Datenschutzmanagementkonzept

der Stadt Köln

zur Erfüllung der Rechenschafts-

und Dokumentationspflichten

nach Art. 5 Abs. 2 und

24 Abs. 1 DSGVO

(Accountability)

Inhalt:

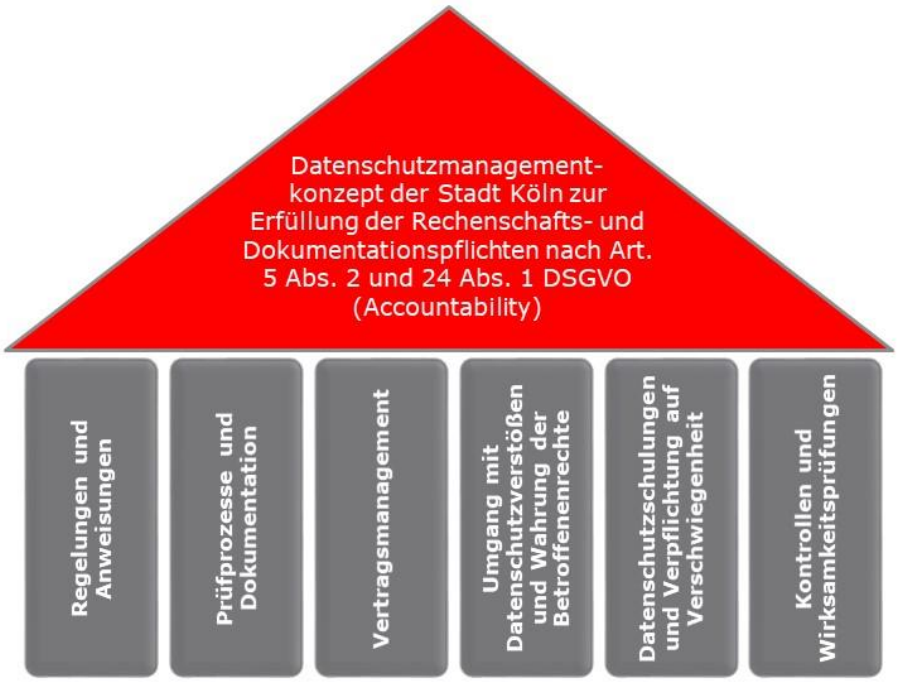
Datenschutzmanagementkonzept der Stadt Köln zur Erfüllung der Rechenschafts- und Dokumentationspflichten – i.d.F v. 11.12.18

I. Präambel

Dieses Datenschutzmanagementkonzept hat zum Ziel, die Vorgehensweise zur Erfüllung der umfassenden Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2, Art. 24 Abs. 1 der EU-Datenschutzgrundverordnung (DSGVO) der Stadt Köln darzustellen. Es dient als zentrales Dokument eines modular aufgebauten Datenschutz- und IT-Managementsystems für die Stadt Köln und ihrer Verwaltung (s. nachfolgendes Schaubild). Gleichzeitig bildet das Konzept die Grundlage für datenschutzrechtliche Prüfungen durch den/die Landesbeauftragte/n für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) bzw. den/die Bundesbeauftragte/n für den Datenschutz und Informationsfreiheit (s. insb. Art. 58 Abs. 1 lit. a DSGVO).

Durch dieses Konzept soll die Einhaltung der Regelungen der DSGVO nicht nur gewährleistet, sondern auch der dokumentierende Nachweis der Einhaltung an sich geschaffen werden. Dieses Konzept sieht einen kontinuierlichen und auf ständige Verbesserung ausgerichteten Optimierungsprozess vor und wird regelmäßig – spätestens alle zwei Jahre – auf seine Wirksamkeit überprüft.

Die Oberbürgermeisterin
Stadt Köln



II. Grundzüge der Datenschutzpolitik der Stadt Köln

Die Stadt Köln misst dem Datenschutz und der IT-Sicherheit größte Bedeutung bei. Die Erhebung und Verarbeitung aller personenbezogenen Daten geschieht unter Beachtung der geltenden datenschutzrechtlichen Vorschriften, insbesondere der EU-Datenschutzgrundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) und des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW).

Dabei werden folgende datenschutzrechtlichen Prinzipien und Grundsätze beachtet:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DSGVO)

  Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise.

- Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

  Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke, wobei eine Weiterverarbeitung diesen Zwecken nicht zuwider laufen darf.

- Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

  Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß.

- Richtigkeit (Art. 5 Abs. lit. d DSGVO)

  Verarbeitung sachlich richtiger und ggf. aktuellster Daten, Treffen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung unzutreffender Daten.

- Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)

  Speicherung von Daten mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist.

- Integrität, Vertraulichkeit, Verfügbarkeit (Art. 5 Abs. 1 lit. f DSGVO)

  Ergreifen geeigneter technischer und organisatorischer Maßnahmen zum angemessenen Schutz der Daten, insbesondere vor unbefugter und/oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung.

Zur Dokumentation dieser Prinzipien bezogen auf alle Maßnahmen, bei denen personenbezogene Daten verarbeitet werden, führt die Stadt Köln Verarbeitungsverzeichnisse gemäß Art. 30 DSGVO, in welchen alle verfahrensspezifischen Verarbeitungstätigkeiten aufgeführt werden (s. auch Ziff. V.). Eine Übersicht hierzu wird durch das Führen laufend aktualisierter Listen bei der/dem Datenschutzbeauftragten hergestellt.

III. Regelungen und Anweisungen (Rechtsgrundlagen)

Die rechtlichen Vorgaben zum Umgang mit Datenschutz und IT-Sicherheit (Compliance) unterteilen sich in städtische Regelungen und geltende Rechtsvorschriften.

1. Regelungen und Anweisungen der Stadt Köln

- Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln
- Prozessbeschreibungen und Formulare der datenschutzrechtlichen und IT-sicherheitstechnischen Zulässigkeitsprozesse für Verarbeitungstätigkeiten, insbesondere Datenschutzfolgenabschätzungen (s. Ziff. V.)
- Handbuch der Stadtverwaltung Köln (als Leitfaden für den dienstlichen Alltag)
- Dienstanweisung zur Nutzung und zum Betrieb der IV-Infrastruktur
- IT-Sicherheitshandbuch
- Richtlinie zur Behandlung von Sicherheitsvorfällen
- Dienstanweisung Betrieb für Geräte der Informations- und Telekommunikationstechnik (IuK)
- Dienstanweisungen Mail und Internet

- Richtlinie für die Bedarfsprüfung bei Hard- und Softwarebeschaffungen sowie die Verwertung von nicht mehr benötigter Software
- Arbeitsanweisungen und Handbücher von 12 und den Fachdienststellen für einzelne IT-Fachanwendungen
- Dienststellenspezifische Dienstanweisungen und Regelungen zum Datenschutz (z.B. Geschäftsanweisung Statistikstelle)

2. Geltende Rechtsvorschriften

Die gesetzlichen Rahmenbedingungen zur Verarbeitung personenbezogener Daten ergeben sich aus der DSGVO (Art. 6 Abs. 1, Art. 9 Abs. 2), dem BDSG und DSG NRW sowie weiteren bundes- und landesspezifischen Spezialregelungen z.B. zum Sozial- und Gesundheitsschutz.

Spezialgesetzliche Regelungen mit Vorgaben zur IT-Sicherheit bleiben von den Ausführungen dieses Datenschutzkonzeptes unberührt.

IV. Strukturen (Organisation der Verantwortlichkeiten)

Zur Gewährleistung des Datenschutzes und der IT-Sicherheit wurden folgende Funktionen und Beratungsgremien bei der Stadtverwaltung eingerichtet und personell besetzt:

- Behördliche/r Datenschutzbeauftragte/r und Stellvertreter/in (weisungsfrei mit unmittelbarer Anbindung an den/die Oberbürgermeister/in)
- Dezentrale Ansprechpartner/innen für den Datenschutz (Dezentrale Datenschutzkoordinatoren/innen) in den Fachdienststellen
- IT-Sicherheitsverantwortliche/r
  (als Stabstelle bei der Amtsleitung 12)
- Amt 12 mit verschiedenen Abteilungen zur Einrichtung und dem Betrieb von Informationsverarbeitungssystemen
- Funktionseinheit IT-Sicherheit
  (als Sachgebiet 122/3 im Amt 12)

- Unterausschuss digitale Kommunikation und Organisation (UdiKO) (als beratendes Fachgremium für den Ausschuss Allgemeine Verwaltung und Rechtsfragen/ Vergabe/ Internationales – AVR)

- Beirat für Sicherheit in der Informationstechnik (SKIT) (als verwaltungsinternes Beratungs- und Beschlussgremium)

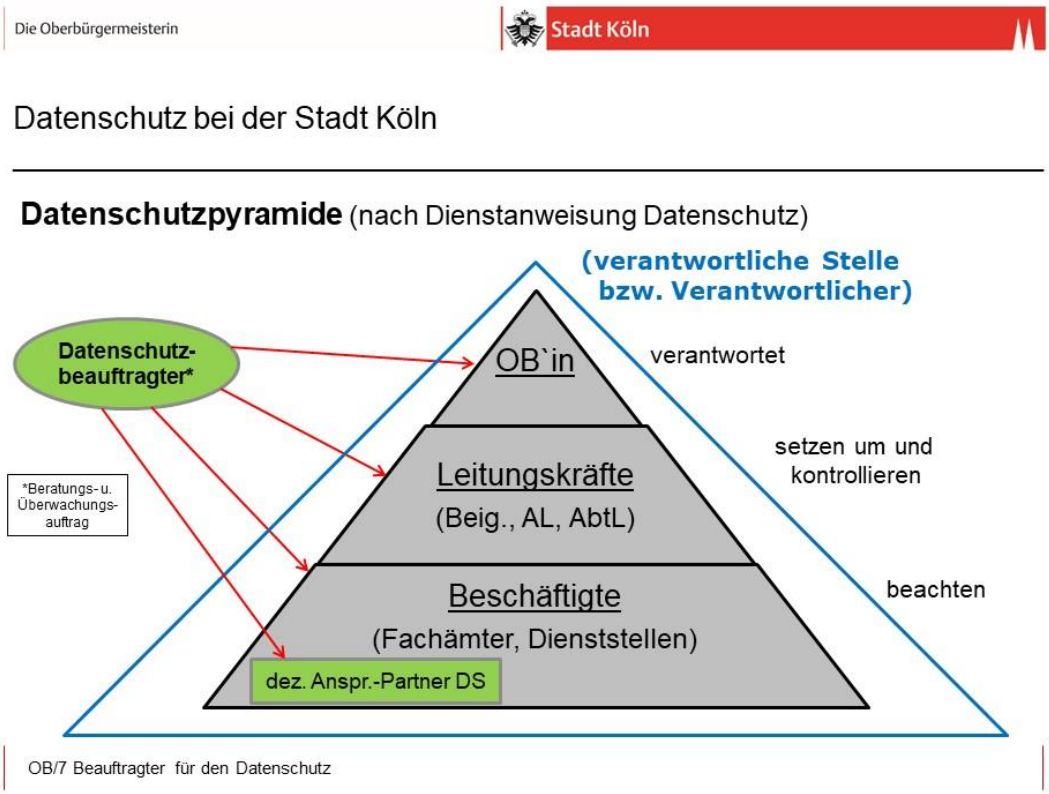
Gesamtverantwortliche/r i.S. v. Art. 4 Nr. 7 DSGVO ist der/die Oberbürgermeister/in der Stadt Köln, der/die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Hierarchisch nachgeordnet sind die Leitungskräfte (Beigeordnete, Amtsleitungen, Abteilungsleitungen etc.) der Stadtverwaltung Köln, die alle Maßnahmen und Regelungen i.S.d. DSGVO umsetzen und kontrollieren, also operativ für die Einhaltung des Datenschutzes verantwortlich sind (s. nachfolgendes Schaubild). Den Leitungen der Fachdienststellen obliegt im Wege der Delegation durch den/die Oberbürgermeister/in über die zuständigen Fachbeigeordneten die datenschutzrechtliche Verantwortung für den zugeordneten Aufgabenbereich. Dies drückt sich seit dem 25.05.18 beispielsweise in der Schlusszeichnungsverantwortung für datenschutzrechtliche und IT-sicherheitstechnische Zulässigkeitsprozesse, wie z.B. Datenschutzfolgenabschätzungen aus (detaillierte Regelungen in der Dienstanweisung Datenschutz und Informationsfreiheit der Stadt Köln).

Die Beschäftigten in den Fachdienststellen der Stadtverwaltung Köln beachten die Regelungen des Datenschutzes für die ihnen übertragenen Aufgaben in eigener Verantwortung.

Der/die behördliche Datenschutzbeauftragte und sein/e Stellvertreter/in stehen allen Hierarchieebenen der Stadtverwaltung beratend und für die nach der DSGVO verpflichtend vorgesehenen Konsultationen im Rahmen der datenschutzrechtlichen Prüfprozesse zur Verfügung.

Zudem benennen die Fachdienststellen verbindlich dezentrale Ansprechpartner/innen in Angelegenheiten des Datenschutzes vor Ort (dezentrale Datenschutzkoordinatoren/innen). Diese werden jeweils durch den/die behördliche/n Datenschutzbeauftragte/n in ihre Funktion eingewiesen. Die hierbei zugewiesenen Aufgaben sind der Dienstanweisung Datenschutz und Informationsfreiheit der Stadt Köln zu entnehmen.



V. Prüfprozesse und Dokumentation

1. Datenschutzrechtliche und IT-sicherheitstechnische Zulässigkeitsprüfung (incl. Datenschutzfolgenabschätzung)

Bei jeder Art der automatisierten Verarbeitung personenbezogener Daten durch eine IT-Fachanwendung oder einen Web-Dienst bzw. ein IT-Basisprodukt ist bei der Stadt Köln ein datenschutzrechtliches und IT-sicherheitstechnisches Inbetriebnahmeverfahren etabliert (s. nachfolgendes Schaubild). Dieser Prüfprozess wird im Falle eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen im Wege einer Datenschutzfolgenabschätzung durchgeführt (Art. 35 ff. DSGVO).

Akteure in diesem datenschutzrechtlichen Zulässigkeitsverfahren sind die zuständige Fachdienststelle, das Amt für Informationsverarbeitung (12) – dort insbesondere die Inbetriebnahmekoordinatoren und die IT-Sicherheit, der/die IT-Sicherheitsverantwortliche sowie der/die Beauftragte für den Datenschutz.

Vor jeder Verarbeitung personenbezogener Daten ist eine Risikobewertung mit Blick auf das informationelle Selbstbestimmungsrecht aus Sicht der betroffenen Person durchzuführen. In diesem Zusammenhang sind folgende Prüfschwerpunkte und Dokumente vorgesehen:

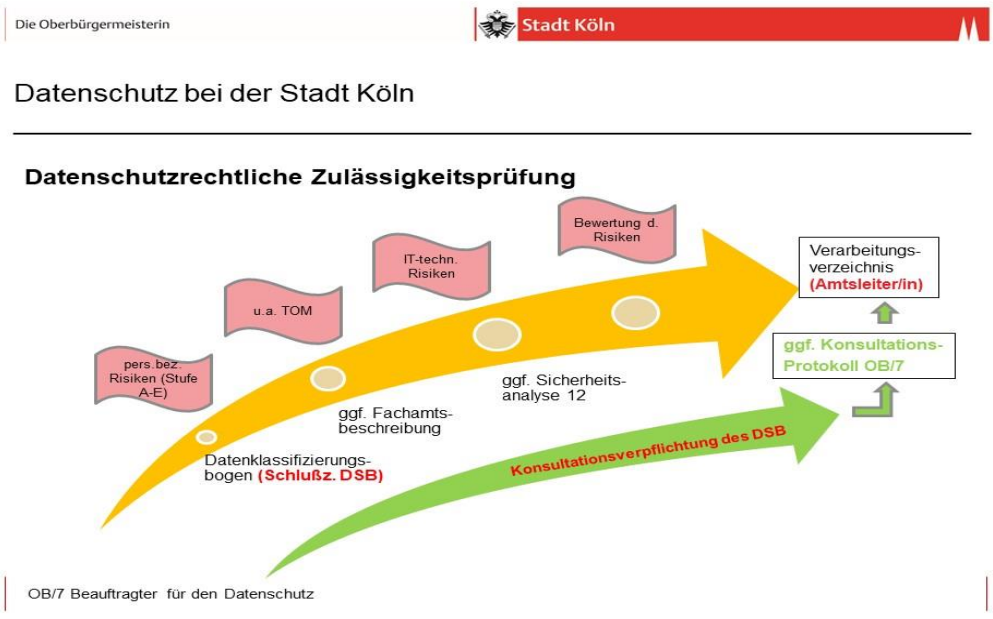
- Risikoanalyse mittels eines Datenklassifizierungsbogens: Qualifizierte Einschätzung der Schutzwürdigkeit der personenbezogenen Daten über Schutzstufen 0, A bis E

- Fachamtsbeschreibung:
  Festlegung der technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten auf der Grundlage der Risikobewertung der zuständigen Fachdienststelle

- Sicherheitsanalyse 12:
  IT-sicherheitstechnische Prüfung zur Einbindung der Fachanwendung in das städtische Netz – CAN – auf der Grundlage der Risikoanalyse

- Nachweis der Konsultation des Datenschutzbeauftragten nach Art. 35 Abs. 2, 39 Abs. 1 lit. c DSGVO durch den Datenklassifizierungsbogen bzw. der Datenschutzfolgenabschätzung

- Verarbeitungsverzeichnis nach Art. 30 DSGVO: Verfahrensspezifische Dokumentation des datenschutzrechtlichen und IT-sicherheitstechnischen Zulässigkeitsprozesses



Dieser Dokumentationsprozess dient zum einen der Qualitätssicherung als auch der steten Überprüfung der Maßnahmen an die Anforderungen der DSGVO, insbesondere in Bezug auf die Datenschutzfolgenabschätzung nach Art. 35 DSGVO.

In folgenden Fällen sind datenschutzrechtliche Zulässigkeitsprüfungen vorgesehen, die in eigens hierfür entwickelten Verarbeitungsverzeichnissen dokumentiert werden:

a) IT-Fachanwendungen und Web-Dienste (Online-Verfahren)

b) Auftragsverarbeitungen bzw. ggf. gemeinsame Verantwortlichkeit

c) Videoüberwachungen

d) sonstige darüber hinausgehende Verarbeitungstätigkeiten

Die Regelungen und die zu verwendenden Formulare zum operativen Vorgehen sind in der Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln festgelegt und darüber hinaus dem Intranet-Auftritt des/der Datenschutzbeauftragten zu entnehmen.

2. Dokumentation (Verarbeitungsverzeichnisse)

Die umfassende Dokumentation der datenschutzrechtlichen Zulässigkeitsprüfung auf der Grundlage insbesondere der in Ziff. 1 aufgeführten Prüfschwerpunkte erfolgt unter Berücksichtigung aller in Art. 30 DSGVO genannten verbindlichen Angaben in jeweils einem verfahrensspezifischen Verarbeitungsverzeichnis (s. Ziff. 1 a) bis d)).

3. Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten

Die technischen und organisatorischen Maßnahmen werden im Rahmen jeder Verarbeitung von personenbezogenen Daten individuell auf das jeweilige Verfahren angewendet und dokumentiert. Grundlage bildet das "Standard-Datenschutzmodell" (SDM). Als SDM bezeichnen die deutschen Datenschutzaufsichtsbehörden eine Methode, mit der für den Bereich des operativen Datenschutzes sichergestellt ist, dass eine einheitliche Datenschutz-Beratungs- und Prüfpraxis in Bezug insbesondere zu den technischen und organisatorischen Maßnahmen der DS-GVO erreicht werden kann.

Die wesentliche Komponente des SDM besteht aus einem Konzept "elementarer Gewährleistungsziele". Als Gewährleistungsziele - verankert in Art. 5 und 32 DSGVO – gelten

- Sicherung der Verfügbarkeit,
- Integrität,
- Vertraulichkeit,

- Transparenz,
- Belastbarkeit,
- Intervenierbarkeit und
- Nicht-Verkettung von personenbezogenen Verfahren, ergänzt
- um die übergreifende Anforderung der Datenminimierung.

VI. Auftragsverarbeitung (Vertragsmanagement)

Die Vertragsbeziehungen der Stadt Köln mit externen Dienstleistern bei der Verarbeitung personenbezogener Daten werden nach den Regelungen der DSGVO gestaltet (Auftragsverarbeitung nach Art. 28 ff. DSGVO). Gleiches gilt für die Regelungen zur gemeinsamen Verantwortlichkeit (Art. 26 DSGVO).

Zur Einhaltung der Regelungsinhalte der DSGVO sind folgende Prüfschwerpunkte mit standardisierten Formularen etabliert:

- Risikoanalyse mittels eines Datenklassifizierungsbogens
- Abschluss eines Mustervertrages zur Auftragsverarbeitung incl. „Checkliste Datenschutz“ zum Nachweis der technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter/ Auftragnehmer bzw. Vertrag zur Übernahme der gemeinsamen Verantwortlichkeit
- Verarbeitungsverzeichnis nach Art. 30 Abs. 2 DSGVO

VII. Wahrung der Betroffenenrechte

Die Realisierung der nachfolgenden Rechte durch die Betroffenen nach der DSGVO wird durch die Stadtverwaltung Köln als verantwortliche Stelle sichergestellt:

- Recht auf Widerruf einer Einwilligung, Art. 7 Abs. 3
- Recht auf Auskunft, Art. 15
- Recht auf Berichtigung der Daten, Art. 16
- Recht auf Löschung der Daten, Art. 17

- Recht auf Einschränkung der Verarbeitung, Art. 18
- Recht auf Widerspruch, Art. 21

Diese Rechte können nach Art. 23 DSGVO beschränkt werden. Bundes- und Landesgesetzgeber haben von dieser Möglichkeit Gebrauch gemacht.

Sollte die betroffene Person von den oben genannten Rechten Gebrauch machen, prüft die verantwortliche Fachdienststelle, ob die gesetzlichen Voraussetzungen hierfür im Einzelfall erfüllt sind. Die Stadt Köln wird auf Antrag der betroffenen Person tätig. Die Unterrichtung erfolgt unverzüglich, spätestens aber innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 S. 1 DSGVO). Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist (Art. 12 Abs. 3 S. 2 DSGVO).

Die betroffene Person hat zudem das Recht auf Beschwerde bei der/dem behördlichen Datenschutzbeauftragte/n (Art. 38 Abs. 4 DSGVO) und der/dem Landesbeauftragte/n für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Art. 77 Abs. 1 DSGVO), wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen datenschutzrechtliche Bestimmungen verstößt.

Bei der Umsetzung der DSGVO sind alle Fachdienststellen aufgefordert, u.a. auf diese Rechte im Rahmen der erweiterten Informationspflichten nach Art. 13 und 14 hinzuweisen.

VIII. Implementierung von Löschregelungen

Nach der DSGVO und nationalen datenschutzrechtlichen Regelungen ist die verantwortliche Stelle verpflichtet, personenbezogene Daten zu löschen, wenn diese nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungspflichten bestehen. Allgemein gültige Löschregeln und Löschfristen können in diesem Konzept aufgrund der unterschiedlichen Verarbeitungsvorgänge nicht festgelegt werden. Entsprechend hat die verantwortliche Stelle bei jeder Verarbeitung personenbezogener Daten eigenständige Löschkonzepte und Löschroutinen zu erarbeiten und zu implementieren.

Die Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln regelt hierzu, dass die verantwortliche Stelle im ersten Schritt Löschfristen für die jeweiligen Fachdaten sowie ggf. für die Protokolldaten im Verarbeitungsverzeichnis festzulegen hat. Im zweiten Schritt hat die verantwortliche Stelle die Umsetzung der Löschfristen durch das Treffen von geeigneten Maßnahmen und die Verteilung entsprechender Verantwortlichkeiten sicherzustellen. Detaillierte technische Mechanismen des Löschens - beispielsweise Löschen durch Überschreiben von Attributen, Löschen von Datensätzen oder Löschen ganzer Tabellen oder Dateien – sind durch die verantwortliche Stelle selbständig zu bestimmen. Als Alternative zur Löschung können Daten auch unumkehrbar anonymisiert werden.

Die Weiterentwicklung von Geschäftsprozessen, Änderungen der Rechtsvorschriften und die Veränderungen an IT-Systemen können die Anpassung der entsprechenden Löschregelungen erforderlich machen.

IX. Umgang mit Datenschutzverletzungen

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet die verantwortliche Fachdienststelle unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, diese der/dem Landesbeauftragte/n für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Artikel 33 DSGVO), es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Wann die Schwelle zu einer Verletzung des Schutzes personenbezogener Daten überschritten ist, definiert Art. 4 Nr. 12 DSGVO legal. Die Wendung meint (anders als der allg. Sprachgebrauch insinuiert) nicht jeden Verstoß gegen Vorschriften zum Schutz der informationellen Selbstbestimmung. Sie bezeichnet vielmehr ausschließlich eine Verletzung der Sicherheit (engl.: „in case of a personal data breach“).

Als Erscheinungsformen nennt die DSGVO die Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung von bzw. den unbefugten Zugang zu verarbeiteten personenbezogenen Daten.

Die Meldung an den/ die Landesbeauftragte/n für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) enthält folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
- den Namen und die Kontaktdaten des/der Datenschutzbeauftragten,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt die verantwortliche Fachdienststelle die betroffene Person unverzüglich von der Verletzung (Art. 34 Abs. 1 DSGVO).

Die detaillierten Regelungen des Vorgehens ist der Dienstanweisung Datenschutz und Informationsfreiheit der Stadt Köln zu entnehmen.

X. Datenschutzschulungen und Verpflichtung auf das Datengeheimnis

Datenschutzschulungen und die Verpflichtung der Beschäftigten auf das Datengeheimnis sind elementare Bestandteile der organisatorischen Maßnahmen der Stadt Köln zum Schutz der personenbezogenen Daten.

1. Datenschutzschulungen

Die DSGVO geht im Hinblick auf die Rechenschaftspflicht davon aus, dass die Beschäftigten wissen, dass sie die gesetzlichen Bestimmungen zum Datenschutz einhalten müssen (Art. 5 Abs. 2). Dies setzt eine Belehrung voraus. Eine Belehrung ohne entsprechende Sensibilisierung bzw. Schulung ist jedoch fruchtlos, sodass sich daraus ein Schulungsauftrag für die Stadt Köln als Verantwortliche ergibt.

Der/die Datenschutzbeauftragte hat zu überwachen, ob die verantwortliche Stadt Köln ein entsprechendes Schulungskonzept zum Datenschutz etabliert und umgesetzt hat (Art. 39 Abs. 1 lit. b DSGVO).

Um fortan sicherzustellen, dass eine entsprechende Sensibilisierung zum Thema Datenschutz und der IT-Sicherheit flächendeckend und in der notwendigen qualitativen Tiefe erfolgt, ist die Beschaffung einer Online-Schulungssoftware vorgesehen. Dies soll auch gewährleisten, dass im Rahmen der Rechenschaftspflichten nachgewiesen werden kann, dass alle städtischen Beschäftigten ausreichend informiert sind.

Im Rahmen seines Überwachungsauftrages hat der Datenschutzbeauftragte bereits die Initiative zur entsprechenden Umsetzung ergriffen und ist im Gespräch mit den zuständigen Fachdienststellen.

Eine erste Marktsichtung durch den Datenschutzbeauftragten ergibt einen Budgetrahmen i.H.v. ca. 160.000 € für die nächsten vier Jahre für eine entsprechende Online-Anwendung (Anschaffungs-, Support- und laufende Folgekosten). Die Diskussion über die Budgetzuordnung wird derzeit mit verschiedenen Fachdienststellen geführt und die Rahmenbedingungen für die notwendige Ausschreibung ermittelt. Ein Einsatz der Onlinesoftware wird im Laufe des Jahres 2019 anvisiert.

In der Vergangenheit wurden Schulungen zum allgemeinen Datenschutz (2x im Jahr) sowie zum Sozialdatenschutz für neue Kräfte des Allgemeinen Sozialen Dienstes (2x im Jahr) durch den Datenschutzbeauftragen durchgeführt. Diese werden weiterhin bedarfsorientiert angeboten.

2. Verpflichtung auf das Datengeheimnis

Auch wenn eine Verpflichtung der Beschäftigten nach der DSGVO nicht mehr ausdrücklich gefordert wird, soll bei der Stadt Köln die bisher praktizierte Sensibilisierung und schriftliche Verpflichtung auf das Datengeheimnis bei Dienstantritt weiterhin fortgesetzt werden.

Im ersten Schritt erfolgt die formale Verpflichtung bei der Einstellung in den Dienst der Stadt Köln durch das Amt für Personal- und Verwaltungsmanagement (11). Zur Verpflichtung gehört im zweiten Schritt auch eine operative Belehrung über die sich ergebenden datenschutzrechtlichen Pflichten in der jeweiligen Fachdienststelle. Die Beschäftigten sind – möglichst anhand typischer Fälle – im Rahmen der regelmäßigen Einarbeitung darüber zu informieren, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen und welche Rechtsnormen einschlägig sind.

Aus Nachweisgründen im Rahmen der Rechenschaftspflicht ist die formale Verpflichtung auf das Datengeheimnis zu dokumentieren.

XI. Kontrollen und Wirksamkeitsprüfungen

Neben dem Auftrag zur Unterrichtung und Beratung des Verantwortlichen/ der Stadt Köln und der dort Beschäftigten (Art. 39 Abs. 1 lit a DSGVO) obliegt dem/ der Datenschutzbeauftragten die Aufgabe, die Einhaltung der datenschutzrechtlichen Regelungen zu überwachen (Art. 39 Abs. 1 lit. b DSGVO). Hierzu gehört insbesondere die Überwachung der Durchführung von Datenschutzfolgenabschätzungen nach Ziff. V.1. (Art. 39 Abs. 1 lit. c DSGVO) und die regelmäßige Überprüfung, Bewertung und Evaluation der technischen und organisatorischen Maßnahmen zu Ziff. V.3. auf deren Wirksamkeit (Art. 32 Abs. 1 lit. d DSGVO).

Die Kontrollen werden durch prozessabhängige und prozessunabhängige Prüfungen realisiert.

1. Prozessabhängige Prüfungen

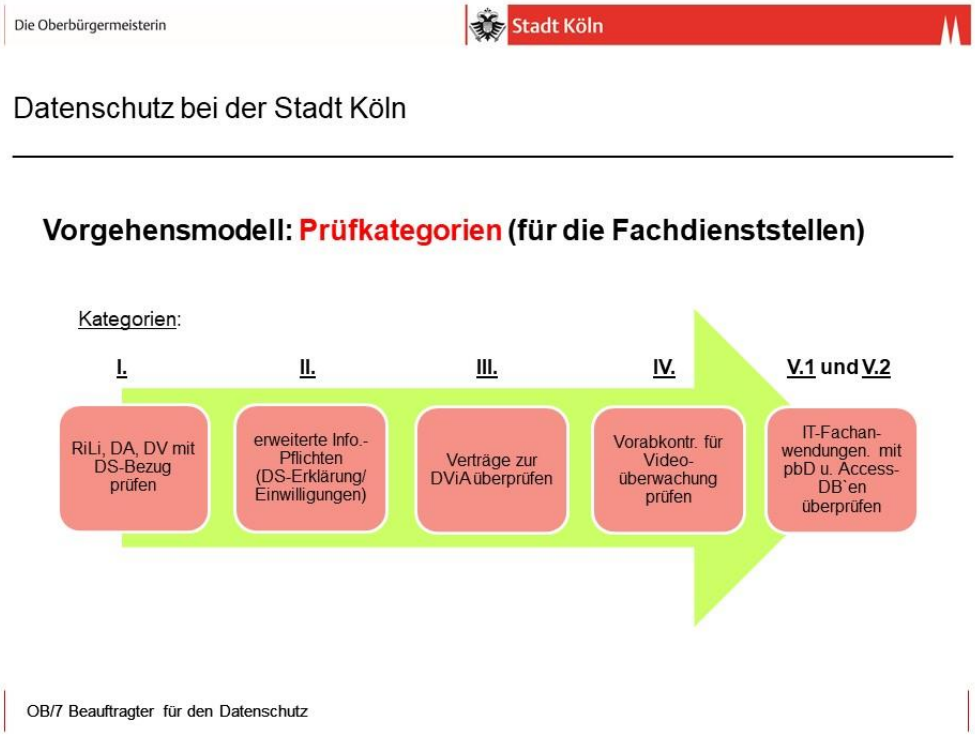
Prozessabhängige Prüfungen stellen alle unter Ziff. V.1. dargestellten datenschutzrechtlichen Zulässigkeitsprozesse dar, bei denen der/die Datenschutzbeauftragte ggf. verpflichtend zu konsultieren ist (s. auch Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln).

Die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Maßnahmen (s. Ziff. V.3.) werden laufend durch die/den Datenschutzbeauftragte/n sowie die/den IT-Sicherheitsverantwortliche/n auf ihre Wirksamkeit in Bezug auf den Stand der Technik überprüft.

2. Prozessunabhängige Prüfungen

Im Wege der prozessunabhängigen Prüfungen führt die/der Datenschutzbeauftragte in regelmäßigen Abständen Stichproben bei den Fachdienststellen durch. Über die Modalitäten, Inhalte und das Verfahren entscheidet der/die Datenschutzbeauftragte. Die Stichproben sind in der Regel angemeldet, werden in einem kooperativen Prozess der Zusammenarbeit durchgeführt und anschließend dokumentiert. Das Ergebnis der Kontrolle wird der Leitung der verantwortlichen Stelle (Leitung der Fachdienststelle) mitgeteilt.

Die operative Umsetzung der prozessunabhängigen Prüfungen ist im Licht der aktuell laufenden Umsetzung der DGSVO zu bewerten. Die systematische Abarbeitung des Vorgehensmodells zur Umsetzung der DSGVO (s. nachfolgendes Schaubild) hat zu einer umfassenden Bestandsaufnahme der wesentlichen datenschutzrelevanten Tatbestände in den Fachdienststellen geführt. Die Abarbeitung offener Zulässigkeitsprüfungen insb. in den Prüfkategorien Auftragsverarbeitung (PK III), Videoüberwachung (PK IV) und IT-Fachanwendungen (PK V.1) erfolgt sukzessive durch die Fachdienststellen bei gleichzeitiger Konsultation der/des Datenschutzbeauftragten. Der insoweit erforderliche Prüfaufwand wird derzeit im Rahmen der Projektgruppe DSGVO gesamtstädtisch erhoben, nach Sensibilität der jeweils verarbeiteten personenbezogenen Daten priorisiert und in Abstimmung mit den Fachdienststellen sowie dem Amt für Informationsverarbeitung (12) – als wesentlich Umsetzungsbeteiligte – einer Zeit-Maßnahmen-Planung zugeführt.



Die sich aus der Bestandsaufnahme ergebenden datenschutzrechtlichen Prüfprozesse werden nach derzeitiger Einschätzung einen zeitlichen Nachlauf von bis zu zwei Jahren für eine abschließende Abwicklung benötigen.

Aus Sicht des Datenschutzbeauftragten sind diese nachzuholenden Prüfaufwände in keiner Weise ein Makel sondern Ausdruck einer ernsthaften Auseinandersetzung der Fachdienststellen mit dem Thema Datenschutz.

Vor dem Hintergrund dieser Bestandsaufnahme – sozusagen eines umfassenden datenschutzrechtlichen „Hausputzes“ – erscheint es aus Sicht des Datenschutzbeauftragten derzeit angemessen, die prozessunabhängigen Prüfungen für die nächsten zwei Jahre nur zurückhaltend durchzuführen.

XII. Zertifizierung

In Art. 42 DSGVO ist die Einführung von datenschutzspezifischen Zertifizierungen geregelt. Das Zertifikat soll bescheinigen, dass datenschutzrechtliche Anforderungen eingehalten werden. Gleichzeitig stellt Art. 42 Abs. 4 klar, dass der/die Verantwortliche trotz der Zertifizierung die ggf. übrigen Anforderungen der DSGVO-Bestimmungen einhalten muss. Zertifikate dürfen nur von den Aufsichtsbehörden oder akkreditierten Zertifizierungsstellen ausgestellt werden (Art. 42 Abs. 5 DSGVO).

Eine Zertifizierung kann damit als Nachweis herangezogen werden, dass bestimmte Anforderungen der DSGVO eingehalten werden. Damit werden Kontrollen, z.B. bei Einsatz von Dienstleistern oder durch den/ die Landesbeauftragte/n für Datenschutz und Informationsfreiheit Nordrhein-Westfalen erleichtert.

Wie die Zertifizierung aussehen wird, ist noch nicht konkretisiert. Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DSGVO ermöglicht wird.

Im Rahmen der laufenden Zertifizierungsbestrebungen des Amts für Informationsverarbeitung (12) mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist in einem ersten Schritt vorgesehen, das vorhandene Datenschutzmodul für den Bereich OB/7 zu durchlaufen.

XIII. Inkrafttreten

Das Datenschutzmanagementkonzept tritt mit Wirkung vom 11.12.18 in Kraft.

Köln, den 11.12.18

Die Oberbürgermeisterin

Dokumenten-/ Versionshistorie

Datum	Version	Änderung/ Status*	gefertigt von
15.11.18	1.0	Entwurf	OB/7
11.12.18	1.1	Beschlussfassung im VV am 11.12.18	OB/7
18.12.19	1.1	Qualitätsüberprüfung (kein substantieller Anpassungsbedarf)	30/1 (bDSB)
14.12.20	1.1	Qualitätsüberprüfung (kein substantieller Anpassungsbedarf)	30/1 (bDSB)
15.12.21	1.1	Qualitätsüberprüfung (kein substantieller Anpassungsbedarf)	I/1
20.12.22	1.1	Qualitätsüberprüfung (kein substantieller Anpassungsbedarf)	I/1

* Entwurf, Ersterstellung, Fortschreibung, regelmäßige Qualitätssicherung

Elementare Bestandteile des Datenschutzmanagementkonzeptes

Die vorstehenden Ausführungen zur Erfüllung der Dokumentations- und Rechenschaftspflichten werden ergänzt um folgende eigenständige Bausteine:

1. Datenschutz

- Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln
- Fortschreibungsfähiger Maßnahmenüberblick zur Umsetzung der Vorgaben aus dem Datenschutzmanagementkonzept der Stadt Köln
- Prozessbeschreibungen und Formulare der datenschutzrechtlichen und IT-sicherheitstechnischen Zulässigkeitsprozesse für Verarbeitungstätigkeiten, insbesondere Datenschutzfolgenabschätzungen (s. Ziff. V.)
- Listen der verfahrensspezifischen Verarbeitungsverzeichnisse
- Informationen zum Datenschutz im Intranet- und Internet-Auftritt der Stadt Köln
- Nachweis der Schulungsdokumentationen für Datenschutz und IT-Sicherheit (Reporting)
- Vertraulichkeitsvereinbarungen auf das Datengeheimnis (bei 11)

2. IT-Sicherheit

- Dienstanweisung zur Nutzung und zum Betrieb der IV-Infrastruktur
- IT-Sicherheitshandbuch
- Richtlinie zur Behandlung von Sicherheitsvorfällen
- Dienstanweisung Betrieb für Geräte der Informations- und Telekommunikationstechnik (IuK)
- Dienstanweisungen Mail und Internet
- Richtlinie für die Bedarfsprüfung bei Hard- und Softwarebeschaffungen sowie die Verwertung von nicht mehr benötigter Software

3. Allgemeine städtische Regelungen

- Handbuch der Stadtverwaltung Köln (Leitfaden für den dienstlichen Alltag)