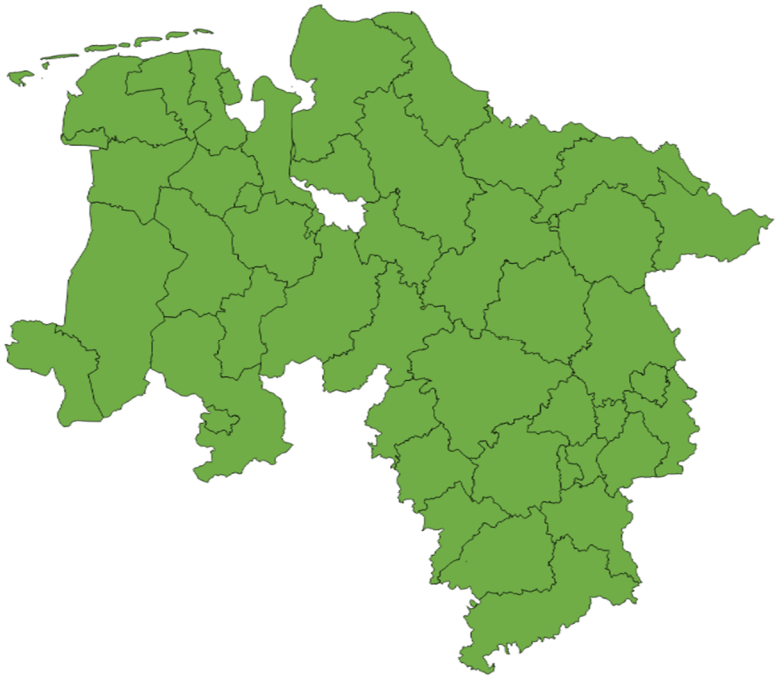
Die Präsidentin des
Niedersächsischen Landesrechnungshofs

- Überörtliche Kommunalprüfung -



Kommunalbericht 2018

Niedersachsen

Kommunalbericht

der

Präsidentin

des Niedersächsischen Landesrechnungshofs

- Überörtliche Kommunalprüfung -

2018

Übersandt an

- Nds. Landtag
- Nds. Landesregierung
- Nds. Landkreistag
- Nds. Städtetag
- Nds. Städte- und Gemeindebund

Herausgeberin:

Die Präsidentin des Nds. Landesrechnungshofs
Justus-Jonas-Str. 4
31137 Hildesheim
http://www.lrh.niedersachsen.de

5.7 Informationssicherheit in Kommunen – Externer Sachverstand muss nicht teuer sein

Die Digitalisierung und die damit einhergehende Abhängigkeit kommunaler Verwaltungen von Informationstechnologien fordern von den Kommunen, den Themen Informationssicherheit und Datenschutz stetig mehr Bedeutung beizumessen. Die geprüften Kommunen hatten die Informationssicherheit noch nicht ausreichend hergestellt. Gesetzliche Vorgaben zu Verfahrensbeschreibungen und Auftragsdatenverarbeitungen beachteten sie nicht in der gebotenen Weise.

Bei der Entscheidung, ob sich Kommunen für eine interne oder externe Wahrnehmung der Aufgaben von Datenschutzbeauftragten entscheiden, sollten neben fachlichen Erwägungen auch Kostenaspekte berücksichtigt werden.

Hintergrund und Ziel der Prüfung

Die Digitalisierung kommunaler Verwaltungsprozesse erfordert, die damit einhergehenden Risiken zu analysieren und zu minimieren. Der Ausfall von IT-Systemen oder der Verlust von Daten führte auch im kommunalen Bereich immer wieder zu materiellen und immateriellen Schäden.[41]

Die überörtliche Kommunalprüfung untersuchte bei zehn Kommunen[42] mit bis zu 33.000 Einwohnern, wie intensiv sich diese mit den Themen Informationssicherheit und Datenschutz auseinandergesetzt hatten. Die Prüfung umfasste Kommunen sowohl mit internem als auch mit externem Datenschutzbeauftragten. Die Prüfungsfragen deckten die Bereiche Informationssicherheitsmanagement, Gebäudesicherheit, Zugang zu IT-Systemen, Notfallmaßnahmen, Sensibilisierung von Mitarbeiterinnen und Mitarbeitern sowie Datenschutzbeauftragte ab.

Fortsetzung der Prüfungsreihe Informationssicherheit

Die Untersuchung setzte auf eine Prüfung von 20 Kommunen aus dem Jahr 2016 auf.[43] Dabei sind die abgeleiteten Ergebnisse im Wesentlichen mit den Feststellungen aus der Prüfung im Jahr 2016 deckungsgleich. Auffällig war jedoch, dass die (größeren) Kommunen aus der 2017 durchgeführten Prüfung im Mittel über alle Themenfelder 13 % bessere Ergebnisse erreichten als die (kleineren) Kommunen aus der 2016 durchgeführten Prüfung.

---

41 Vgl. statt vieler NWZonline vom 15. Februar 2014, Datenverlust in der Finanzabteilung der Gemeinde Ritterhude, wonach infolge eines technischen Defekts aufgrund unzureichender Sicherheitsmaßnahmen mehrere Tausend Datensätze vernichtet worden sein sollen.

42 Geprüft wurden die Städte Achim, Bramsche, Bückeburg, Burgwedel, Cloppenburg, Georgsmarienhütte, Stadthagen und Vechta sowie die Gemeinden Isernhagen und Wedemark.

43 Die Präsidentin des Niedersächsischen Landesrechnungshofs, Kommunalbericht 2017, Kapitel 5.10 „Informationssicherheit in Kommunen – Bisher ist es meist gut gegangen“, S. 64 ff.

Zusätzlich umfasste die aktuelle Prüfung eine vertiefte Betrachtung der Themenfelder Verfahrensbeschreibungen, Auftragsdatenverarbeitung und Kosten der Datenschutzbeauftragten. Die drei letztgenannten Themenfelder bilden daher den Schwerpunkt dieses Beitrags.

Verfahrensbeschreibungen müssen den gesetzlichen Anforderungen genügen

In Verfahrensbeschreibungen ist zu dokumentieren, welche personenbezogenen Daten mithilfe welcher automatisierten Verfahren verarbeitet und welche Datenschutzmaßnahmen dabei getroffen werden (§ 8 NDSG). Eine Liste der Verfahrensbeschreibungen (Verfahrensverzeichnis) ist dem behördlichen Datenschutzbeauftragten zuzuleiten (§ 8a Abs. 2 S. 5 NDSG).

Verfahrensbeschreibungen, in denen datenverarbeitende Stellen, wie Fachbereiche, ihre Verfahren zur automatisierten Verarbeitung personenbezogener Daten darstellen, lagen nur in zwei Kommunen vollständig vor. In den übrigen acht Kommunen gab es entweder keine Verfahrensbeschreibungen für alle Verfahren oder sie genügten nicht den Anforderungen des § 8 NDSG. Nur die Hälfte der Kommunen hatte dem Datenschutzbeauftragten ein Verfahrensverzeichnis zugeleitet. Soweit noch nicht geschehen, sind die Kommunen verpflichtet, ihre Verfahrensbeschreibungen zu erstellen bzw. zu ergänzen. Dem behördlichen Datenschutzbeauftragten ist eine vollständige Übersicht über die automatisierten Verarbeitungen personenbezogener Daten zuzuleiten.

Die rechtlichen Vorgaben zur Auftragsdatenverarbeitung sind zu beachten

In der kommunalen Praxis ist oftmals die sogenannte Auftragsdatenverarbeitung anzutreffen: Dabei wird die automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von der Kommune auf andere öffentliche oder nicht-öffentliche Stellen (beauftragte Stellen) übertragen. Nach den gesetzlichen Bestimmungen in §§ 6 ff. NDSG müssen für diese Auftragsdatenverarbeitung schriftliche Aufträge vorliegen. Es muss sichergestellt sein, dass der Auftragsdatenverarbeiter personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeitet.

Insgesamt untersuchte die überörtliche Kommunalprüfung in den zehn geprüften Kommunen 84 Verfahren, bei denen eine Datenverarbeitung durch Dritte vorlag. Nur für etwas mehr als die Hälfte dieser Verfahren lagen die erforderlichen Verträge über eine Auftragsdatenverarbeitung vor. Lediglich eine Kommune konnte jedes Verfahren mit einem entsprechenden Vertrag zur Auftragsdatenverarbeitung belegen. Sieben Kommunen hatten nicht für alle Verfahren entsprechende Verträge. Zwei Kommunen konnten gar keine schriftlichen Verträge zur Auftragsdatenverarbeitung vorlegen. Die Kommunen ohne Verträge zur Auftragsdatenverarbeitung haben entsprechende Verträge unverzüglich abzuschließen, um den gesetzlichen Anforderungen zu entsprechen. Sie sollten fer-

ner prüfen, inwieweit die Anforderungen der §§ 6 und 7 NDSG in den bestehenden Verträgen mit den beauftragten Stellen Berücksichtigung gefunden haben.[44] So müssen die Kommunen kontrollieren, ob die beauftragte Stelle die Weisungen der Behörde einhält (§ 6 Abs. 2 NDSG) und die Gewähr bietet, die in § 7 NDSG genannten technischen und organisatorischen Maßnahmen einzuhalten. Die überörtliche Kommunalprüfung empfiehlt deshalb den Kommunen, regelmäßig Kontrollen der Weisungen durchzuführen und zu dokumentieren.

Mitarbeiterinnen und Mitarbeiter für das Thema Informationssicherheit sensibilisieren

Für den Schutz von Informationen und Daten reicht es regelmäßig nicht aus, sich auf technische Lösungen zu beschränken. Häufig stellen fehlende Kenntnisse oder mangelndes Problembewusstsein einzelner Mitarbeiterinnen und Mitarbeiter ein Risiko dar. Ein angemessenes Sicherheitsniveau lässt sich nur erreichen und halten, wenn Mitarbeiterinnen und Mitarbeiter regelmäßig für die Themen Datenschutz und -sicherheit, z. B. durch Schulungen, sensibilisiert werden. Nur fünf der zehn geprüften Kommunen sensibilisierten ihre Mitarbeiterinnen und Mitarbeiter im Rahmen einer Schulung für die Themen Datenschutz und -sicherheit. Beachtenswert waren die unterschiedlichen Ansätze jener Kommunen, die Schulungen in relevantem Umfang durchführten. Eine Kommune setzte auf eine flächendeckende Information und Sensibilisierung möglichst vieler Mitarbeiterinnen und Mitarbeiter; eine andere Kommune legte den Schwerpunkt auf eine intensive Schulung allein ihrer IT-Mitarbeiterinnen und Mitarbeiter, welche anschließend als Multiplikatoren für andere Kolleginnen und Kollegen wirkten. Unabhängig vom gewählten Ansatz war festzustellen, dass diese beiden im Bereich der Schulung und Sensibilisierung aktiven Kommunen diejenigen mit den geringsten Handlungsbedarfen im Bereich der Informationssicherheit waren.

Die Bestellung einer oder eines Datenschutzbeauftragten ist gesetzliche Pflicht

Kommunen, die personenbezogene Daten automatisiert verarbeiten, sind verpflichtet, behördliche Datenschutzbeauftragte zu bestellen. Anstelle eigener Mitarbeiterinnen oder Mitarbeiter (interne Datenschutzbeauftragte) können Kommunen gemäß § 8a Abs. 1 NDSG auch externe Personen als Datenschutzbeauftragte beauftragen. Diese Personen gehören der datenverarbeitenden Stelle nicht an.

Datenschutzbeauftragte unterstützen die Kommunen bei der Sicherstellung des Datenschutzes. Als Datenschutzbeauftragte dürfen Kommunen nur Personen bestellen, die die notwendige Sachkenntnis auf den Gebieten der Datenverarbeitung, der behördlichen Organisationen und der einschlägigen Rechtsvorschriften sowie die erforderliche Zuverlässigkeit besitzen. Ferner dürfen Kommunen als Datenschutzbeauftragte nur Personen

---

[44] Hilfestellungen zu datenschutzgerechter Auftragsdatenverarbeitung und zur Ausgestaltung der Verträge mit beauftragten Stellen finden sich beispielsweise auf der Internetseite der Landesbeauftragten für den Datenschutz Niedersachsen (www.lfd.niedersachsen.de) unter Themen/Auftragsverarbeitung nach Art. 28 DS-GVO.

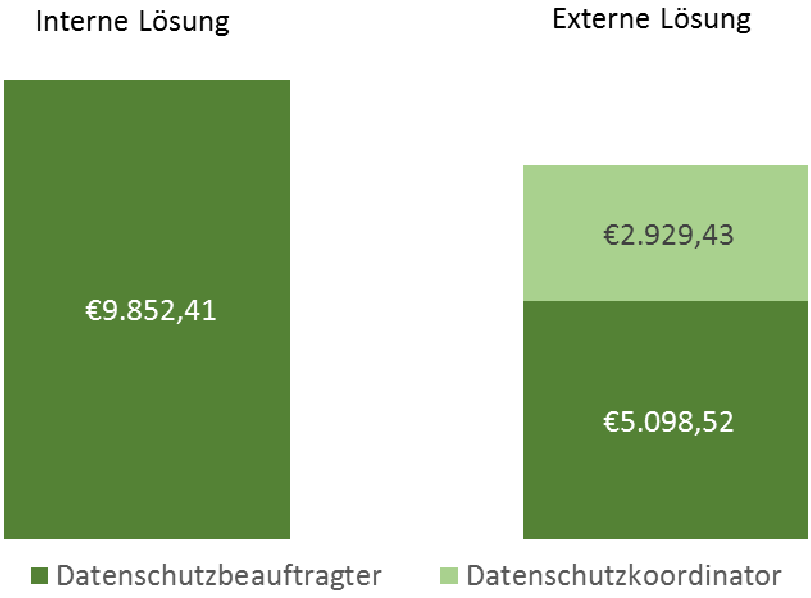
benennen, die durch ihre Bestellung keinen Interessenkonflikten mit anderen dienstlichen Aufgaben ausgesetzt sind (§ 8a Abs. 2 NDSG). Vier Kommunen hatten zum Zeitpunkt der örtlichen Erhebungen einen externen Datenschutzbeauftragten beauftragt. Fünf Kommunen bestellten einen internen Datenschutzbeauftragten, eine Kommune hatte zum Prüfungszeitpunkt keinen Datenschutzbeauftragten. Positiv war festzustellen, dass es allen Kommunen mit einem internen Datenschutzbeauftragten gelungen war, Datenschutzbeauftrage zu bestellen, deren sonstige Tätigkeiten nicht zu Interessenkonflikten führten. Dies wäre beispielsweise der Fall, wenn sie in ihrer Haupttätigkeit als Beschäftigte im IT- oder Personalbereich ebenfalls mit der Verarbeitung personenbezogener Daten befasst wären.

Der Handlungsbedarf war bei externen Datenschutzbeauftragten geringer

Aus den vor Ort erhobenen Antworten und gewonnenen Erkenntnissen wurde deutlich, welche Maßnahmen zur Informationssicherheit die Kommunen bereits ergriffen hatten und bei welchen Punkten noch Handlungsbedarf bestand. Über alle Kommunen stellte die überörtliche Kommunalprüfung im Mittel 39 Handlungsbedarfe fest. Deren Zahl fiel in Kommunen mit einem internen Datenschutzbeauftragten im Mittel um 34 % höher aus als in Kommunen, die einen externen Datenschutzbeauftragten bestellt hatten.

Externe Datenschutzbeauftragte waren nicht teurer

Neben den festgestellten Unterschieden bei den Handlungsbedarfen untersuchte die überörtliche Kommunalprüfung, ob die – nach den Erkenntnissen dieser Prüfung – zu besseren Ergebnissen führende Zusammenarbeit mit externen Datenschutzbeauftragten mit höheren Kosten verbunden war.



Ansicht 25: Vergleich durchschnittlicher Kosten für Datenschutzbeauftrage je Kommune p. a.

Die überörtliche Kommunalprüfung stellte fest, dass bei den hier geprüften Kommunen die Aufwendungen bei der internen Wahrnehmung der Tätigkeit des Datenschutzbeauftragten im Mittel bei rd. 9.900 € im Jahr lagen. Demgegenüber wendeten Kommunen für die externe Wahrnehmung der Tätigkeit des Datenschutzbeauftragen einschließlich dessen Koordinierung in der Kommune (Datenschutzkoordinator) im Mittel rd. 8.000 € auf, mithin etwa 19 % weniger.

Stellungnahmen der Kommunen

Die Kommunen berichteten in ihren Stellungnahmen zur Prüfungsmitteilung detailliert über bereits getroffene Maßnahmen zur Verbesserung der Informationssicherheit und des Datenschutzes. So teilte eine Kommune mit, dass sie nunmehr einen externen Datenschutzbeauftragten berufen wolle. Zwei Kommunen informierten über inzwischen abgeschlossene Verträge zur Auftragsdatenverarbeitung. Eine weitere Kommune kündigte den Umbau ihres Serverraums an, eine andere teilte die Anschaffung eines Programms zur Erstellung und Verwaltung von Verfahrensbeschreibungen mit. Durchweg zeigten die eingegangen Stellungnahmen, dass sich die Kommunen aufgrund der Prüfungsergebnisse intensiv mit ihrer Informationssicherheit auseinandergesetzt, bestehende Handlungsbedarfe zielgerichtet abgestellt oder Maßnahmen hierzu ergriffen haben.

Fazit

Die überörtliche Kommunalprüfung empfiehlt den Kommunen unter Beachtung des Grundsatzes der Wirtschaftlichkeit,

- ihre Mitarbeiterinnen und Mitarbeiter noch stärker für die Themen Informationssicherheit und Datenschutz zu sensibilisieren und ihnen zu diesen Themen bedarfsgerechte Schulungen anzubieten,
- der Erstellung und Pflege der Verfahrensbeschreibungen mehr Aufmerksamkeit zu widmen, ein vollständiges Verzeichnis aller Verfahrensbeschreibungen zu erstellen und den jeweiligen Datenschutzbeauftragten vorzulegen,[45]
- alle für sie erbrachten Auftragsdatenverarbeitungen personenbezogener Daten den gesetzlichen Erfordernissen entsprechend schriftlich zu regeln,[46]
- zu prüfen, ob die häufig komplexen, einem fortlaufenden Wandel unterliegenden Aufgaben des Datenschutzes und der -sicherheit allein noch ordnungsgemäß abgebildet werden können oder ob es zur Reduzierung von Risiken geboten erscheint, Aufgaben auf eine hierauf spezialisierte externe Stelle oder Einrichtung, wie einen Zweckverband oder ein Dienstleistungsunternehmen, zu übertragen und

---

45 Dabei sind die an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) angepassten neuen Regelungen des NDSG in der jeweils aktuellen Fassung zu berücksichtigen.

46 Ebenda.

- bei der Beantwortung der Frage, inwieweit sich die Kommune für eine interne oder externe Wahrnehmung der Aufgaben des Datenschutzbeauftragten entscheidet, für sich individuell die Kostenseite mittels Wirtschaftlichkeitsuntersuchung und Erfolgskontrolle in die Entscheidung mit einzubeziehen.