Stadt Köln

Die Oberbürgermeisterin

Dezernat, Dienststelle
OB/01/01

Vorlagen-Nummer 07.05.2019
1555/2019

Mitteilung

öffentlicher Teil

Gremium	Datum
Unterausschuss Digitale Kommunikation und Organisation	17.06.2019

Strukturierte Qualitätsstanderhebung zum Datenschutz bei der Stadt Köln sowie Sachstandsdarstellung zur Umsetzung der Datenschutzgrundverordnung (DSGVO) ein Jahr nach Inkrafttreten

Auf der Grundlage des vom Verwaltungsvorstand am 11.12.18 beschlossenen Datenschutzmanagementkonzeptes zur Erfüllung der Rechenschafts- und Dokumentationspflichten nach der DSGVO (s. Mitteilung im UdiKO zu Session 0101/2019) wurden Maßnahmenkriterien hergeleitet, die geeignet sind, den Qualitätsstand zum Datenschutz sowie zur Umsetzung der DSGVO in einer Kommunalverwaltung in strukturierter Art und Weise zu erheben und systematisch zu bewerten (s. Ziff. I).

Zeitgleich wird ein Jahr nach Inkrafttreten der DSGVO der Stand der Umsetzung bei der Stadt Köln dargestellt (s. Ziff. II.).

I. Strukturierte Qualitätsstanderhebung zum Datenschutz bei der Stadt Köln

Im Rahmen des Inkrafttretens der EU-Datenschutzgrundverordnung (DSGVO) zum 25.05.18 sind umfassende Rechenschafts- und Dokumentationspflichten zum Nachweis der Einhaltung der datenschutzrechtlichen Vorgaben zu erfüllen (s. Art. 5 Abs. 2 und 24 Abs. 1 DSGVO). Der Verwaltungsvorstand hat sich mit seinem Beschluss vom 11.12.18 als erste große Kommunalverwaltung, landes- bzw. bundesweit auf die vorgeschriebenen Regelungen nach dem europäischen Datenschutzrecht umfassend und mit Gültigkeit für alle Organisationseinheiten und Beschäftigten der Stadtverwaltung Köln verpflichtet (s. Session 3767/2018).

Auf der Grundlage dieses Datenschutzmanagementkonzeptes als stadtintern gerichtetes Instrument der Selbstbindung zur Gewährleistung von Datenschutz und IT-Sicherheit wurden insgesamt 15 Maßnahmen hergeleitet, die geeignet sind, den Qualitätsstand zum Datenschutz sowie zur Umsetzung der DSGVO in einer Kommunalverwaltung in strukturierter Art und Weise zu erheben und systematisch zu bewerten. Aus den Ergebnissen der Bewertung lassen sich offene datenschutzrechtliche Handlungsbedarfe ableiten.

Folgende 15 Einzelmaßnahmen wurden für die Qualitätsstandserhebung herangezogen:

Datenschutzmanagementkonzept zur Erfüllung der Rechenschaftspflichten	Prüfung der Maßnahmen bei Auftragsverarbeitung (Vertragsmanagement)
Verantwortlichkeiten im Datenschutz	Datenübermittlung an andere öffentliche und nicht-öffentliche Stellen
Beachtung des Prinzips der Datenminimierung (insb. Erforderlichkeit)	Umsetzung der Informationspflichten nach Art. 13, 14 DSGVO (Datenschutz- und Einwilligungserklärungen)
datenschutzrechtliche und IT-sicherheitstechnische Zulässigkeitsverfahren	Erhebung von Daten für festgelegte, eindeutige und legitime Zwecke (Zweckbindung)
technisch-organisatorische Maßnahmen im Fachamt entsprechend dem Stand der Technik	Erfüllung der Dokumentationspflichten (insb. Verarbeitungsverzeichnisse)
Verpflichtung der Beschäftigten auf den Datenschutz und Schulungsmaßnahmen	Aufrechterhaltung des Datenschutzes im laufenden Betrieb (Datenschutzkontrolle)
Sicherstellung der Rechte der Betroffenen	Umsetzung der Löschfristen (Speicherbegrenzung)
Sicherstellung der Meldepflichten bei Datenschutzverletzungen	

Die mit den Bewertungsmaßnahmen verbundenen operativen Fragestellungen entnehmen Sie bitte der **Anlage 1**.

Die 15 einzelnen Maßnahmen sind in einem ersten Schritt im Rahmen eines Treffens zum europäischen Datenschutztag am 28.01.19 von den dezentralen Datenschutzkoordinatoren/innen der Fachdienststellen mit der Fragestellung „Wie erleben Sie in Ihrer Funktion als dezentrale Datenschutzkoordinatoren/innen die Umsetzung vor Ort?“ und „Sind die Maßnahmen bekannt und werden beachtet?“ bewertet worden (hier nach Erfüllungsgrad der Einzelmaßnahmen von 0 bis 100%; s. Folie 7 der **Anlage 2**). Das Ergebnis entnehmen Sie bitte der Folie 8 der **Anlage 2**.

In einem zweiten Schritt, mit etwas veränderter Fragestellung ist die Bewertung der Maßnahmen aus Sicht des Datenschutzbeauftragten vorgenommen worden: „Sind die Maßnahmen geregelt (etabliert) und für alle Verantwortlichen bekannt?“ (Ergebnis s. Folie 10 der **Anlage 2**).

Zwischenfazit:

Die Auswertungen in den Übersichten zeigen, dass sowohl aus Sicht der dezentralen Datenschutzkoordinatoren/innen als auch des Datenschutzbeauftragten die Maßnahmen zum Datenschutz qualitativ weitgehend über dem definierten Soll-Minimum (= 80% Erfüllungsgrad) liegen.

Handlungsbedarfe:

Aus den Ergebnissen beider Bewertungen ergeben sich konkrete Handlungsanleitungen, nämlich bei den Einzelmaßnahmen, die im Erfüllungsgrad unterhalb des Soll-Minimums von 80% liegen (s. Folien 11 bis 13 der **Anlage 2**). Hierbei ist eine Übereinstimmung der Einschätzungen der dezentralen Datenschutzkoordinatoren/innen und des Datenschutzbeauftragten für zwei Maßnahmen festzustellen (s. nachfolgende lfd. Nr. 1 und 2).

Handlungsbedarf ergibt sich demnach bei folgenden datenschutzrechtlichen Bewertungsmaßnahmen:

1. Sicherstellung der Meldepflichten bei Datenschutzverletzungen (70%)

   Grundlage für die Umsetzung der Meldepflicht von Datenschutzverletzungen gegenüber der Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI NRW) ist die „Dienstanweisung Datenschutz und Informationsfreiheit für die Stadt Köln i.d.F. v. 11.12.18“ (s. dort § 16). Aufgrund des erkannten Handlungsbedarfes sind hierzu allgemeine Informationen (s. hier) und konkrete Handlungsanweisungen im Intranet seitens des Datenschutzbeauftragten veröffentlicht worden (s. hier). Zur operativen Abwicklung ist ein verbindlich zu verwendendes Standardmeldeformular mit gezielten Fragestellungen zu einer ggf. vorliegenden datenschutzrechtlichen Verletzung bereitgestellt.

2. Verpflichtung der Beschäftigten auf den Datenschutz und Schulungsmaßnahmen (75%)

   Gemeinsam mit dem Amt für Personal und Verwaltungsmanagement ist seitens des Datenschutzbeauftragten vorgesehen, dass jede/r Beschäftigte einmal im Jahr verbindlich einen Online-Schulungskurs zum Datenschutz und IT-Sicherheit absolviert, um die entsprechende Sensibilisierung zu gewährleisten und Sicherheitsrisiken zu minimieren (Sachstand: Ausschreibung erfolgt im Laufe 2019).

3. Datenschutzmanagementkonzept zur Erfüllung der Rechenschaftspflichten (75%)

   Der Datenschutzbeauftragte hat die Informationen dazu im Intranet für alle Beschäftigten veröffentlicht (s. hier) und das Datenschutzkonzept in seinem Intranet-Auftritt zur Verfügung gestellt (s. hier).

   Weitere regelmäßige Informationsmaßnahmen werden als notwendig erkannt und seitens des Datenschutzbeauftragten durchgeführt.

4. Erfüllung der Dokumentationspflichten, insb. Verarbeitungsverzeichnisse (75%)

   Für alle datenschutzrechtlichen Maßnahmen stehen Verarbeitungsverzeichnisse zur Erfüllung der Dokumentationspflichten zur Verfügung: s. hierzu Ausführungen im Datenschutzmanagementkonzept (Ziff. V.), in der Dienstanweisung Datenschutz und Informationsfreiheit (§ 19 und 23) sowie im unter Ziff. 3. bereits genannten Intranet-Auftritt des Datenschutzbeauftragten.

   Weitere regelmäßige Informationsmaßnahmen werden als notwendig erkannt und seitens des Datenschutzbeauftragten durchgeführt.

5. Beachtung des Prinzips der Datenminimierung; insb. Erforderlichkeit (75%)

   Seitens des Datenschutzbeauftragten wird zu verschiedenen Verarbeitungsvorgängen festgestellt, dass insb. in der Vergangenheit teilweise mehr Daten als erforderlich im Rahmen der Aufgabenwahrnehmung durch die Fachdienststellen erhoben werden. Hier ist jede Dienststelle aufgefordert, Anträge, Formulare oder sonstige Dokumente zu überprüfen/ zu überarbeiten und die Verarbeitung personenbezogener Daten auf das für die Aufgabe notwendige Maß zu beschränken. Hierauf wirkt der Datenschutzbeauftragte in laufenden Beratungen der Fachdienststellen sowie im Rahmen der verbindlichen Beteiligung an den datenschutzrechtlichen Zulässigkeitsprozessen (Datenschutzfolgenabschätzungen) ein.

Gesamtfazit zur Qualitätsstandserhebung:

Insgesamt ist festzustellen, dass anhand der aus dem Datenschutzmanagementkonzept abgeleiteten 15 Einzelmaßnahmen der Datenschutz bei der Stadt derzeit einem positiv hohen Qualitätsstand entspricht.

Insbesondere die im Zuge der DSGVO-Umsetzung zu treffenden Regelungen wie die Sicherstellung der Rechte der Betroffenen, die Umsetzung der Informationspflichten oder auch die Sicherstellung der Meldepflichten an die Landesdatenschutzbeauftragte (LDI NRW) sind über dem Soll-Minimum von 80% Erfüllungsgrad bewertet bzw. sind bereits konkrete Verbesserungsmaßnahmen im Rahmen des erkannten Handlungsbedarfes getroffen worden (s. laufende Nr. 1.).

An den weiteren datenschutzrechtlichen Maßnahmen mit Handlungsbedarf (Soll-Minimum unter 80% Erfüllungsgrad) wird wie oben dargestellt (s. laufenden Nr. 2. bis 5.) mit dem Ziel der weiteren Verbesserung konkret und fortlaufend gearbeitet.

Nicht auszuschließen ist unabhängig davon, dass es trotz dieser weitgehend guten Bewertungsergebnisse nicht (mehr) zu Datenschutzverletzungen oder -pannen kommen wird. Die aufgebauten personellen Strukturen – insb. mit dem behördlichen Datenschutzbeauftragten und seinem Stellvertreter, den dezentralen Datenschutzkoordinatoren in den Fachdienststellen und dem IT-Sicherheitsverantwortlichen – und die im Verwaltungsvorstand beschlossenen verbindlichen Regeln zum Umgang mit dem Datenschutz bei der Stadt Köln (s. Datenschutzmanagementkonzept und Dienstanweisung Datenschutz und Informationsfreiheit) bilden die unabdingbare Grundlage für ein gesichertes Handeln im Zusammenhang mit dem Datenschutz. Am Ende ist das Verwaltungshandeln überall dort, wo keine vollständige Automatisierung erfolgt, getragen von Menschen. Hier kann und wird es aller Erfahrung nach auch in Zukunft zu individuellem Fehlverhalten in allen Ausprägungen, sei es fahrlässiger Natur bis Vorsatz kommen.

Durch fortlaufende Sensibilisierung aller Beschäftigten, die permanente Beratung der Kolleginnen und Kollegen und der Fachdienststellen, der Überwachung durch das Team des Datenschutzbeauftragten sowie regelmäßige Schulungen in Sachen Datenschutz und IT-Sicherheit kann das v.b. Fehlerrisiko verringert, allerdings nie auf null reduziert werden.

Sowohl in NRW als auch auf Bundesebene wird die vorliegende Form systematischer Bewertung der Qualität des Datenschutzes bei einer großen Kommunalbehörde erstmals angewandt und kann insoweit wegweisend einerseits für die vergleichende Eigenbewertung innerhalb der kommunalen Familie, als auch als Grundlage für die Beratungs- und Überwachungsarbeit der Landesdatenschutzbeauftragten dienen.

Ein wesentliches Erfolgsmerkmal für dieses positive Qualitätsergebnis war auch die dauerhafte Ausweisung einer Stelle für den stellvertretenden Datenschutzbeauftragten im Amt der Oberbürgermeisterin, die seit April 2018 erfolgreich besetzt werden konnte.

II. Sachstandsdarstellung zur Umsetzung der Datenschutzgrundverordnung (DSGVO) ein Jahr nach Inkrafttreten

Seit Beginn des Transformationsprozesses hat die interdisziplinäre Projektgruppe zur DSGVO-Umsetzung nach ihrer konstituierenden Sitzung im März 2017 bisher in 11. Sitzungen getagt. Die regelmäßigen Treffen haben gezeigt, dass die Idee, die Fachdienststellen so eindeutig in die Umsetzungsverantwortung zu nehmen, funktioniert hat. Die jeweiligen Vertreter/innen der Fachdezernate in der Projektgruppe tragen den Prozess sehr positiv mit, übermitteln beschlossene Umsetzungsaufträge in die Fachdienststellen ihres Dezernatsgeschäftsbereiches und spiegeln diese mit entsprechenden Ergebnissen oder Hinweisen auf Umsetzungshemmnisse zurück in die Projektgruppe.

Ebenso wichtig war und ist die Beteiligung verschiedener Querschnittsfunktionen in der Projektgruppe wie des Amtes für Informationsverarbeitung und des IT-Sicherheitsverant-wortlichen, des Amtes für Personal und Verwaltungsmanagement, der Onlineredaktion im Amt für Presse- und Öffentlichkeitsarbeit und der Stabstelle Digitalisierung sowie die frühzeitige vertrauensvolle Einbindung des Gesamtpersonalrates.

Mit steigender Tendenz ist in der Webanwendung DSGVO, die als strukturiertes Dokumentationsinstrument des Kölner Vorgehensmodells zur DSGVO-Umsetzung dient, die Anzahl der Eintragungen umzusetzender Einzelmaßnahmen zu verzeichnen (1.270 zum Stand 21.03.19; s. Folie 2 der **Anlage 3**). Die Verteilung dieser Maßnahmen auf die Prüfkategorien (PK) des Kölner Vorgehensmodells ergibt eindeutige Schwerpunkte bei den Datenschutz-/ und Einwilligungserklärungen (PK II – erweiterte Informationspflichten) sowie IT-Fachanwendungen (PK V.1). Die Angabe von Fehlanzeigen war in diesem Zusammenhang eine wichtige Prüfaussage, da eine Fachdienststelle hiermit dokumentieren konnte, keine Maßnahmen einer bestimmten Prüfkategorie in ihrem Aufgabengebiet verzeichnet zu haben (s. Folie 3 der **Anlage 3**).

Die Kennzahl zu Fachdienststellen, die keine Eintragung in die Webanwendung DSGVO vorgenommen und sich damit bisher nicht nachvollziehbar an dem Umsetzungsprozess beteiligt haben, hat sich nunmehr fast auf null reduziert (s. Folie 2 der **Anlage 3**).

Insgesamt ist festzustellen, dass noch rd. 400 Einzelmaßnahmen zur Umsetzung auf die DSGVO-Regelungen anstehen, da diese mit dem Status „Prüfung offen“ in der Webanwendung DSGVO verzeichnet sind (s. Folie 4 der **Anlage 3**). Wesentliche Teilmenge dieser Gesamtzahl bilden Maßnahmen aus den Prüfkategorien Auftragsverarbeitung (PK III), Videoüberwachung (PK IV) und IT-Fachanwendungen (PK V.1). Da für diese Prüfkategorien datenschutzrechtlich relevante Zulässigkeitsverfahren durchzuführen sind, werden diese Maßnahmen derzeit in einer sog. „Arbeitsplanung“ zusammengeführt, um mit Blick auf die erforderlichen Umsetzungsressourcen in den zuständigen Fachdienststellen und bei den wesentlich Beteiligten 12 (Inbetriebnahmekoordination), 12/1 (IT-Sicherheits-verantwortlicher) und 01/01 (Datenschutzbeauftragter) eine Zeit-Maßnahmen-Planung mit prioritärer Abwicklung aufstellen zu können.

Festzuhalten ist, dass die in diesem Zusammenhang noch durchzuführenden datenschutzrechtlichen Zulässigkeitsverfahren (wesentlich Datenschutzfolgenabschätzungen) einen Umsetzungshorizont von voraussichtlich 2 bis 3 Jahren aufweisen.

Dies ist aus hiesiger Sicht insoweit unproblematisch, da sich der nachlaufende Prüfbedarf aus einer – vergleichbar einem „datenschutzrechtlichen Hausputz“ – durchgeführten Bestandsaufnahme im Rahmen des DSGVO-Umsetzungsprozesses ergeben hat und jetzt in einem strukturierten und nachvollziehbaren Verfahren abgearbeitet wird. Von hier wird nicht davon ausgegangen, dass es in diesem Zusammenhang zu Beanstandungen seitens der Landesdatenschutzbeauftragten (LDI NRW) kommen wird.

Fazit zur DSGVO-Umsetzung:

Der Transformationsprozess hat sich im Wesentlichen wie geplant stabil entwickelt. Das Vorgehensmodell zur operativen Umsetzung der DSGVO hat alle relevanten Inhaltsaspekte des Umstellungsprozesses umfasst und war praxisorientiert durch die verantwortlichen Fachdienststellen anwend- und umsetzbar (s. Mitteilung im UdiKO zu Session 3137/2017).

Die als Dokumentations- und Controllingsinstrument vom Amt für Informationsverarbeitung eigenentwickelte Webanwendung DSGVO hat sich für die zuständigen Beschäftigten in den Fachdienststellen nach entsprechenden Einweisungsschulungen als intuitiv nutzbar herausgestellt. Die Auswertungsfunktionen in der Anwendung sind eine sinnvolle und zielorientierte Unterstützung für das Umsetzungscontrolling sowohl der Dezernate und Fachdienststellen, als auch des Datenschutzbeauftragten.

Die weitere Umsetzung der DSGVO-Regelungen wird wie geplant fortgesetzt. Das Fortbestehen der interdisziplinären Projektgruppe DSGVO ist bis auf weiteres erforderlich.

Gez. Reker