die Aufgabenerfüllung vorliegt, oder ob dafür nicht auch eine mildere Massnahme (z. B. lediglich die Mitteilung, dass Anzeige erhoben wurde) ausreichend wäre. Dabei hatte es zu berücksichtigen, dass gemäss Art. 33 Abs. 2 VSG das zuständige Gericht das Urteil nach Eintritt der Rechtskraft umgehend der Schulkommission und der Schulleitung zustellen muss. Spätestens dann erhalten die genannten Schulorgane daher Kenntnis vom (abgeschlossenen) Strafverfahren.

Die FADS erachtete daher eine systematische Zustellung der Anzeigen an die Schulleitungen und die Schulkommissionen ohne nähere Angaben zur erwähnten zwingenden Erforderlichkeit aus Sicht Datenschutz als unverhältnismässig.

Adressänderung bei Aufhebung des gemeinsamen Haushalts

Ein Anzeiger beanstandete den Umstand, dass die Einwohnerdienste gestützt auf eine Meldung seiner Ehefrau zufolge seines Auszugs aus dem ehelichen Domizil eine Adressänderung im Einwohnerregister vollzogen hatten, ohne ihn entsprechend zu informieren. Im Weiteren machte er in Bezug auf seine neue Partnerin geltend, die Einwohnerdienste hätten trotz Adresssperrung die Wohnadresse deren sich ebenfalls in Trennung befindlichem Ehemann bekannt gegeben. Den Grund für die Adresssperrung bildeten Stalking-Vorwürfe.

Die Abklärungen der FADS bei den Einwohnerdiensten ergaben, dass die Vornahme der Adressänderung des Anzeigers in der Tat aufgrund einer Vorsprache der Ehefrau und ohne Rücksprache mit diesem erfolgte. Überdies hatte sich auch die Steuerverwaltung bei den Einwohnerdiensten nach der aktuellen Wohnadresse des Anzeigers erkundigt. Es ergab sich im Weiteren, dass der Anzeiger seiner gesetzlichen Meldepflicht (Meldung von Adressänderungen innert 14 Tagen) nicht nachgekommen war. Die Einwohnerdienste räumten aber ein, dass der Anzeiger aufgrund eines Versehens nicht über die Adressänderung informiert wurde und entschuldigten sich bei diesem. Zudem stellten die Einwohnerdienste in Aussicht, die internen Prozesse entsprechend anzupassen.

Bezüglich der Partnerin des Anzeigers konnten keine Hinweise auf eine Datenbekanntgabe durch die Einwohnerdienste trotz Adresssperrung gefunden werden.

Das revidierte Datenschutzgesetz des Bundes

Die Einwohnerdienste, Fremdenpolizei und Migration (EMF) wollten wissen, ob das neue Bundesdatenschutzgesetz (nDSG) und insbesondere die neuen Strafbestimmungen auf EMF auch dann nicht anwendbar seien, wenn bundesrechtliche Bestimmungen bezüglich Migration und Integration vollzogen werden.

EMF wurde darauf hingewiesen, dass sie bei Vollzug von Bundesrecht nur dann zu einer Behörde des Bundes werde und damit unter den Anwendungsbereich des DSG falle, wenn das Bundesrecht dies ausdrücklich festhalte. Im Bereich des Ausländer- und Integrationsgesetzes, des Asylgesetzes sowie in der kantonalen Einführungsgesetzgebung ist dies nicht der Fall. Damit sind für EMF das neue DSG des Bundes und dessen Strafbestimmungen grundsätzlich nicht anwendbar. Als Strafbestimmungen sind weiterhin Art. 320 und 321 StGB relevant. Datenbearbeitungen durch EMF erfolgen wie bis anhin im Anwendungsbereich des KDSG. Vorbehalten bleibt eine differenziertere Beurteilung des anwendbaren Rechts gestützt auf einen konkreten Anwendungsfall.

EMF wurde bei dieser Gelegenheit auf die laufende Vernehmlassung zum revidierten KDSG hingewiesen.

Datenaustausch Stadtgärten und Vereine Familiengärten

Der Bereich Stadtgärten von Stadtgrün Bern (SGB) verwaltet die städtischen Familiengartenareale und verpachtet die einzelnen Gartenparzellen. Er wandte sich an die FADS mit der Bitte um Beratung zur Anwendbarkeit des neuen Bundesdatenschutzgesetzes (nDSG) auf die Vereine für Familiengärten sowie zum Datenaustausch zwischen den Vereinen bzw. dem Verband der Familiengärtner*innen und SGB. Bezüglich der Vereine für Familiengärten wurden Entwürfe für an das nDSG angepasste Vereinsstatuten sowie für eine Datenschutzerklärung zur Prüfung vorgelegt.

Die FADS hielt zunächst fest, dass die Vereine Familiengärten im Verhältnis zu ihren Mitgliedern und Dritten (nicht Stadtverwaltung) dem nDSG unterstehen. Im Anwendungsbereich des nDSG ist der EDÖB für die Datenschutzaufsicht zuständig. Bezüglich Datenschutzerklärungen und Anpassung der Vereinsstatuten konnte auf die Website des EDÖB verwiesen werden. Wie sich zeigte, beruhten die eingereichten Unterlagen bereits darauf.

Im Verhältnis zwischen SGB und den Vereinen bzw. ihren Mitgliedern ist demgegenüber das KDSG anwendbar. SGB erbringt für die Vereine und auch für den Verband der Berner Familiengärten Dienstleistungen im Zusammenhang mit der Bewirtschaftung der städtischen Familiengärten. So nimmt SGB Anmeldungen entgegen, führt die Warteliste, und schliesst die Pachtverträge für die Gartenparzellen mit den Vereinsmitgliedern ab. Nach Vertragsabschluss werden die Kommunikationsdaten dem Verein Familiengärten bekanntgegeben (Mitgliedschaft ist eine Bedingung für Pacht). Ferner werden die Rechnungsdaten der Pachtenden bei SGB geführt. Insgesamt konnte festgestellt werden, dass die dargelegten Datenbearbeitungen durch die massgeblichen Rechtsgrundlagen abgedeckt werden.

Antrag

Kenntnisnahme des Tätigkeitsberichts 2023 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 wertvolle Unterstützung bei der Einarbeitung, die konstruktive Zusammenarbeit bei der Trennung von Datenschutzaufsicht und Ombudsstelle und für die bereichernde Büronachbarschaft;
- beim ihrem Team für den offenen Empfang, für das tägliche Engagement und die bereichernde Zusammenarbeit.