

Tätigkeitsbericht der behördlichen Datenschutzbeauftragten 2019/2020

Datenschutzreform 2018 – Teil 3

Darstellung der positiven Effekte durch Stellenzuschaltungen sowie der negativen Effekte durch Unterschreitung des ermittelten Stellenmehrbedarfs

Sitzungsvorlage Nr. 20-26 / V 02635

6 Anlagen

**Bekanntgabe in der Sitzung des Verwaltungs- und Personalausschusses
vom 17.03.2021**
Öffentliche Sitzung

I. Vortrag des Referenten

Teil A - Tätigkeitsbericht der behördlichen Datenschutzbeauftragten 2019/2020

Bis 2016 hat der behördliche Datenschutzbeauftragte den Stadtrat alle zwei Jahre im Rahmen einer Bekanntgabe über seine Tätigkeiten informiert.

Die Jahre 2017/2018 waren geprägt von intensiver, stadtweiter Projektarbeit zur Umsetzung der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; im Folgenden: DSGVO). Dazu wurden zwei Beschlussvorlagen in den Stadtrat eingebracht (vgl. Stadtratsbeschluss vom 23.11.2017, Nr. 14-20 / V 10080: „Datenschutzreform 2018 – Umsetzung der europäischen Datenschutz-Grundverordnung (DSGVO), Bericht und Finanzierungsvorschlag“; Stadtratsbeschluss vom 24.10.2018, Nr. 14-20 / V 12422: „Datenschutzreform 2018 – Teil 2, IT-Vorhaben Datenschutz – Bericht zum Umsetzungsstand der DSGVO – Personalbedarf“).

Zu den Jahren 2019/2020 kann Folgendes berichtet werden:

1. Organisation und Management des Datenschutzes bei der LHM

1.1. Neue Organisationseinheit behördlicher Datenschutz

Seit 2019 bildet die behördliche Datenschutzbeauftragte eine eigene Organisationseinheit im Direktorium. Ergänzend dazu sind – wie gehabt – örtliche Datenschutzbeauftragte in den Referaten benannt. Die Eigenbetriebe haben formal eigenständige Datenschutzbeauftragte, die jedoch eng mit den Datenschutzbeauftragten der LHM kooperieren. Die Organisationsstruktur ist in der neu gefassten Datenschutz-Geschäftsweisung geregelt, wie auch die Zuständigkeiten und Verantwortlichkeiten hinsichtlich des Datenschutzes in der Verwaltung. Die Datenschutzvorschriften müssen, wie andere Gesetze auch, von der Verwaltung eingehalten und vollzogen werden. Die Landeshauptstadt München ist als öffentliche Stelle datenschutzrechtlich verantwortlich. Die Datenschutzbeauftragten haben innerhalb der Verwaltung eine Beratungs- und Überwachungsfunktion, verfügen jedoch über keine Entscheidungs- oder Weisungsrechte.

1.2. Vernetzung mit der IT

Seit Februar 2020 wird die neue Organisationseinheit durch eine technisch-organisatorische Fachkraft für den Datenschutz verstärkt. Dies bildet eine wertvolle Ergänzung zu der vorhandenen juristischen Expertise und stellt eine weitere Brücke zu den Kolleg*innen der IT, insbesondere zur IT-Sicherheit dar. Es findet ein intensiver und fruchtbarer Austausch zwischen den Datenschutzbeauftragten und der IT-Sicherheit statt, durch gegenseitige Einbindung in die jeweiligen Gremien (Treffen örtliche Datenschutzbeauftragte, ISM-Board, ISB-Forum), durch Jour Fixe auf Referatsebene und durch konkrete fachliche Zusammenarbeit.

Mit der zunehmenden Digitalisierung und wegen der it- und risikoorientierten Ausrichtung der DSGVO ist effektiver Datenschutz ohne Schulterschluss mit der IT gar nicht mehr denkbar. Dies zeigt sich gerade jetzt, in Zeiten von Corona, durch den verstärkten Einsatz digitaler Arbeitsmittel und -formen bei der Landeshauptstadt, z.B. vermehrtes Arbeiten in Homeoffice oder Nutzung des Konferenztools Cisco Webex. Diese Entwicklung wird von der behördlichen Datenschutzbeauftragten ausdrücklich unterstützt, da sie nicht nur in Krisenzeiten Kontinuität bei der Aufgabenerfüllung der LHM sichert, sondern flexiblere Arbeitsformen für die Beschäftigten möglich macht. Die Mitarbeiter*innen des Behördlichen Datenschutzes beraten die Verwaltung dabei, die digitalen Möglichkeiten datenschutzkonform einzusetzen.

1.3. Datenschutz-Management-Tool Risk2Value (R2V)

Gemäß Stadtratsbeschluss vom 24.10.2018 sollte eine IT-Unterstützung für das Datenschutz-Management und die Datenschutz-Prozesse zur Verfügung gestellt werden. Im Rahmen des IT-DSGVO-Projekts ergab sich die Möglichkeit, das Risikomanagement-Tool Risk2Value (R2V) zusätzlich für das Datenschutzmanagement einzusetzen. R2V soll langfristig die wichtigsten Datenschutz-Prozesse abbilden und die damit verbundenen stadtweiten Arbeitsabläufe erleichtern. Gleichzeitig sollen Synergieeffekte mit den Bereichen der IT-Sicherheit sowie des IT-Risikomanagements erzielt werden, für die das Tool ebenfalls eingesetzt wird.

2. Inhaltliches

2.1. EuGH-Urteil „Schrems II“ – EU-US-Privacy Shield ungültig

Im Rahmen von Dienstleistungsverhältnissen kann es seitens der LHM zu Datenübermittlungen in die USA kommen. Viele dieser Datenübermittlungen fanden bislang im Rahmen des sog. EU-US-Privacy-Shields statt, einem Beschluss der EU-Kommission, der für die in die USA übermittelten Daten ein der DSGVO angemessenes Schutzniveau feststellte.

Der EuGH hat das EU-US-Privacy-Shield in seinem Urteil vom 16. Juli 2020 (Schrems II; Rechtssache C 311/18) mit sofortiger Wirkung für nichtig erklärt. Dies bedeutet, dass Datenübermittlungen in die USA, die ausschließlich auf Grundlage des Privacy-Shields vorgenommen werden, nicht mehr rechtmäßig sind. Für die betreffenden Vertragsverhältnisse müssen nun Alternativlösungen gefunden werden.

Die bisherige Sondierung der Vertragsverhältnisse der LHM mit US-amerikanischen Anbieter*innen hat ergeben, dass keines davon ausschließlich auf dem Privacy-Shield basiert. In der Regel sind zusätzlich sogenannte Standardvertragsklauseln abgeschlossen worden. Dennoch genügen diese Klauseln nicht in jedem Fall den Anforderungen der DSGVO. Die Verträge müssen im Einzelnen geprüft und ggf. ein angemessenes Datenschutzniveau mit zusätzlichen, etwa technischen Vorgaben sichergestellt werden.

Bei den bisher eingeleiteten bzw. laufenden Verhandlungen mit den jeweiligen Anbietern sind die Mitarbeiter*innen des Behördlichen Datenschutzes, sowie die betreffenden örtlichen Datenschutzbeauftragten und das Team des Datenschutzbeauftragten von it@M beratend beteiligt. Allerdings ist eine umfassende datenschutzrechtliche Beratung bei der Prüfung sämtlicher Verträge der LHM mit Anbieter*innen aus Drittstaaten inklusive der Einhaltung eines angemessenen Datenschutzniveaus mangels ausreichender personeller Ausstattung der behördlichen und der örtlichen Datenschutzbeauftragten im juristischen Bereich derzeit nicht leistbar.

2.2. Datenschutz und Corona

Auf den coronabedingt für Bayern ausgerufenen Katastrophenfall hat der Bayerische Landesbeauftragte für den Datenschutz (LfD) mit Sonderinformationen zur datenschutzrechtlichen Zulässigkeit von Ausnahmelösungen reagiert, die für diese Zeit im Rahmen der Beratungstätigkeit als datenschutzrechtlichen Maßstab zu Grunde gelegt wurden. So waren insbesondere möglich:

- Nutzung privater Mailadressen zu dienstlichen Zwecken
- Kurzfristige Ertüchtigung des Konferenztools von Cisco Webex für den stadtweiten Einsatz
- Nutzung von Microsoft Teams Education an Schulen
- Erhebung von privaten Kontaktdaten städtischer Beschäftigter für die Erreichbarkeit im Krisenfall.

Möglichst viele dieser Lösungen sollen langfristig nutzbar bleiben. Für den „Normalbetrieb“ werden die datenschutzrechtlichen, aber auch die IT-Sicherheitsanforderungen sicher höher sein. Daher hat die behördliche Datenschutzbeauftragte in Zusammenarbeit mit den Kolleg*innen von der IT-Sicherheit einen Prozess angestoßen mit dem Ziel, datenschutz- und it-sicherheitskonforme digitale Arbeitsmöglichkeiten für die Zukunft aufzuzeigen, die technisch realisierbar sind. Darunter fallen u.a. die Optimierung der technischen Voraussetzungen für das Homeoffice, die Implementierung eines Instant-Messengers, sowie Anpassungen im Bereich 2-Faktor-Authentifizierung. Hierzu steht die behördliche Datenschutzbeauftragte in engem Austausch mit dem IT-Referat.

2.3. Microsoft Teams an Schulen

Das Referat für Bildung und Sport hat die LHM-Services GmbH (LHM-S), eine Tochter der Stadtwerke, mit der IT-Ausstattung der Schulen beauftragt. Die LHM-S setzt derzeit für die Ermöglichung des Distanzunterrichts während der Corona-Pandemie Microsoft Teams ein. Hierzu wird den Schulen von der LHM-S eine datenschutzrechtliche Mustereinwilligungserklärung für die Erziehungsberechtigten bzw. ab dem 14. Geburtstag zusätzlich für die jeweiligen Schülerinnen und Schüler zur Nutzung von MS-Teams zur Verfügung gestellt. Die Nutzung von MS-Teams erfolgt auf freiwilliger Basis.

Diese Lösung wird vom Bayerischen Staatsministerium für Unterricht und Kultus auch für die staatlichen Schulen empfohlen. Die datenschutzrechtliche Einordnung sowie die Sondierung von Alternativlösungen wird von der LHM-S durchgeführt, die als Auftragnehmerin eine eigene bestellte Datenschutzbeauftragte hat. Datenschutzrechtlich verantwortlich bleibt jedoch das Referat für Bildung und Sport bzw. die LHM für die durch die LHM-S eingesetzte IT und die damit verbundene Datenverarbeitung.

2.4. Personalaktendaten in der Cloud

Zum 01.01.2019 wurde das Bayerische Beamtengesetz u.a. dahingehend geändert, dass Personalaktendaten nur unter engen Voraussetzungen von externen Auftragnehmer*innen verarbeitet werden dürfen (Art. 108 Abs. 3 BayBG). Auftragnehmer*innen können auch Cloud-Anbieter*innen sein.

Die Personalverwaltung wird zunehmend digitalisiert. Zur Datenverarbeitung wird teilweise auf den Service externer Dienstleister*innen zurückgegriffen. Daher war eine Klärung der Frage unerlässlich, in welchen Fällen die Vorschrift anzuwenden ist und welche Grenzen sie insbesondere bei der Verarbeitung von Personalaktendaten in Clouds zieht.

Dazu stand das Personal- und Organisationsreferat mit dem Bayerischen Staatsministerium der Finanzen in Kontakt. Im Mai 2019 hat sich das Ministerium schriftlich zur Auslegung von Art. 108 Abs. 3 BayBG geäußert. Auf dieser Grundlage wird nun eine datenschutzrechtliche Beratung für Digitalisierungsvorhaben im Personal- und Organisationsreferat vorgenommen.

2.5. neoHR

In dem Programm neoHR wird in mehreren Projekten (Digitale Zeiterfassung, Talentmanagement Suite, Digitale Personalakte, Beihilfe-App, Enable-Now, HR-Reporting) intensiv an innovativen Personalmanagementlösungen und der weiteren Digitalisierung der Personalverwaltung gearbeitet.

Hierbei beraten und unterstützen die Datenschutzbeauftragten des POR, von it@M sowie der behördliche Datenschutz die einzelnen Projekte aus datenschutzrechtlicher Sicht. In enger Abstimmung mit den Projektleiter*innen werden dabei die neuen digitalen Personalprozesse in Konzeption, Entwicklung und Einführung datenschutzrechtlich begleitet. Gerade die Verwendung neuer Technologien bedingt eine intensive datenschutzrechtliche Prüfung und stellt Projektleiter*innen, Teammitglieder, Datenschutzbeauftragte sowie sämtliche Stakeholder im Prozess vor neue und spannende Herausforderungen.

2.6. Online-Zugangsgesetz (OZG)

Die Umsetzung des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) birgt eine Reihe an datenschutzrechtlichen Anforderungen, etwa wie die elektronische Kommunikation mit Bürger*innen DSGVO-konform ablaufen kann. Das Vorhaben wird datenschutzrechtlich vom örtlichen Datenschutz des IT-Referats unter Beteiligung der behördlichen Datenschutzbeauftragten begleitet.

2.7. Städtisches Akkreditierungsverfahren UEFA EURO 2020

Gemäß dem integrierten städtischen Sicherheitskonzept ist für bestimmte Personen, die im Rahmen der UEFA EURO 2020 eingesetzt werden, ein Akkreditierungsverfahren inklusive polizeilicher Zuverlässigkeitsüberprüfung geplant. Dies betrifft insbesondere Mitarbeitende privater Dienstleister*innen (Sicherheitsdienste, Reinigungspersonal, Imbissverkauf usw.). Für die erforderliche Datenverarbeitung, insbesondere den Datenaustausch mit der Polizei und dem Bayerischen Landeskriminalamt fehlt, obwohl seit Jahren von vielen Bundes- und Landesdatenschutzbeauftragten angemahnt, eine bereichsspezifische gesetzliche Grundlage. Bisher wurde diese durch eine informierte Einwilligung der Betroffenen ersetzt. Dies wird jedoch vom BayLfD kritisiert. Adressat der Kritik des BayLfD ist in erster Linie das Bayerische Staatsministerium des Innern, für Sport und Integration sowie die Polizei. Leidtragend ist aber auch die LHM als Host City, z. B. bei der Veranstaltung der offiziellen Fanzone im Olympiapark. Der BayLfD ist daher intensiv in die Abstimmungen zum städtischen Akkreditierungsverfahren bei der UEFA EURO 2020 einbezogen. Das Referat für Bildung und Sport ist für die LHM federführend unter Beteiligung der behördlichen Datenschutzbeauftragten an den Gesprächen beteiligt.

2.8. Datenpannen, Betroffenenrechte und Verarbeitungsverzeichnis – Zahlen, Daten, Fakten

Die DSGVO hat neben vielem anderen drei Neuerungen mit sich gebracht, für die stadtweite Prozesse etabliert bzw. aktualisiert wurden: die Pflicht, Datenschutzverletzungen an die Aufsichtsbehörde zu melden, die Stärkung der Betroffenenrechte, sowie die erweiterte Führung eines Verzeichnisses über sämtliche bei der Stadt vorgenommene Verarbeitungstätigkeiten.

Die Koordination bzw. Durchführung dieser Aufgaben wurden bei der „Zentralen Stelle“ gebündelt, die bei der behördlichen Datenschutzbeauftragten angesiedelt ist. Die Zentrale Stelle nimmt damit Aufgaben der LHM als verantwortliche Stelle wahr. Mangels ausreichender personeller Ausstattung ist die Erfüllung dieser Aufgaben bislang nur mit Unterstützung durch Nachwuchskräfte möglich. Dies ist jedoch keine Dauerlösung aufgrund des ständigen Wechsels der Nachwuchskräfte sowie der stets neu erforderlichen Einarbeitung. Aufgrund der bisherigen Erfahrung hat sich dennoch herauskristallisiert, dass es einen ständigen Bedarf für die Aufgaben der Zentralen Stelle gibt. So können v.a. die kurzen gesetzlichen Fristen bei der Erfüllung von Betroffenenrechten und der Meldung von Datenpannen sichergestellt werden, indem die Zentrale Stelle als einheitliche Anlaufstelle und als Koordinatorin fungiert. Die Nähe zur behördlichen Datenschutzbeauftragten vereinfacht zudem die parallel oft notwendige datenschutzrechtliche Beratung.

2.8.1. Datenpannen

Im Falle einer Datenschutzverletzung muss die Aufsichtsbehörde informiert werden, außer die Verletzung bringt voraussichtlich „kein Risiko für die Rechte und Freiheiten der betroffenen Personen“ mit sich (Art. 33 DSGVO). Für die Meldung an die Aufsichtsbehörde gilt eine Frist von 72 Stunden ab Bekanntwerden der Verletzung. Für die Einhaltung dieser sehr kurzen Frist wurde ein stadtweiter Prozess erarbeitet, der sich gut etabliert hat, auch wenn viele wichtige Detailfragen noch ungeklärt sind (wann ist die Risikoschwelle erreicht; wann gilt eine Verletzung als „bekannt“; wem muss sie bekannt sein; zählen Wochenenden und Feiertage bei der Fristberechnung mit usw.). Wichtig ist jedoch vor allem die Sensibilisierung aller Beschäftigten, bei Datenpannen sofort zu handeln und diese den zuständigen Stellen in der Verwaltung zu melden.

Im Zeitraum vom 25. Mai 2018 bis Februar 2021 ergibt sich folgendes Bild:

Datenpannen gesamt, soweit an Zentrale Stelle gemeldet	Davon an die Aufsichtsbehörde gemeldet	Davon nicht meldepflichtig	Rückfragen der Aufsichtsbehörde
174	79	95	In 8 Fällen

2.8.2. Betroffenenrechte

Betroffene Personen können u.a. Auskunft darüber verlangen, welche personenbezogenen Daten von ihnen bei der LHM verarbeitet werden. Sie haben das Recht, dass falsche Daten berichtigt und unter bestimmten Voraussetzungen nicht (mehr) benötigte Daten gelöscht werden (Art. 15 ff. DSGVO). Macht eine Person einen solchen Anspruch geltend, hat die LHM einen Monat Zeit, um ihn zu erfüllen. Dazu müssen Daten in den vielen Fachverfahren, Datenbanken, lokalen Speicherorten und Aktenablagen der städtischen Referate und Dienststellen eruiert werden. Die Monatsfrist kann daher nur mit einem gut organisierten, stadtweiten Prozess eingehalten werden.

Der im Rahmen des städtischen DSGVO-Projekts erarbeitete Prozess hat sich dabei bewährt. Bis auf wenige Fälle, in denen stets besondere Umstände vorlagen, konnten sämtliche der mehr als 100 Anträge seit Mai 2018 fristgerecht und datenschutzkonform beantwortet werden.

2.8.3. Verzeichnis von Verarbeitungstätigkeiten

Im Verzeichnis von Verarbeitungstätigkeiten werden alle Datenverarbeitungsvorgänge bei der LHM aufgelistet und beschrieben. Ein solches Verzeichnis gab es bereits nach altem Recht, es wurde durch die DSGVO jedoch erheblich ausgeweitet (Art. 30 DSGVO). Es muss nicht nur automatisierte Datenverarbeitungen (z.B. IT- Fachverfahren, Videoüberwachungsanlagen usw.) enthalten, sondern auch Verarbeitungsvorgänge in

papiergebundenen Dateisystemen (z.B. Aktensammlungen, die nach Namen sortiert sind), sowie Datenverarbeitungen, für die nach früherem Recht Ausnahmen zur Aufnahme in das Verzeichnis galten (z.B. Kontaktlisten, Datenbanken).

Das neue Verarbeitungsverzeichnis ist um knapp 1.000 Beschreibungen angewachsen:

Im Verzeichnissverzeichnis nach altem Recht enthaltenen Beschreibungen	Im Verarbeitungsverzeichnis nach DSGVO enthaltenen Beschreibungen (Stand: Oktober 2020)
ca. 350	ca. 1.300

Für die kontinuierliche Pflege des Verzeichnisses steht das Datenschutz-Management-Tool Risk2Value zur Verfügung.

Die Führung des Verzeichnisses ist bei der Zentralen Stelle bei der behördlichen Datenschutzbeauftragten angesiedelt. Die Pflege des Verzeichnisses obliegt den jeweils verantwortlichen Fachdienststellen und Referaten (d.h. inhaltliche Richtigkeit, Aktualität usw.).

Der behördlichen Datenschutzbeauftragten ist bei automatisierten Verarbeitungstätigkeiten sowie bei Videoüberwachung vor deren Einführung bzw. bei wesentlichen Änderungen Gelegenheit zur Stellungnahme zu geben (Art. 12 Abs. 1 Nr. 2, 24 Abs. 5 Bayerisches Datenschutzgesetz). Dies kann ebenfalls durch das Tool Risk2Value abgebildet werden.

2.9. Schulung und Awareness

Eine Aufgabe der LHM als datenschutzrechtlich Verantwortliche ist die regelmäßige Schulung und Sensibilisierung ihrer Beschäftigten zum Datenschutz. Als Kommune verarbeitet die LHM Daten aus sämtlichen Lebensbereichen ihrer Bürger*innen. Als Arbeitgeberin ist sie verantwortlich für die Personaldaten ihrer über 40.000 Beschäftigten. Im Januar 2020 wurde das stadtweite, verpflichtende E-Learning zum Datenschutz gestartet, als eines der ersten E-Learning-Formate bei der LHM überhaupt. Es haben bislang 65,8 % aller Beschäftigten die Schulung absolviert.

Parallel zum E-Learning sieht das Schulungskonzept Präsenzs Schulungen in den Dienststellen vor. Diese können von den örtlichen Datenschutzbeauftragten aus Kapazitätsgründen jedoch nur für bestimmte Zielgruppen angeboten werden.

Als weitere breitenwirksame Sensibilisierungsmaßnahme wurde im Rahmen des DSGVO-Projekts der Datenschutz-Auftritt in WiLMA neu als Wissensdatenbank mit vielen Arbeitshilfen für die tägliche Praxis konzipiert. Die Rückmeldungen zu dem Auftritt sind durchweg positiv.

Die örtlichen Datenschutzbeauftragten werden in alle zwei Monate stattfindenden Treffen über aktuelle Themen, Rechtsprechung usw. informiert. Für zusätzliche Schulungen, insbesondere von neuen Kolleg*innen, muss auf externe Angebote zurückgegriffen werden.

3. Beteiligung an Projekten und Gremien

An folgenden stadtweiten Projekten nimmt die behördliche Datenschutzbeauftragte beratend teil:

- neoHR - PMB T&S
- neoIT - Lenkungskreis
- Programmbeirat digital/4finance

In folgenden internen und externen Gremien ist die behördliche Datenschutzbeauftragte beteiligt:

- ISM-Board (intern)
- ISB-Forum (intern)
- Erfahrungsaustausch der Gesellschaft für Datenschutz und Datensicherheit
- Erfahrungsaustausch der bayerischen kommunalen Datenschutzbeauftragten
- Arbeitskreis Datenschutz des Bayerischen Staatsministerium des Innern
- Arbeitskreis Datenschutz im Deutschen Städtetag

Teil B - Datenschutzreform 2018 – Teil 3

Darstellung der positiven Effekte durch Stellenzuschaltungen sowie der negativen Effekte durch Unterschreitung des ermittelten Stellenmehrbedarfs

1. Auftrag des Stadtrats 2018

Im Eckdatenbeschluss vom 25.07.2018 (Vorlagennummer: 14-20 / V 11494) wurden für die örtlichen Datenschutzbeauftragten in den Referaten aufgrund der zusätzlichen Aufgaben durch die Datenschutz-Grundverordnung insgesamt 9,57 VZÄ beantragt.

Dem Antrag lag eine qualifizierte Schätzung des Personal- und Organisationsreferats zu Grunde, aus der sich ein Stellenbedarf von 15,71 VZÄ für den örtlichen Datenschutz in den Referaten ergeben hatte.

Mit Stadtratsbeschluss vom 24.10.2018 (Vorlagennummer 14-20 / V 12422) wurden insgesamt 1,71 VZÄ für den örtlichen Datenschutz bewilligt:

Referat	VZÄ gemäß qualifizierter Schätzung des POR	Im Eckdatenbeschluss vom 25.07.2018 beantragte VZÄ	Im Beschluss vom 24.10.2018 bewilligte VZÄ
PLAN	0,36	0,50	-
RAW	0,49	0,50	-
POR	0,97	1,50	-
RGU	1,82	1,75	-
SOZ	2,63	0,00	-
KOM	0,53	0,00	-
BAU	0,69	1,25	-
RBS	4,32	0,00	-
DIR	1,29	0,50	-
SKA	Keine Schätzung	0,00	-
REV	0,46	0,50	0,50
KULT	0,48	0,75	0,21
KVR	1,86	2,50	1,00
Summe	15,71	9,75	1,71

Das Direktorium wurde vom Stadtrat mit o.g. Beschluss vom 24.10.2018 weiter beauftragt, darzustellen, welche positiven Effekte durch die beantragten Stellenzuschaltungen erreicht wurden sowie welche möglichen negativen Auswirkungen sich durch die Unterschreitung des ermittelten Stellenmehrbedarfs ergeben haben.

2. Neue gesetzliche Aufgaben für Datenschutzbeauftragte nach DSGVO

Die Aufgaben der Datenschutzbeauftragten wurden durch die DSGVO erweitert. Neben den bereits vor der DSGVO bestehenden Beratungspflichten gegenüber der Verwaltung sind nun insbesondere der Überwachungsauftrag sowie die Beratung betroffener Personen hinzugekommen.

Die LHM als „Verantwortliche“ treffen mit der DSGVO deutlich mehr Dokumentations-, Transparenz-, Schulungs- und Meldepflichten. Auch wenn diese Pflichten klar dem

„Verantwortlichen“ zugeordnet sind und nicht den Datenschutzbeauftragten, entsteht für letztere dadurch erhöhter Beratungs- und Beteiligungsaufwand:

- Beteiligung an Datenschutz-Folgenabschätzungen
- Beurteilung der Meldepflicht von Datenschutzverletzungen an die Aufsichtsbehörde
- Sicherstellung der datenschutzkonformen Auskunftserteilung an Betroffene
- Beratung bei Erstellung von Dienstvereinbarungen und -anweisungen
- Beratung beim Abschluss von Auftragsverarbeitungs-Vereinbarungen
- Beratung bei der Umsetzung aktueller Rechtsprechung und Gesetzgebung
- Unterstützung bei Erstellung von Einwilligungserklärungen
- Unterstützung bei Erstellung von Datenschutzhinweisen
- Schulung der Beschäftigten in den Referaten

3. Positive Effekte durch die Stellenzuschaltungen in KVR, KULT und REV

Durch die vom Stadtrat 2018 bewilligten zusätzlichen Stellen wurde die Erfüllung der gesetzlichen Pflichten zumindest in den betreffenden Bereichen unterstützt.

Die Implementierung der durch das stadtweite DSGVO-Projekt neu geschaffenen Prozesse und deren Begleitung durch die Datenschutzbeauftragten ist gut vorangeschritten. Anträge von Betroffenen auf Auskunft, Löschung oder Berichtigung ihrer Daten konnten dank der kontinuierlichen Begleitung durch die Datenschutzbeauftragten zu fast 100% fristgerecht und immer datenschutzkonform bearbeitet werden. Weder in diesem Bereich noch aus sonstigen Anlässen gab es Beanstandungen der LHM durch die Aufsichtsbehörde. Die Vernetzung der Datenschutzbeauftragten mit Kolleg*innen von der IT sowie von anderen bayerischen Kommunen und deutschen Großstädten konnte ausgebaut werden.

4. Negative Auswirkungen durch die Unterschreitung des ermittelten Stellenmehrbedarfs

Nichts desto trotz muss aufgrund der Rückmeldungen der Datenschutzbeauftragten konstatiert werden, dass die Praxis und die Erfahrung der knapp drei Jahre seit Geltung der DSGVO gezeigt haben, dass die für den Stadtratsbeschluss 2018 mit Unterstützung des POR mit großem Aufwand durchgeführte qualifizierte Schätzung nicht umsonst auf den deutlich höheren Stellenbedarf kam.

4.1 Keine ausreichende Erfüllung der gesetzlichen Aufgaben

Allein die Erfüllung der gesetzlich vorgeschriebenen Pflichten kann den Rückmeldungen zufolge stadtweit nicht immer in ausreichendem Umfang und nur durch hohes persönliches Engagement der Kolleg*innen sichergestellt werden.

Die laufende Beratungstätigkeit bei komplexen datenschutzrechtlichen Fragestellungen, die zeitintensive Begleitung der Datenschutz-Folgenabschätzungen bei IT-Vorhaben usw. lassen neben dem Alltagsgeschäft kaum zu, insbesondere den gesetzlichen Überwachungsauftrag vollständig zu erfüllen. Diesem kann derzeit lediglich anlassbezogen nachgekommen werden. Eine regelmäßige, anlasslose Auditierung einzelner Fachbereiche oder IT-Verfahren ist darüber hinaus derzeit nicht leistbar.

4.2 Keine ausreichende Sensibilisierung der Beschäftigten möglich

Die Qualität des Datenschutzes einer Organisation hängt zudem in hohem Maß von dem Bewusstsein der Beschäftigten für die Bedeutung des Themas für ihre tägliche Arbeit ab. Dazu gehören neben Schulungs- und Sensibilisierungsmaßnahmen seitens der LHM als verantwortlicher Stelle auch der Kontakt zu und die Kommunikation der Beschäftigten mit den Datenschutzbeauftragten. Nur wenn diese in ihrer Funktion in den Referaten bekannt sind und sie selbständig „mitgedacht“ werden, wenn keine Scheu besteht, sich bei jeder Art von Fragen oder bei Datenschutzverletzungen vertrauensvoll an sie zu wenden, kann Datenschutz nachhaltig in die tägliche Arbeit, aber auch in die größeren Prozesse und die fortschreitende Digitalisierung integriert werden. Dieses Vertrauensverhältnis kann nur durch fortwährenden persönlichen Kontakt entstehen und gepflegt werden. Der Aufbau dieser „Soft Skills“ steht jedoch hinten, solange die Pflichtaufgaben der Datenschutzbeauftragten nicht umfänglich erfüllt werden können.

4.3 Einhaltung des Datenschutzes erforderlich

Datenschutz ist Grundrechtsschutz. Er muss daher für eine Kommune zwingend bei all ihren Aufgaben mitgedacht werden. Eine Kommune ist umgekehrt auch auf das Vertrauen ihrer Bürger*innen in die Rechtmäßigkeit ihrer Aufgabenerfüllung angewiesen. Nur dann kann die angestrebte Digitalisierung der Verwaltungsprozesse gelingen. Die bisherige Erfahrung zeigt, dass in der Bevölkerung mit der DSGVO ein erhöhtes Bewusstsein für den Schutz ihrer Daten entstanden ist.

Zudem gewinnt durch die zunehmende Digitalisierung der Arbeit in der Stadtverwaltung ein effektiver, von Anfang an eingebundener Datenschutz an Bedeutung.

Dies wird verstärkt durch die datenschutzfreundliche Rechtsprechung des EuGH sowie der nationalen Gerichte, die jedoch oft in einem Spannungsverhältnis zur gelebten Wirklichkeit steht. Besonders deutlich wird dies an dem jüngsten EuGH-Urteil zu Datenübermittlungen in die USA (Urteil vom 16.07.2020, „Schrems II“), die alle

Verantwortlichen in der EU vor enorme Herausforderungen stellt. Anbieter von IT-Systemen, die Lösungen liefern, die den Bedürfnissen einer modernen, effizienten und dienstleistungsorientierten Großstadtverwaltung wie der LHM entsprechen, erfüllen nicht immer die Vorgaben der DSGVO. Hier besteht immenser Handlungsbedarf seitens der LHM als verantwortliche Stelle. Vor diesem Hintergrund spielt der Datenschutz beim Thema „Digitale Souveränität“ eine nicht zu unterschätzende Rolle.

4.4 Zusammenfassung

Aufgrund der deutlich unter dem Antrag bleibenden Stellenzuschaltungen im Jahr 2018 können die gesetzlich vorgeschriebenen Pflichtaufgaben der Datenschutzbeauftragten nicht in ausreichendem Umfang erfüllt werden. Auch in den folgenden Jahren 2019 und 2020 wurden die Stellen im Rahmen des Eckdatenbeschlussverfahrens nicht verwirklicht. Zusätzliche, vom Gesetz nicht ausdrücklich erwähnte Zielsetzungen, die die Einhaltung und Berücksichtigung des Datenschutzes stadtweit nachhaltig verbessern würden, bleiben unerfüllt.

4.5 Mögliche Folgen für die LHM

Auch wenn die LHM als Kommune selbst von Bußgeldandrohungen ausgenommen ist, ist sie doch an Recht und Gesetz gebunden, Art. 20 Abs. 3 Grundgesetz.

Zudem sieht sie sich der Möglichkeit von Beanstandungen und Untersagungsverfügungen durch die Aufsichtsbehörde ausgesetzt. Letzteres bedeutet, dass bestimmte Verarbeitungstätigkeiten komplett untersagt werden können, mit erheblichen finanziellen Auswirkungen für die LHM. So wurde kürzlich in Baden-Württemberg erstmals eine Kommune mit einer Untersagungsverfügung belegt. Daneben sind aus dem Bereich der Privatwirtschaft Untersagungsverfügungen wegen des Einsatzes von Google Analytics in Rheinland-Pfalz bekannt.

Das Bayerische Datenschutzgesetz enthält darüber hinaus Ordnungswidrigkeiten- und Straftatbestände für bestimmte Fälle rechtswidriger Datenverarbeitung.

Schadensersatzforderungen von Betroffenen – auch für nicht-materielle Schäden - bei nicht datenschutzkonformem Umgang mit ihren Daten sind ebenfalls möglich und wurden Kläger*innen in den ersten Fällen bereits zugesprochen.

5. Beteiligung der Referate

Die Referate wurden bei der Bekanntgabe beteiligt. Folgende Referate haben Stellungnahmen abgegeben:

- Kommunalreferat
- Kulturreferat
- Personal- und Organisationsreferat

- Referat für Bildung und Sport
- Sozialreferat
- Kreisverwaltungsreferat

Die Stellungnahmen sind der Bekanntgabe als Anlagen 1 – 6 beigelegt.

Eine Mitzeichnung erfolgte durch das Personal- und Organisationsreferat, das Referat für Bildung und Sport sowie durch das IT-Referat.

Anhörung des Bezirksausschusses

In dieser Beratungsangelegenheit ist die Anhörung des Bezirksausschusses nicht vorgesehen (vgl. Anlage 1 der BA-Satzung).

Der Verwaltungsbeirätin des Direktoriums, Zentrale Verwaltungsangelegenheiten und Rechtsabteilung, Frau Stadträtin Lüttig ist ein Abdruck der Sitzungsvorlage zugeleitet worden.

II. Bekannt gegeben

Der Stadtrat der Landeshauptstadt München

Der / Die Vorsitzende

Der Referent

Ober-/Bürgermeister/-in
ea. Stadtrat/-rätin

Dieter Reiter
Oberbürgermeister

III. Abdruck von I. mit II.
über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt
z. K.

IV. Wv. Direktorium

1. Die Übereinstimmung vorstehenden Abdrucks mit der beglaubigten Zweitschrift wird bestätigt.
2. **An die behördliche Datenschutzbeauftragte**

z. K.

Am