ÜBERÖRTLICHE PRÜFUNG

Umsetzung der DSGVO der Stadt Köln im Jahr 2019

INHALTSVERZEICHNIS

Datenschutz als kommunale Aufgabe

Ausgangslage

Die Datenschutz-Grundverordnung (DSGVO) wurde im April 2016 von den Gremien der EU beschlossen und gilt seit dem 25.05.2018 unmittelbar in den Mitgliedsstaaten. Gleichzeitig wurde das Datenschutzgesetz NRW (DSG NRW) grundlegend verändert und an die neuen Bestimmungen angepasst. Es füllt nunmehr die Öffnungsklauseln der DSGVO auf Landesebene aus bzw. setzt die Regelungsaufträge um.

Die Einführung der neuen DSGVO führt somit zu einer neuen Struktur des Datenschutzrechts, wenngleich zentrale materielle Kernelemente und Regelungen, wie z. B. die Zweckbindung der Daten, beibehalten bleiben.

Eine wesentliche Änderung der DSGVO ist eine verstärkte Einbindung der Behördenleitungen zur Umsetzung der datenschutzrechtlichen Vorgaben. Insgesamt erfordert die DSGVO ein umfassendes Zusammenspiel von behördlichen Datenschutzverantwortlichen, Organisationsverantwortlichen, IT-Beauftragten und Fachabteilungen.

Erhebung des Sachstandes und Dokumentation

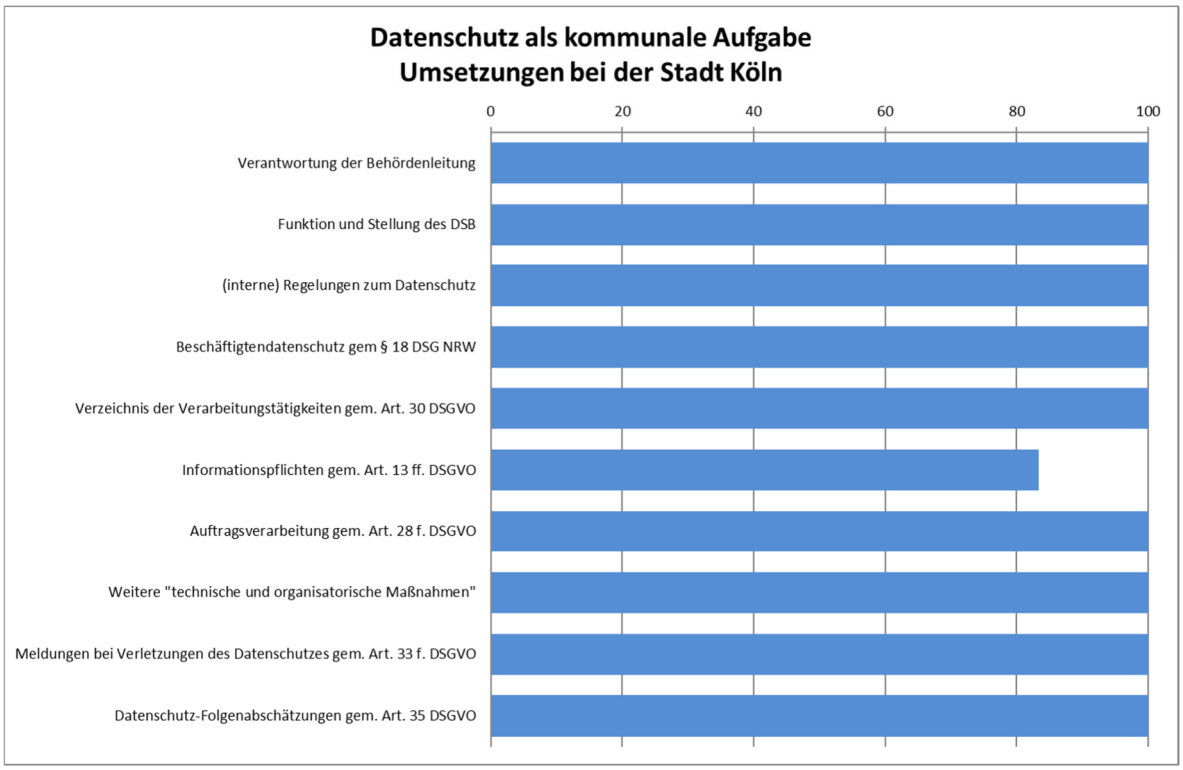
In Köln wurde das Gespräch zur Erhebung des Sachstandes zur aktuellen Umsetzung der DSGVO am 14. November 2019 mit dem Datenschutzbeauftragten und seinem Stellvertreter geführt. Die Inhalte wurden kurzfristig nach den Gesprächen gemeinsam für diese Dokumentation abgestimmt.

Der vorliegende „dokumentierte Sachstand“ bildet damit die Grundlage für die Aufnahme des Abschnitts „Umsetzung der DSGVO“ in den noch zu fertigenden abschließenden Prüfungsbericht.

Umsetzung der Anforderungen in der Stadt Köln

Zur Umsetzung der Vorgaben aus der DSGVO sind alle Kommunen in NRW verpflichtet. Im Interview wurden die jeweiligen Anforderungen erörtert und der Umsetzungsstand bestimmt.

Schematisch lässt sich der aktuell (November 2019) erreichte Stand wie folgt darstellen.



Die Ausprägung der Balken dient nur der Verdeutlichung. Sie soll insofern zunächst einen grafischen Eindruck von der in der Stadt Köln erreichten Umsetzungsreife vermitteln.

Die Darstellung repräsentiert – bezogen auf die jeweilige rechtliche Anforderung - demzufolge keinen erreichbaren Maximalwert, sondern soll aufzeigen, inwieweit bereits Handlungsnotwendigkeiten erkannt und konkrete Maßnahmen geplant oder sogar schon umgesetzt wurden.

Nachfolgend werden die einzelnen Anforderungen detaillierter beschrieben.

Verantwortung der Behördenleitung

Die DSGVO weist dem „Verantwortlichen“ bei der Verarbeitung personenbezogener Daten eine zentrale Rolle zu. „Verantwortlicher“ ist nach Art. 4 Nr. 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Für Kommunalverwaltungen bedeutet dies, dass „Verantwortlicher“ für die Verarbeitung personenbezogener Daten im Sinne der DSGVO die für die Verarbeitung zuständige öffentliche Stelle ist und damit „die Behörde“.

Diese kann durch interne Regelungen festlegen, wer die vielfältigen Pflichten des Verantwortlichen in der öffentlichen Stelle konkret erfüllen soll und kann dabei zwischen zentralen Ansprechpartnern für IT, Organisation und Datenschutz sowie den Fachabteilungen differenzieren. Dabei verbleibt die so genannte „Letztverantwortlichkeit“ immer bei der Behördenleitung.

Gem. Art. 24 DSGVO setzt die Behördenleitung daher geeignete technische und organisatorische Maßnahmen um. Hierbei hat sie die Art, den Umfang und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Darüber hinaus ist die Behördenleitung auch Adressat der Rechte der betroffenen Personen nach Art. 12 ff. DSGVO.

Der Verantwortliche hat nicht nur die Rechtmäßigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten zu gewährleisten, sondern muss auch den Nachweis dafür erbringen, dass die Datenverarbeitung im Einklang mit den Vorgaben der DSGVO erfolgt (sog. Rechenschaftspflicht, Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Die Rechenschaftspflicht besteht gegenüber der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

Die Gesamtverantwortung für die Umsetzung des Datenschutzes liegt bei der Oberbürgermeisterin der Stadt Köln. Die Amtsleitungen verantworten den Datenschutz für ihre Fachdienststellen. Die Amtsleitungen der Fachdienststellen benennen für ihren Verantwortungsbereich jeweils eine/n dezentrale/n Datenschutzkoordinator/in als Ansprechpartner/in für die dortigen Beschäftigten und Bürger. Daneben sind die Beschäftigten verpflichtet, die Vorgaben des Datenschutzes in ihrem Aufgabenbereich zu beachten. Die verschiedenen Verantwortungsebenen hat die Stadt Köln in einer Pyramide visualisiert und im Datenschutzmanagementkonzept zur Erfüllung der Rechenschafts- und Dokumentationspflichten (Accountability) veröffentlicht.

Das Datenschutzmanagementkonzept bildet den Überbau des modular aufgebauten Datenschutz- und IT-Managementsystems der Stadt Köln. Es hat zum Ziel, die Vorgehensweise zur Erfüllung der umfassenden Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2, Art. 24 Abs. 1 der DSGVO darzustellen.

Die technischen und organisatorischen Maßnahmen werden auf Grundlage einer Risikobewertung festgelegt, die die schutzwürdigen Belange bei Missbrauch bzw. den Verlust der personenbezogenen Daten berücksichtigt. Zur Auswahl erforderlicher und angemessener Sicherheitsmaßnahmen in Bezug auf den Datenschutz werden personenbezogene Daten nach dem Grad möglicher Beeinträchtigung aus der Perspektive der betroffenen Person sowie der schutzwürdigen Belange bei Missbrauch dieser Daten in fünf Schutzstufen untergliedert. Für die Risikobewertung wird ein Datenklassifizierungsbogen vorgegeben.

Funktion und Stellung des DSB

Nach Art. 37 DSGVO muss der Verantwortliche einen Datenschutzbeauftragten (DSB) benennen, der die notwendige berufliche Qualifikation und das Fachwissen vorweisen kann, um die ihm obliegenden Aufgaben sachgerecht erfüllen zu können. Der Verantwortliche ist verpflichtet

die Kontaktdaten des DSB auf der Homepage zu veröffentlichen und ihn bei der Landesbeauftragten für Datenschutz und Informationsfreiheit zu melden.

Zu den originären Aufgaben des DSB zählen im Wesentlichen die Überwachung und Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften sowie die Beratung der Verantwortlichen und Mitarbeiter. Eine Ausweitung der Zuständigkeiten ist möglich, soweit die zu übertragenden Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Dem DSB sind zur Erfüllung der Aufgaben die erforderlichen Ressourcen zur Verfügung zu stellen. Ihm ist ferner der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewährleisten.

Der Verantwortliche muss in geeigneter Weise sicherstellen, dass der DSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

Bei der Stadt Köln sind ein behördlicher Datenschutzbeauftragter und ein ständiger Stellvertreter benannt und bei der LDI gemeldet worden. Der berufene DSB sowie der Stellvertreter besitzen die in Art. 37 Absatz 5 DSGVO geforderte berufliche Qualifikation und das Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis. Beide haben neben ihrer Tätigkeit als behördliche DSB keine weiteren Aufgaben übertragen bekommen. Auf der Website der Stadt Köln sind die Kontaktdaten und umfangreiche Informationen zu den Aufgaben des Datenschutzbeauftragten veröffentlicht worden.

Der Aufgabenbereich des DSB wurde an die neuen Vorgaben der DSGVO anpasst. Der DSB ist gem. § 8 der Dienstanweisung Datenschutz und Informationsfreiheit frühzeitig und umfassend im Rahmen der datenschutzrechtlichen Zulässigkeitsprozesse zu konsultieren.

Der DSB berichtet dem Stadtdirektor und damit gem. Art. 38 Absatz 3 Satz 3 DSGVO unmittelbar der höchsten Managementebene. Des Weiteren erstellt der DSB in unregelmäßigen Abständen Datenschutzberichte sowie zwei Mal jährlich einen internen Sachstandsbericht.

Regelungen zum Datenschutz

Aus Art. 24 Absatz 2 DSGVO lässt sich ableiten, dass es der Leitung der jeweiligen öffentlichen Stelle insbesondere obliegt, ein Datenschutzkonzept aufzustellen, mit dem sichergestellt wird, dass im Zuständigkeitsbereich der öffentlichen Stelle die datenschutzrechtlichen Pflichten erfüllt und datenschutzrechtliche Bestimmungen eingehalten werden. Dies setzt voraus, dass datenschutzrechtliche Zuständigkeiten konkret einzelnen Organisationseinheiten oder Personen innerhalb der öffentliche Stelle zugewiesen und notwendige Verfahrensabläufe festgelegt werden.

Vorgaben der DSGVO, die die IT-Sicherheit betreffen sind in ein IT-Sicherheitskonzept, eine IT-Sicherheitslinie oder vergleichbares Dokument aufzunehmen. Berechtigungs- und Löschkonzepte sind wichtige interne Regelungen, um die datenschutzrechtlichen Pflichten umzusetzen.

Wie bereits dargestellt, bildet das Datenschutzmanagementkonzept den Überbau des modular aufgebauten Datenschutz- und IT-Managementsystems der Stadt Köln. Ein Baustein sind die Regelungen und Anweisungen, worunter auch die Dienstanweisung „Datenschutz und Informationsfreiheit“ gefasst ist. Ergänzend hat die Stadt Prozessbeschreibungen und Formulare der datenschutzrechtlichen und IT-sicherheitstechnischen Zulässigkeitsprozesse für Verarbeitungstätigkeiten, insbesondere Datenschutzfolgenabschätzungen erstellt. Des Weiteren unterstützt

das „Handbuch der Stadtverwaltung Köln“ die Umsetzung der rechtlichen Vorgaben als Leitfaden im dienstlichen Alltag.

Bei der Stadt Köln bestehen Zugriffsberechtigungen im Active Directory und innerhalb der Fachverfahren. Bei Mitarbeiterwechseln gibt es einen Meldedienst, welcher die Änderung der Zugriffsberechtigungen sicherstellt.

Die Dienstanweisung zum Datenschutz und Informationsfreiheit enthält Regelungen zur Löschung von Daten. Nach § 10a der Dienstanweisung werden keine allgemein gültigen Löschregeln und Löschfristen definiert, sondern die Verantwortlichen erarbeiten für jede Verarbeitung eigenständige Löschkonzepte und –routinen. Darüber hinaus sind die Löschfristen und entsprechenden Verantwortlichkeiten im Verarbeitungsverzeichnis zu hinterlegen.

Beschäftigtendatenschutz gem. § 18 DSG NRW

Auf der Grundlage von Art. 88 DSGVO regelt § 18 Abs. 1 DSG NRW den Beschäftigtendatenschutz. Hiernach gelten für die Verarbeitung von personenbezogenen Daten von Bewerberinnen und Bewerbern sowie Beschäftigten besondere Voraussetzungen. Diese Daten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht oder die oder der Beschäftigte eingewilligt hat.

Die Bestandsmitarbeiterinnen und -mitarbeiter wurden im Mai 2018 über die verarbeiteten Beschäftigtendaten durch eine Beilage zum Gehaltszettel informiert. Neue Kräfte werden bei der Einstellung datenschutzrechtlich mit verbindlicher Unterschrift verpflichtet. Schulungen werden seitens des DSB angeboten, E-Learning-Module zum Datenschutz und der IT-Sicherheit sind in konkreter Planung. Die Personalvertretung wurde seitens des DSB in mehreren Terminen über die Regelungen der DSGVO und insbesondere den Beschäftigtendatenschutz informiert. Bei der Verarbeitung und Veröffentlichung von Mitarbeiterfotos wird die Einwilligung der betroffenen Personen eingeholt.

Bewerberdaten dürfen nur zweckgebunden gespeichert werden, was in der Regel nur das Bewerbungsverfahren umfasst. Sollte der Verantwortliche die Daten länger speichern wollen, benötigt er dafür eine Einverständniserklärung des Bewerbers.

Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO

Gem. Art. 30 DSGVO sind die Verantwortlichen verpflichtet ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Bevor neue Verarbeitungen in das Verzeichnis aufgenommen werden, soll dem Datenschutzbeauftragten die Gelegenheit zur Stellungnahme gegeben werden. Das Verarbeitungsverzeichnis muss neben den automatisierten Verarbeitungen (Programme/Fachverfahren) auch nicht-automatisierte Verarbeitungen (Karteien/Archive) umfassen. Grundsätzlich ist der Verantwortliche zur Führung des Verarbeitungsverzeichnisses verpflichtet. Er kann diese Pflicht jedoch auf den DSB übertragen. Aber auch im Übertragungsfall muss der Verantwortliche weiterhin für die Vollständigkeit und Aktualität des Verzeichnisses sorgen.

Sämtliche Tätigkeiten der Stadt Köln, mit denen personenbezogene Daten verarbeitet werden, werden von den zuständigen Fachdienststellen in Verarbeitungsverzeichnissen dokumentiert. Hierzu zählen IT-Fachanwendungen, Auftragsverarbeitungen/gemeinsame Verantwortlichkeiten, allgemeine Verarbeitungstätigkeiten sowie Videoüberwachung.

Die Verarbeitungsverzeichnisse sind Dokumentationen der datenschutzrechtlichen und IT-sicherheitstechnischer Zulässigkeitsprüfungen. Die Eintragungen werden im IT-Sicherheitsportal (Datenbanklösung) zentral erfasst.

In der Dienstanweisung ist geregelt, dass der DSB Form und Inhalt der Datenschutzdokumente vorgibt und die ordnungsgemäße Umsetzung überwacht. Der DSB hat die Datenschutz-Koordinatoren im Vorfeld geschult. Er erhält alle Verarbeitungsverzeichnisse zur Kenntnis und dokumentiert die erforderlichen datenschutzrechtlichen Konsultationen.

Informationspflichten gem. Art. 13 ff. DSGVO

- **Sachstand**
  Die Datenschutzhinweise im Bewerbungsprozess entsprechen nicht den Vorgaben der DSGVO.

Bei der Erhebung von personenbezogenen Daten hat der Verantwortliche Informationspflichten gem. Art. 13 f. DSGVO zu beachten. Die Informationen sind in präziser, transparenter, verständlicher Form und in einer klaren und einfachen Sprache zu erteilen. Bei Papierformularen sollten zumindest die Grundinformationen sowie ein Hinweis mitgeteilt werden, wo weitergehende Informationen erhältlich sind. Bei der Erhebung im Internet sollte auf der Erhebungsseite ein deutlich sichtbarer Link auf die Informationen verweisen. Bei einem Einsatz von Videoüberwachung müssen Hinweistafeln über die datenschutzrechtlichen Grundinformationen informieren.

Bei der Umsetzung der Informationspflichten bei der Stadt Köln werden drei verschiedene Ebenen unterschieden. Zum einen werden in der allgemeinen Datenschutzerklärung die grundsätzlichen Regelungen im Umgang der Stadt Köln mit dem Datenschutz dargestellt. Daneben werden den Betroffenen bei jeder Aufgabe, bei der personenbezogene Daten erhoben werden, verfahrensspezifische Datenschutzerklärungen und –einwilligungen zur Verfügung gestellt. Zuletzt werden Informationen zu ordnungsbehördlichen Verfahren auf der Internetseite bereitgestellt.

Nach Auskunft der Gesprächspartner kann die Umsetzung der Informationspflichten weitestgehend gewährleistet werden. Das operative Vorgehensmodell zur DSGVO-Umsetzung hat die Gewährleistung der entsprechenden Informationsrechte prioritär zum Mai 2018 beinhaltet. Die Informationsrechte sind auch elementarer Bestandteil der datenschutzrechtlichen Zulässigkeitsprozesse z.B. für IT-Fachanwendungen und Auftragsverarbeitung. Strukturell sind somit alle Vorgaben für die Umsetzung der Anforderungen der DSGVO nach Art. 13, 14 gelegt. Im Rahmen der datenschutzrechtlichen Beratung und Kontrolle fallen ungeachtet dessen immer mal wieder einzelne Verarbeitungsvorgänge auf, in denen die Datenschutzinformationen nachzureglulieren sind.

Bei neuen Online-Services, bei denen personenbezogenen Daten erhoben werden, wird durch einen Freigabeprozess sichergestellt, dass die pflichtigen Informationen mitgeteilt werden. Sollten die Vorgaben nach Art. 13 DSGVO nicht umgesetzt sein, erfolgt keine Freischaltung der Dienstleistung durch das Amt für Informationsverarbeitung.

Allerdings entsprechen die Datenschutzhinweise im Bewerbungsprozess nicht den Vorgaben der DSGVO. Zum einen beziehen sich die genannten Rechtsgrundlagen auf die alte Rechtslage. Zum anderen werden die Bewerberdaten für die Dauer von zwei Jahren ab Eingang der Bewerbung gespeichert, sofern der Bewerber dieser Vorgehensweise nicht schriftlich widerspricht.

Bei der Stadt Köln sind Kameras zur Überwachung von kommunalen Einrichtungen bzw. öffentlich zugänglichen Bereichen installiert. Die Informationspflichten werden durch angebrachte Hinweistafeln mitgeteilt. Hierzu wird ein eigens entwickeltes Muster genutzt, welches einen QR-Code zu einer Internetseite mit weiteren Informationen beinhaltet.

→ **Hinweis**
Der Verantwortliche sollte die Datenschutzhinweise im Bewerbungsprozess an die Regelungen der DSGVO anpassen.

Auftragsverarbeitung gem. Art. 28 f. DSGVO

Bei der Auftragsvergabe muss die Behördenleitung die Geeignetheit des Auftragsverarbeiters prüfen. Zur Prüfung können u. a. Verhaltensregeln oder Zertifizierungen nach Art. 40 DSGVO herangezogen werden. In einem Vertrag sind

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen

festzulegen. Ältere Verträge über Auftragsverarbeitungen sind an die neuen Vorgaben der DSGVO anzupassen.

Bei der Stadt Köln besteht über den datenschutzrechtlichen Zulässigkeitsprozess im Verarbeitungsverzeichnis eine Übersicht über die Auftragsverarbeitungen. Die Auftragsverarbeitungen werden ebenfalls anhand der o. g. Schutzstufen bewertet. Die Einhaltung der TOMs bei den Auftragnehmern und Auftragsverarbeitern werden über eine sog. Checkliste Datenschutz verbindlich dokumentiert. Diese ist Bestandteil des Verarbeitungsvertrages. Ab der Schutzstufe C wird die Einhaltung der technischen und organisatorischen Maßnahmen (TOMs) durch die Stadt vor Ort überprüft.

Die bestehenden Verträge zur Auftragsverarbeitung wurden an die Vorgaben der DSGVO angepasst. Darüber hinaus wurde seitens der Stadt ein Muster für Verträge erstellt, welches in der

Regel als Grundlage für neue Vertragsabschlüsse genutzt wird. Spezielle Verarbeitungsverzeichnisse für Auftragsverarbeitung wurden entwickelt.

Weitere „technische und organisatorische Maßnahmen“

Gem. Art. 24 Abs. 1 und Art. 32 DGSVO stellt die Behördenleitung sicher, dass geeignete TOMs zum Schutz der verarbeiteten Daten getroffen werden. Zum Nachweis im Rahmen der Rechenschaftspflicht gem. Art. 5 DSGVO sollen die ergriffenen Maßnahmen schriftlich dokumentiert werden.

Wie bereits dargestellt werden die Schutzbedarfe im Verarbeitungsverzeichnis dokumentiert. Auf Grundlage der Schutzbedarfsfeststellung werden mithilfe einer Checkliste unterschiedliche TOMs abgeleitet.

Die eingesetzten Fachverfahren werden grundsätzlich auf datenschutzfreundliche Voreinstellungen (Datensparsamkeit/Privacy by Default/Privacy by Design) geprüft.

Die Sensibilisierung der Beschäftigten hinsichtlich der Einhaltung der datenschutzrechtlichen Vorgaben erfolgt auf verschiedene Weise. Zunächst sind im städtischen Intranet Informationen zum Datenschutz bereitgestellt. Daneben hat der DSB die dezentralen Datenschutzkoordinatoren geschult. Des Weiteren bietet der DSB allgemeine und spezielle Datenschutzschulungen an. Perspektivisch soll eine E-Learning-Plattform zur Sensibilisierung und Fortbildung in den Themen Datenschutz und IT-Sicherheit genutzt werden.

Sowohl die Beschäftigten als auch Praktikanten unterschreiben eine schriftliche Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen. Die Verpflichtung wird zentral durch das Personalamt vorgenommen und dokumentiert.

Meldungen bei Verletzungen des Datenschutzes gem. Art. 33 f. DSGVO

Datenschutzverletzungen sind innerhalb von 72 Stunden der LDI NRW zu melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Darüber hinaus sind die Betroffenen über die Datenschutzverletzungen zu informieren, falls die Datenschutzverletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten der Personen zur Folge hat. Zur Meldung von Verstößen hat die LDI NRW ein Formular bereitgestellt.

Die Datenschutz Dienstanweisung für die Stadtverwaltung Köln beinhaltet die wichtigsten Vorgaben der DSGVO zum Umgang mit Datenschutzverstößen. Darüber hinaus sind im Intranet weitere Hinweise und Vordrucke veröffentlicht. Die Risikobewertung wird durch die Fachdienststelle mit dem DSB und dem IT-Sicherheitsverantwortlichen geprüft und bewertet. Die ggf. erforderliche Meldung erfolgt durch die zuständige Fachdienststelle.

Bis zum Zeitpunkt der Prüfung wurden etwa ein Dutzend Datenschutzverletzungen an die LDI gemeldet.

Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO

Eine Datenschutz-Folgenabschätzung (DSFA) ist durchzuführen, wenn die Verarbeitung von personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Der Verantwortliche muss hierzu zunächst die Risiken der Verarbeitungen beschreiben und bewerten. Er muss anschließend entscheiden, ob ein hohes Risiko besteht und folglich eine Datenschutz-Folgenabschätzung durchzuführen ist. Der Verantwortliche muss sowohl neue Verarbeitungen als auch bestehende Verarbeitungen bewerten, die weitreichend geändert wurden. Anhand der Risikobewertung muss der Verantwortliche Maßnahmen zur Abhilfe formulieren und umsetzen.

Im Rahmen des datenschutzrechtlichen Zulässigkeitsprozesses werden die Risiken für die Rechte und Freiheiten der betroffenen Personen eingeschätzt, die durch Verarbeitung entstehen können. Der gesamte Prozess zur Durchführung der DSFA ist ein einem Prozessablaufplan modelliert und in der Dienstanweisung Datenschutz und Informationsfreiheit festgehalten.

Die Verantwortung für die Durchführung der DSFA obliegt der zuständigen Fachdienststelle. Diese bedient sich der Beratung und Unterstützung der für die technische Datenverarbeitung zuständigen Organisationseinheit (Amt für Informationsverarbeitung) sowie des IT-Sicherheitsverantwortlichen. Die Beratung wird in einem strukturierten datenschutzrechtlichen Konsultationsprotokoll erfasst und im Verarbeitungsverzeichnis dokumentiert.

Einschätzung des aktuellen Umsetzungsstandes

Die Stadt Köln hat ein umfassendes Datenschutzmanagementsystem etabliert. Dabei greift sie auf ein eigens entwickeltes Datenschutzmanagementkonzept zurück, welches den Oberbau des modularen aufgebauten Datenschutz- und IT-Managementsystem bildet. Mit den weiteren Regelungen und Anweisungen verfügt die Stadt über gute und individuelle Vorgaben.

Die Verantwortung zur Gewährleitung des Datenschutzes und der IT-Sicherheit wurde im Datenschutzmanagementkonzept sowie der Dienstanweisung Datenschutz und Informationsfreiheit eindeutig geregelt. Neben der Gesamtverantwortung der Oberbürgermeisterin setzen die weiteren Leitungskräfte der verschiedenen Ebenen die Vorgaben der DSGVO im Wesentlichen um. Die Beschäftigten beachten den Datenschutz in ihrem Tätigkeitsbereich und setzen ihn entsprechend um.

Insgesamt ist die Stadt Köln die Umsetzung der Vorgaben der DSGVO planvoll und strategisch angegangen. Ein zentrales Element ist die datenschutzrechtliche Zulässigkeitsprüfung, welche u. a. auch die Risikobewertung und ggf. DSFA umfasst. Sämtliche Tätigkeiten sind in den Verarbeitungsverzeichnissen zu dokumentieren.

Darüber hinaus überwacht der DSB den Stand der Umsetzung der DSGVO. Hierzu zählen besonders die Umsetzung der Informationspflichten und datenschutzrechtlichen Zulässigkeitsprozesse. Dennoch wurde im Rahmen der Prüfung zumindest Nachholbedarf im Bereich des Datenschutzes bei den Informationspflichten festgestellt. Dies trübt die insgesamt sehr gute Gesamteinschätzung geringfügig.

Kontakt

Gemeindeprüfungsanstalt Nordrhein-Westfalen
Heinrichstraße 1, 44623 Herne

Postfach 10 18 79, 44608 Herne
t 0 23 23/14 80-0
f 0 23 23/14 80-333
e info@gpa.nrw.de
i www.gpa.nrw.de