Telefon: 233 - 28261
Telefax: 233 - 28606

Direktorium
Datenschutzbeauftragte

Tätigkeitsbericht der behördlichen Datenschutzbeauftragten 2021/2022

Sitzungsvorlage Nr. 20-26 / V 09928

3 Anlagen

Bekanntgabe in der Sitzung des Verwaltungs- und Personalausschusses vom 19.07.2023
Öffentliche Sitzung

I. Vortrag des Referenten

1. Tätigkeitsbericht der behördlichen Datenschutzbeauftragten 2021/2022

1.1. Fünf Jahre DSGVO – Rückblick und Ausblick

Am 25. Mai 2018 wurde die europäische Datenschutz-Grundverordnung (Verordnung (EU) 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 (Datenschutz-Grundverordnung); im Folgenden: DSGVO) in allen EU-Mitgliedsstaaten unmittelbar anwendbares Recht. Dieses Datum war der Start für ein neues, europaweit einheitliches Regelungsregime im Datenschutz, das viele Veränderungen mit sich gebracht hat, bei dem jedoch auch einiges Wesentliches gleich geblieben ist. Vor allem blieb - anders als von vielen befürchtet -, die Verarbeitung von Daten, die bisher rechtlich erlaubt war, unter der DSGVO zulässig. Bereits vor Geltung der DSGVO durften personenbezogene Daten nur dann verarbeitet werden, wenn ein Gesetz, ein Vertrag oder die Einwilligung der betroffenen Person es erlaubten. Datenschutz war seit jeher Grundrechtsschutz.

Geändert hat sich durch die DSGVO dennoch viel:

- Stärkerer Zusammenhang zwischen Technik und Datenschutz in der DSGVO;
- Klarere Abgrenzung von „Verantwortlichen“ und „Datenschutzbeauftragten“: Verantwortliche haben die Entscheidungsmacht und -verantwortung, Datenschutzbeauftragte beraten und kontrollieren;
- Stärkung der Betroffenenrechte durch mehr Transparenz und Information sowie durch mehr Möglichkeiten, die Verarbeitung der eigenen Daten zu steuern und deren Schutz durchzusetzen;
- Umfangreichere Dokumentations- und Rechenschaftspflichten des Verantwortlichen.

Was bedeuten diese Neuerungen für die Landeshauptstadt München?

- Hoher Umsetzungsdruck der neuen, vor allem formellen Vorgaben der DSGVO: bereits vor Geltung der DSGVO wurde ein stadtweites Projekt ins Leben gerufen. Es hat in intensiver, mehrjähriger Arbeit die Anforderungen des neuen Rechtsregimes umgesetzt und neue Prozesse und Vorgaben in die tägliche Arbeit der Stadtverwaltung erfolgreich integriert.
- Mehr Aktivität der Aufsichtsbehörden, deren Vorgaben, Entschließungen und aufsichtsrechtliche Maßnahmen umgesetzt werden müssen.
- Mehr Rechtsprechung zum Datenschutz sowohl des EuGH als auch der nationalen Gerichte: die DSGVO gewinnt immer mehr an Bedeutung bei Entscheidungen zu den verschiedensten Rechtsgebieten wie z.B. Arbeitsrecht, IT-Recht, Verwaltungsrecht; die Entwicklungen in der Rechtsprechung müssen beobachtet und bei der LHM in allen Bereichen umgesetzt werden.
- Stärkere Vernetzung und Zusammenarbeit von Datenschutz und IT bei der LHM.
- Erhöhte Dokumentations- und Rechenschaftspflichten, die u.a. bei aufsichtsbehördlichen Maßnahmen und in Gerichtsverfahren eine wichtige Rolle spielen (z.B. bei der Frage der Beweislast).

All diese neuen Vorgaben und Entwicklungen haben einen großen Einfluss sowohl auf die tägliche Arbeit aller Beschäftigten, die sie umsetzen müssen, als auch auf den Aufgabenumfang der Datenschutzbeauftragten, der damit enorm gestiegen ist.

1.2. Pandemiebekämpfung und Datenschutz – geht das?

In den beiden Berichtsjahren spielten die Maßnahmen zur Pandemiebekämpfung beim Datenschutz eine dominante Rolle. Immer wieder waren kurzfristig praxistaugliche Lösungen gefragt, um die Notwendigkeit von schnellem Handeln mit dem Schutz vor allem von Gesundheitsdaten unter sich fast wöchentlich ändernden tatsächlichen und rechtlichen Bedingungen so gut wie möglich zu vereinbaren.

1.2.1. Vereinbarkeit von schnellem Handeln und Datenschutz im CTT

Am deutlichsten zeigte sich dies bei der Arbeit des Contact Tracing Teams (CTT) im Gesundheitsreferat. Dort war die schnelle Kontaktaufnahme mit Infizierten und deren Kontaktpersonen, der Versand von Quarantäneanordnungen u.v.m. oberstes Gebot. Dies konnte mit den der LHM zur Verfügung stehenden technischen Mitteln teilweise nur schwer datenschutzkonform umgesetzt werden. Bei den meisten der in diesem Rahmen verarbeiteten Daten handelt es sich um schützenswerte Gesundheitsdaten, für die ein besonders hoher Schutzstandard gilt (Art. 9 DSGVO).

In intensiver Zusammenarbeit mit dem GSR und dem dortigen örtlichen Datenschutzbeauftragten wurden laufend mögliche Lösungen für die einzelnen Fallkonstellationen erarbeitet und dabei stets eine Abwägung zwischen den praktischen Notwendigkeiten und den Anforderungen des Datenschutzrechts vorgenommen.

1.2.2. Umfangreiche Datenerfassung: Kontaktdaten, Impf- und Genesenenstatus, Testergebnisse

Im Zusammenhang mit der Kontaktdatenerfassung, mit der Erhebung von Daten der Beschäftigten über ihren Impf- und Genesenenstatus, sowie von Daten über Corona-Testergebnisse durch die LHM als Arbeitgeberin haben uns im Berichtszeitraum zahlreiche Beratungsbitten von Bürger*innen und städtischen Beschäftigten erreicht. Letzteren Themenkomplex hat federführend das Team des örtlichen Datenschutzbeauftragten des Personal- und Organisationsreferats beratend begleitet, wir wurden laufend eingebunden. Aufgrund des dynamischen Geschehens waren immer wieder kurzfristig Anpassungen erforderlich.

1.2.3. Digitales Arbeiten

Durch die pandemiebedingte Notwendigkeit der vermehrten Arbeit im Homeoffice hat die Digitalisierung der Arbeitswelt auch bei der LHM einen enormen Schub erhalten. Vieles, was während der Pandemie angestoßen wurde, ist mittlerweile in den „Normalbetrieb“ überführt und die digitalen Arbeitsmöglichkeiten bleiben für die städtischen Beschäftigten erfreulicherweise weiter bestehen. Dieser Digitalisierungsprozess wurde vom Datenschutz intensiv begleitet. Dadurch konnte sichergestellt werden, dass die personenbezogenen Daten von Bürger*innen und Beschäftigten auch digital dsgvo-konform verarbeitet werden. So ist es beispielsweise gelungen, durch intensive Verhandlungen mit Cisco Webex die Nutzung dieses Videokonferenztools datenschutzkonform zu ermöglichen.

1.2.4. Hybride Stadtratssitzungen/ Digitale Stadtratssitzungen

Mit Art. 47a Bayerische Gemeindeordnung wurde während Corona die Rechtsgrundlage für das Abhalten digitaler bzw. hybrider Stadtratssitzungen geschaffen. In Folge haben sich sowohl der Stadtrat sowie die Bezirksausschüsse mit der Thematik befasst. In diesem Zusammenhang wurden zahlreiche datenschutzrechtliche Fragen geprüft, z.B. die Wahl eines dsgvo-konformen Videokonferenzsystems, die Erforderlichkeit einer Einwilligung in die Ton-Bild-Übertragung, Verhinderung der Kenntnisnahme der Sitzung durch im selben Raum anwesende Personen, etwa im Homeoffice. An der Erstellung entsprechender Beschlussvorlagen war die behördliche Datenschutzbeauftragte beteiligt, ebenso an Treffen mit anderen Kommunen, sowohl aus Bayern als auch aus anderen Bundesländern mit ähnlichen kommunalrechtlichen Regelungen.

1.3. Social Media und Datenschutz – geht das auch?

Theoretisch ja, und es gibt mittlerweile Anbieter, die eine datenschutzkonforme Alternative zur Verfügung stellen. Wie in vielen anderen Bereichen scheitert auch die rechtskonforme Nutzung von Social-Media-Kanälen nicht in erster Linie an den datenschutzrechtlichen Rahmenbedingungen, sondern vor allem daran, dass diese von den großen Social-Media-Anbietern nicht beachtet werden. Datenschutzkonforme Alternativen wie etwa Mastodon verfügen nicht über dieselbe Reichweite wie Facebook, Instagram & Co., so dass sie bislang nur bedingt attraktiv erscheinen. Zudem ist die Verhandlungsmacht einzelner verantwortlicher

Stellen gegenüber den großen Playern so gering, dass die Einhaltung der DSGVO kaum durchgesetzt werden kann. Hier wäre eine schlagkräftige Initiative auf europäischer Ebene wohl der einzige Weg, für mehr Datenschutz auf den Social Media Plattformen zu sorgen.

Die behördliche Datenschutzbeauftragte erreichen regelmäßig Anfragen aus der gesamten Stadtverwaltung zur Zulässigkeit der Nutzung von Social Media, neben Facebook insbesondere Instagram. Das Bedürfnis, über diese Kanäle vor allem jüngere Bevölkerungsgruppen zu erreichen und mit ihnen zu kommunizieren, ist durchaus nachvollziehbar. Allerdings belegen die Äußerungen der Aufsichtsbehörden zu dem Thema, dass eine finale datenschutzrechtliche Beurteilung der Nutzung äußerst schwierig ist, da die Social Media-Anbieter in keinster Weise transparent machen, wie und zu welchen Zwecken von ihnen personenbezogene Daten verarbeitet werden. Ob und in welchem Umfang in der Stadtverwaltung Social Media genutzt werden, ist letztendlich eine politische Entscheidung.

Insofern hat uns im Berichtszeitraum das Thema Social Media auf verschiedene Weise beschäftigt:

1.3.1. Facebook

Die Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ist in ihrem Gutachten von März 2022 zu dem Ergebnis gekommen, dass der Betrieb von Facebook Fanpages durch öffentliche Stellen derzeit nicht datenschutzkonform möglich ist. Der Deutsche Städtetag hat seine Mitglieder über das Gutachten informiert, empfiehlt ihnen jedoch nicht, die Fanpages abzuschalten. Es solle zunächst abgewartet werden, wie sich die deutschen Aufsichtsbehörden gegenüber den Bundes- und den Landesverwaltungen positionieren. Die Landeshauptstadt München folgt der Empfehlung des Deutschen Städtetags. Die zentral vom Presse- und Informationsamt veröffentlichten Datenschutzhinweise zu Facebook (Art. 13 DSGVO) wurden entsprechend angepasst.

Mit Verfügung vom 17.02.2023 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dem Bundespresseamt (BPA) den Betrieb der Facebook-Fanpage der Bundesregierung untersagt. Das Bundespresseamt hat gegen den Bescheid Klage vor dem VG Köln erhoben und in der Pressekonferenz vom 27.02.2023 bekräftigt, dass sie die Seiten zunächst nicht abschalten wird, da sie ihren Facebook-Auftritt als wichtigen Bestandteil ihrer verfassungsrechtlich gebotenen Öffentlichkeitsarbeit ansieht und sich bei der Wahl der Kommunikationskanäle an der tatsächlichen Mediennutzung der Bürger*innen orientiert.

Der Ausgang des Verfahrens wird von maßgeblicher Bedeutung für öffentliche und private Betreiber*innen einer Facebook-Fanpage sein.

1.3.2. Instagram

Im Jahr 2022 kam es zu einem Hacker-Angriff auf einen städtischen Instagram-Account mit ca. 5.000 Followern aufgrund einer Phishing-Mail. Dank schneller und effizienter Zusammenarbeit der IT-Sicherheit und der zuständigen Datenschutzbeauftragten konnten alle notwendigen Schritte ergriffen werden, um den Schutz der Daten der betroffenen Personen

sicherzustellen. Die rechtlich verpflichtende Meldung des Vorfalls an den Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) wurde vorgenommen. Aufgrund der schnell ergriffenen Schutzmaßnahmen durch die LHM konnte kein Schaden für die betroffenen Personen festgestellt werden, und die Meldung an den BayLfD blieb ohne aufsichtsrechtliche Konsequenzen.

1.4. Livestream bei Bürgerversammlungen

Im Zuge der Stadtrats-Beschlussvorlage für den Livestream bei Bürgerversammlungen hat der behördliche Datenschutz gemeinsam mit der örtlichen Datenschutzbeauftragten des Direktoriums die datenschutzrechtliche Zulässigkeit geprüft. Aufgrund seiner bisherigen kritischen Haltung zum Livestream wurde zudem der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) konsultiert.

Erfreulicherweise hat dieser die geplante Vorgehensweise der Landeshauptstadt München gutgeheißen, so dass am 21.07.2021 der erste Livestream einer Bürgerversammlung im Circus Krone erfolgreich durchgeführt werden konnte.

1.5. Datenübermittlungen in die USA: nach dem Schrems ist vor dem Schrems?

Datenübermittlungen in Länder außerhalb der EU sind nach der DSGVO nur unter bestimmten Voraussetzungen zulässig. Eine Möglichkeit besteht darin, dass die EU-Kommission einen sogenannten Angemessenheitsbeschluss erlässt. Dieser besagt, dass das Datenschutzniveau in dem jeweiligen Drittland demjenigen der EU entspricht und personenbezogene Daten in das Drittland übermittelt werden dürfen, wenn einige weitere Voraussetzungen erfüllt sind. Für die USA bestand bis zum 16.07.2020 ein solcher Angemessenheitsbeschluss („EU-US-Privacy-Shield“).

Aufgrund einer Klage des österreichischen Datenschutz-Aktivisten Max Schrems hat der EuGH mit Urteil vom 16.07.2020 („Schrems II“, Az.: C 311/18) das Privacy-Shield für nichtig erklärt, insbesondere weil Zugriffsmöglichkeiten der US-Sicherheitsbehörden und -Geheimdienste auf die Daten europäischer Bürger*innen nicht ausreichend beschränkbar waren und den Betroffenen kein entsprechend umfänglicher Rechtsschutz gegen Zugriffe auf ihre Daten in den USA zur Verfügung stand. Über Nacht waren damit Datenübermittlungen in die USA nicht mehr dsgvo-konform möglich. Auf den ersten Blick mag dies die LHM als bayerische Kommune nicht weiter betreffen, jedoch finden auch bei der Stadtverwaltung vielfach Datenübermittlungen in die USA statt, z.B. durch den Einsatz von Software von IT-Dienstleistern mit Sitz in den USA.

In Folge dieses Urteils wurde europaweit nach Lösungsmöglichkeiten gesucht, erschien doch die Unterbrechung sämtlicher Datenflüsse aus der EU in die USA praktisch unmöglich. Die behördliche Datenschutzbeauftragte hat in enger Zusammenarbeit mit den örtlichen Datenschutzbeauftragten, den Kolleg*innen von der IT und dem Datenschutzbeauftragten von IT@M mit hohem Arbeitsaufwand versucht, die Folgen des Urteils für die digitale Arbeit der Stadtverwaltung möglichst gering zu halten, die betreffenden Dienststellen entsprechend zu

beraten und teilweise langwierige Verhandlungen mit US-amerikanischen Software-Anbietern geführt, um einen dsgvo-konformen Einsatz bei der LHM zu ermöglichen. In großen Teilen ist dies glücklicherweise gelungen.

Derzeit zeichnet sich erfreulicherweise eine übergeordnete Lösung ab. Am 25.03.2022 haben sich EU-Kommissionspräsidentin von der Leyen und US-Präsident Biden auf einen „Trans-Atlantic-Data-Privacy-Framework“ geeinigt. In Folge dieser Einigung wurde am 07.10.2022 von US-Präsident Biden eine entsprechende Presidential Executive Order veröffentlicht. Die EU-Kommission hat daraufhin den Entwurf eines Angemessenheitsbeschlusses nach Art. 45 DSGVO vorgelegt, der derzeit mit den EU-Mitgliedsstaaten verhandelt wird. Die Erwartung besteht, dass der Entwurf bis Sommer 2023 angenommen und damit eine neue Grundlage für die Datenübermittlungen in die USA geschaffen wird. Die Fachwelt rechnet zwar damit, dass Herr Schrems auch an dem neuen Angemessenheitsbeschluss Kritik üben wird, allerdings bleibt dies abzuwarten. Bis dahin kann hoffentlich in naher Zukunft die Datenübermittlung in die USA durch den neuen Angemessenheitsbeschluss wieder auf datenschutzrechtlich sichere Beine gestellt werden.

1.6. Arbeiten der Zukunft I: E-Akte

Auf Wunsch der behördlichen Datenschutzbeauftragten ist diese seit 2021 sowohl im Programmbeirat als auch im Lenkungskreis eAkte vertreten. So kann der Datenschutz bei der Umstellung auf digitale Verwaltungsabläufe von Anfang an mitgedacht und realisiert werden (u.a. bei der Umsetzung der Grundsätze für die Verarbeitung von personenbezogenen Daten gem. Art. 5 DSGVO und bei der Berücksichtigung von Betroffenenrechten gem. Art. 15 ff. DSGVO).

1.7. Arbeiten der Zukunft II: Cloud Computing

Der Einsatz von Cloud-Lösungen wird in den kommenden Jahren immer weiter zunehmen, da viele IT-Dienstleister keine sogenannten On-Premise-Lösungen mehr anbieten werden (Betrieb von Software/Fachanwendungen auf eigenen Servern).

Dies stellt die LHM vor datenschutzrechtliche Herausforderungen, die die behördliche Datenschutzbeauftragte in Zusammenarbeit mit den örtlichen Datenschutzbeauftragten in den Referaten, dem Datenschutzbeauftragten von IT@M sowie der IT-Sicherheit beratend begleitet.

Fragen, die sich bei der Planung von Cloud-Nutzungen u.a. stellen sind:

- Wo stehen die Server des Cloud-Anbieters – in der EU, im Europäischen Wirtschaftsraum oder einem Drittland?

- Wenn Drittland: ist das Datenschutzniveau dort ähnlich wie in der EU (Angemessenheit)?

- Müssen zusätzliche Vereinbarungen geschaffen oder zusätzliche technisch-organisatorische Maßnahmen ergriffen werden?

- Wer hat Zugriffsrechte auf die in der Cloud liegenden personenbezogenen Daten? Arbeitet der Cloud-Anbieter mit Unterauftragnehmern zusammen (z.B. für den technischen Support)?

- Können die Daten verschlüsselt in der Cloud abgelegt werden? Wer hat den Schlüssel und damit die Kontrolle über den Zugriff auf die Daten?

- Kann die LHM personenbezogene Daten in der Cloud selbständig löschen?

- Wie sensibel sind die personenbezogenen Daten, die in der Cloud gespeichert werden sollen?

- Gibt es gesetzliche Vorgaben für bestimmte Datenarten bei deren Speicherung in einer Cloud?

Der Datenschutzbeauftragte von IT@M hat gemeinsam mit dem behördlichen Datenschutz eine Orientierungshilfe erarbeitet, die die wichtigsten datenschutzrechtlichen Punkte bei der Beschaffung von Cloud-Diensten durch die LHM enthält. Sie soll eine hinreichend informierte Entscheidung durch die jeweils zuständigen Gremien ermöglichen.

1.8. Arbeiten der Zukunft III: Desk Sharing

Am 20.10.2021 hat der Stadtrat das „Konzept für die zukünftige Arbeitsgestaltung im Verwaltungsbereich der LHM“ sowie die „Reform des Personal- und Organisationsmanagements der LHM – Grundsatzbeschluss neoHR“ beschlossen. Danach sollen u.a. dauerhaft ein breiter Einsatz von mobilem Arbeiten/Homeoffice erfolgen, die Verwaltungsstandortstrategie überarbeitet und Büroarbeitsplätze durch Zellenbüro-Desksharing reduziert werden.

Bei all diesen Themen ist der Datenschutz zu berücksichtigen. Im Rahmen von neoHR berät die behördliche Datenschutzbeauftragte gemeinsam mit dem örtlichen Datenschutzbeauftragten des Personal- und Organisationsreferats zu den datenschutzrechtlichen Besonderheiten, zumal besondere Anforderungen zum Schutz personenbezogener Daten zu beachten sind (z.B. Clean Desk Policy, abschließbare Container, vertrauliche Gesprächsführung etc.).

1.9. digital 4 finance (d4f)

Das städtische Rechnungswesen wird mit d4f auf neue digitale Beine gestellt. Das Projekt wird datenschutzrechtlich vom örtlichen Datenschutz der Stadtkämmerei intensiv und mit großer Expertise begleitet, eine Einbindung des behördlichen Datenschutzes erfolgt in allen relevanten Themen. Im Berichtszeitraum war u.a. die datenschutzrechtliche Einbettung der im

Rahmen von d4f vorgesehenen Zugriffsmöglichkeiten auf die sogenannten Einheitsgeschäftspartner*innen durch alle zuständigen Dienststellen stadtweit erforderlich. Mit den stadtweiten Zugriffsmöglichkeiten auf diese große Zahl von Datensätzen gehen Risiken für die betroffenen Personen einher. Gemeinsam mit dem örtlichen Datenschutz der Stadtkämmerei konnten wichtige datenschutzrechtliche Fragen geklärt und praxistaugliche Lösungsmöglichkeiten aufgezeigt werden.

1.10. UEFA 2024: Akkreditierungsverfahren nun datenschutzkonform möglich

Bislang fehlte eine datenschutzrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Behördenakkreditierung bei Sportgroßveranstaltungen, was die Stadtverwaltung vor Schwierigkeiten gestellt hat. Der Landesgesetzgeber hat zwischenzeitlich Art. 60 a Polizeiaufgabengesetz (PAG) neu geschaffen. Diese Neuregelung kann – obwohl im Polizeirecht verankert – nach Auffassung des BayLfD im Ergebnis als Rechtsgrundlage für die Zuverlässigkeitsüberprüfung und die damit verbundene Datenübermittlung dienen.

1.11. Schulen als datenschutzrechtlich Verantwortliche – klingt banal, ist es aber nicht

Der BayLfD vertritt die Auffassung, dass alle Schulen eigene Verantwortliche im Sinne der DSGVO sind. Daran knüpfen sich viele rechtliche, aber auch praktische Zuständigkeitsfragen, die nun im laufenden Betrieb geklärt und umgesetzt werden müssen. So war bislang z.B. offen, in welcher Form Datenverarbeitungs-Vereinbarungen zwischen der LHM als Sachaufwandsträgerin und den Schulen geschlossen werden müssen, und inwieweit die Schulen personell in der Lage sind, sämtliche Pflichten zu erfüllen, die sie als Verantwortliche im Sinne der DSGVO treffen – um nur einige der drängendsten ungeklärten Punkte zu nennen. Hier werden weitere intensive Abstimmungs- und Klärungsprozesse innerhalb der LHM nötig sein. Erfreulicherweise hat der Stadtrat der Schaffung einer Stelle für eine*n gemeinsame*n Datenschutzbeauftragte*n für sämtliche städtische Schulen im Referat für Bildung und Sport, Stabsstelle Recht, zugestimmt. Dies ermöglicht die Bündelung von Aufgaben und Fachwissen, und stellt eine effiziente und kompetente datenschutzrechtliche Beratung der Schulen sicher.

1.12. Faxen: nicht wegzudenken aus dem Arbeitsalltag?

Die Nutzung von Fax als Kommunikationsweg mit externen Stellen ist stadtweit immer noch üblich. Die Übertragung von Faxen erfolgt – ebenso wie die herkömmliche E-Mail-Kommunikation – unverschlüsselt und ist für den Versand personenbezogener Daten daher nur bedingt geeignet. Die von der behördlichen Datenschutzbeauftragten ins Leben gerufene Arbeitsgruppe Faxversand (AG Fax) hat im Berichtszeitraum Informationen und Handlungsempfehlungen für die Referate erarbeitet, mit denen die Beschäftigten entsprechend sensibilisiert und über mögliche Alternativen zum Fax in Kenntnis gesetzt werden.

1.13. Drucken: nicht wegzudenken aus dem Arbeitsalltag

Im Oktober 2022 hat der stadtweite Rollout der neuen Client Print-Infrastruktur begonnen. Die neu eingesetzte Software Virtual Print Service Enterprise (VPSX) ermöglicht u.a. den sogenannten „vertraulichen Druck“, bei dem der Druckvorgang erst nach Authentifizierung am Druckgerät ausgelöst wird. Die behördliche Datenschutzbeauftragte hat im Projekt-Lenkungskreis die klare Empfehlung ausgesprochen, die Möglichkeit des vertraulichen Drucks stadtweit zu nutzen, um das Ansteuern eines falschen Druckers oder das Liegenlassen vertraulicher Dokumente in öffentlich zugänglichen Druckern zu vermeiden und somit meldepflichtigen Datenschutzverletzungen (Art. 33 DSGVO) präventiv entgegenzuwirken.

1.14. Recht auf Vergessenwerden – auch gegenüber dem behördlichen Datenschutz

Auch Datenschutzbeauftragte dürfen nicht alle personenbezogenen Daten, die ihnen im Rahmen ihrer Aufgabenerfüllung bekannt werden, zeitlich unbegrenzt speichern und aufbewahren. Das gesetzlich verbriefte Recht auf „Vergessenwerden“ gilt gegenüber Datenschutzbeauftragten genauso wie gegenüber jeder anderen städtischen Dienststelle.

Aus diesem Grund hat die behördliche Datenschutzbeauftragte ein Löschkonzept für die Datenverarbeitungsvorgänge erarbeitet, die bei ihr stattfinden (z.B. Beratungstätigkeit für städtische Dienststellen und örtliche Datenschutzbeauftragte, Bearbeitung von Beschwerden von Betroffenen, Meldung von Datenschutzverletzungen, koordinierte Bearbeitung von Betroffenenrechten, etc.). Das Löschkonzept wird dieses Jahr umgesetzt und dient den örtlichen Datenschutzbeauftragten in den Referaten als Muster für ihre eigene Tätigkeit.

1.15. Information, Schulung und Awareness: für effizienten Datenschutz unerlässlich

Der Schutz personenbezogener Daten obliegt jeder*jedem einzelnen städtischen Beschäftigten bei der täglichen Arbeit. Ein effizienter Schutz setzt voraus, dass das entsprechende Bewusstsein vorhanden ist bzw. geschaffen wird, dass alle Mitarbeitenden über das nötige Wissen zum Datenschutz verfügen und ihnen die dafür erforderlichen Informationen und Hilfsmittel an die Hand gegeben werden.

Dies erfolgt bei der LHM auf vielfältige Weise:

1.15.1. Neue Online-Schulung zum Datenschutz für die städtischen Beschäftigten

Die Organisation und Durchführung von Schulungen ist nach der DSGVO die Aufgabe des Verantwortlichen, also der LHM. Die Datenschutzbeauftragten überwachen lediglich die Erfüllung dieser Aufgabe. Insofern liegt es grundsätzlich in der Verantwortung der Referate, ihren Mitarbeitenden entsprechende Datenschutz-Schulungen anzubieten.

Darüber hinaus wurde den städtischen Beschäftigten im Jahr 2020 ein E-Learning zum Datenschutz zur Verfügung gestellt, das im Rahmen des stadtweiten Projekts „Umsetzung DSGVO“ beschafft wurde. Das E-Learning stand den Mitarbeiter*innen ein Jahr zur

Verfügung, die Teilnahmequote stadtweit betrug 54%. Mit diesem Schritt hat der Datenschutz echte Pionierarbeit geleistet, da es ein stadtweit ausgerolltes E-Learning bis dato noch nicht gegeben hat. Die dabei gesammelten praktischen Erfahrungen konnten an das Personal- und Organisationsreferat für künftige E-Learning-Vorhaben weitergegeben werden.

Da Datenschutzschulungen von externen Anbietern oftmals nicht ausreichend die Besonderheiten der öffentlichen Verwaltung berücksichtigen, erarbeitet das Team des örtlichen Datenschutzbeauftragten des POR in Abstimmung mit dem behördlichen Datenschutz derzeit eine Online-Schulung für alle städtischen Beschäftigten. Die Schulungsmaßnahme kann den städtischen Beschäftigten voraussichtlich noch im Jahr 2023 zur Verfügung gestellt werden.

1.15.2. Die Datenschutzseite in WiLMA für aktuelle Informationen im Arbeitsalltag

Im Rahmen des Projekts „Umsetzung DSGVO“ wurde die Datenschutzseite in WiLMA neu konzipiert und mit umfassenden Informationen zu datenschutzrechtlichen Themen, mit Arbeitshilfen, Musterformularen u.v.m. bestückt. Die Rückmeldungen aus den Referaten zur Praxistauglichkeit und -relevanz der dort angebotenen Informationen sind durchweg positiv, die Seite hat konstant um die 2.600 Abonnent*innen.

Der behördliche Datenschutz hält die Informationen auf der WiLMA-Seite mit Unterstützung der örtlichen Datenschutzbeauftragten aktuell und schreibt regelmäßig Beiträge zu aktuellen Themen.

Die Datenschutzseite in WiLMA hat sich damit als wichtige Informationsquelle für die städtischen Beschäftigten zu Fragen rund um den Datenschutz etabliert und bewährt.

1.15.3. Schulung der örtlichen Datenschutzbeauftragten der Referate

Eine Schulung im engeren Sinne für die örtlichen Datenschutzbeauftragten kann vom behördlichen Datenschutz aus Kapazitätsgründen nicht angeboten werden. Neben der regelmäßigen Beratung im Einzelfall finden vierteljährlich die „Treffen der örtlichen Datenschutzbeauftragten“ statt, bei denen zum Einen der Austausch der Datenschutzbeauftragten untereinander, zum Anderen die Informationsweitergabe durch den behördlichen Datenschutz über aktuelle Entwicklungen in Rechtsprechung und Literatur, bei den Aufsichtsbehörden und auf europäischer Ebene im Mittelpunkt stehen.

Mit der regelmäßigen „Fragestunde“ konnte der behördliche Datenschutz im Berichtszeitraum ein neues Schulungsformat für die örtlichen Datenschutzbeauftragten etablieren, das diesen die Möglichkeit bietet, im direkten Dialog formlos offene Fragen zu klären und Informationen für ihre Arbeit in den Referaten zu erhalten.

1.15.4. Der behördliche Datenschutz goes „Learn@Lunch“

Im Dezember 2021 hatte das Team der behördlichen Datenschutzbeauftragten die Gelegenheit, im Rahmen des stadtinternen Online-Formats „Learn@Lunch“ die städtischen Beschäftigten zum Thema „Datenschutz bei der LHM – Einblicke in die Praxis“ zu informieren.

In einem halbstündigen Vortrag konnten die wichtigsten Themen leicht zugänglich präsentiert werden. Im Anschluss gab es eine interaktive Fragerunde mit den Teilnehmenden.

Der behördliche Datenschutz nutzt damit auch neue Kommunikationsformate, um die Awareness und Akzeptanz des Themas „Schutz personenbezogener Daten“ bei den städtischen Mitarbeiter*innen zu erhöhen und um „dem Datenschutz ein Gesicht zu geben“. Letzteres senkt die Hürden deutlich, bei Fragen Kontakt mit den Kolleg*innen vom Datenschutz aufzunehmen.

1.15.5. Regelmäßiger Bericht an den Oberbürgermeister

Die behördliche Datenschutzbeauftragte erstellt jährlich vier Quartalsberichte über ihre Tätigkeit für den Oberbürgermeister, wovon der letzte jeweils als Jahresbericht konzipiert ist. In den daran gekoppelten Jour Fixe mit dem Büro des Oberbürgermeisters werden einzelne Themen besprochen und erläutert.

In einigen Referaten werden von den örtlichen Datenschutzbeauftragten zudem Jahresberichte über ihren Tätigkeitsbereich für die Referatsleitung erstellt.

1.16. Bürger*innen-Datenschutzservice: Umsetzung des Online-Zugangsgesetzes (OZG)

Bereits im Jahr 2020 hat der behördliche Datenschutz seine Geschäftsprozesse in Zusammenarbeit mit den Kolleg*innen des Geschäftsprozess- und Anforderungsmanagements des Direktoriums definiert und pflegt diese kontinuierlich.

Auf dieser Grundlage konnte im Berichtszeitraum eine Anforderung aus dem Katalog des OZG umgesetzt werden: die Möglichkeit für Bürger*innen, Datenschutzverletzungen oder vermutete Datenschutzverletzungen durch die LHM online zu melden.

Eine weitere OZG-Anforderung soll noch im Jahr 2023 verwirklicht werden: die Möglichkeit, Betroffenenrechte online geltend zu machen (Recht aus Auskunft, Löschung, Berichtigung etc., Art. 15 ff. DSGVO).

Leider musste dabei – wie von vielen anderen Stellen – die Erfahrung gemacht werden, dass ein reiner Online-Zugang von Bürger*innen zur Verwaltung noch lange nicht eine vollständige Digitalisierung von Verwaltungshandeln und -kommunikation darstellt. Insbesondere die fehlende Möglichkeit, in beide Richtungen verschlüsselt elektronisch zu kommunizieren führt dazu, dass der echte Mehrwert eines Online-Formulars für beide Seiten sehr beschränkt bleibt.

1.17. Die behördliche Datenschutzbeauftragte ist Vorsitzende des Arbeitskreises Datenschutz im Deutschen Städtetag

Die behördliche Datenschutzbeauftragte ist im Jahr 2022 aufgrund ihrer langjährigen Teilnahme und ihrer von den Mitgliedern sehr geschätzten Professionalität und Expertise zur Vorsitzenden des Arbeitskreises Datenschutz im Deutschen Städtetag gewählt worden. Dem Arbeitskreis gehören neben den drei Stadtstaaten je eine Stadt aus jedem Bundesland an. Er dient nicht nur dem Austausch zu datenschutzrechtlichen Themen von überregionaler Bedeutung, sondern auch als Sprachrohr des Deutschen Städtetags für datenschutzrechtliche Belange gegenüber Bundes- sowie europäischen Gremien und Institutionen.

1.18. Beteiligungen

An folgenden stadtweiten Projekten nahm die behördliche Datenschutzbeauftragte im Berichtszeitraum beratend teil:

- neoHR - PMB T&S
- neoIT – Lenkungskreis
- Lenkungskreis und Programmbeirat E-Akte
- Programmbeirat digital/4finance

In folgenden internen und externen Gremien war die behördliche Datenschutzbeauftragte im Berichtszeitrum beteiligt:

- Leitung des Arbeitskreises Datenschutz im Deutschen Städtetag
- Erfahrungsaustausch der bayerischen kommunalen Datenschutzbeauftragten; die Teilnahme der Datenschutzbeauftragten der LHM ist für die anderen Kommunen wichtig, da München als bayerische Landeshauptstadt Vorbildcharakter hat und oftmals eine Vorreiterrolle bei der Umsetzung des Datenschutzes einnimmt
- Arbeitskreis Datenschutz des Bayerischen Staatsministeriums des Innern
- Erfahrungsaustausch der Gesellschaft für Datenschutz und Datensicherheit (GDD)
- ISM-Board (intern)
- ISB-Forum (intern; mittlerweile aufgelöst aufgrund der Zentralisierung der ISB im RIT)

1.19. Datenschutz-Abmahnwelle

Dass Datenschutz auch zu ganz anderen Zwecken missbraucht werden kann, bewies eine deutschlandweite Abmahnwelle im Jahr 2022. Wie viele andere öffentliche und private Stellen haben dabei auch die LHM sowie städtische Schulen mehrere Abmahnungen wegen der vermeintlich nicht datenschutzkonformen Nutzung von Google Fonts auf Webseiten erreicht. Anlass war ein Urteil des LG München vom 20.01.22 (Az. 3 O 17493/20). Nach dem Urteil ist Google Fonts nicht datenschutzkonform einsetzbar, wenn es nicht lokal gespeichert und eingebunden wird.

Die Abmahnungen wurden deutschlandweit überwiegend von zwei Rechtsanwälten initiiert. Dazu hat die Generalstaatsanwaltschaft Berlin am 21.12.2022 per Pressemeldung mitgeteilt, dass in einem Verfahren gegen einen Rechtsanwalt und dessen Mandanten wegen des Verdachts des (teils) versuchten Abmahnbetruges und der (versuchten) Erpressung in mindestens 2.418 Fällen Durchsuchungsbeschlüsse sowie zwei Arrestbeschlüsse mit einer Gesamtsumme vom 346.000 Euro vollstreckt wurden.

Die LHM hat Google Fonts datenschutzkonform, d.h. lokal gespeichert und eingebunden und auf die Abmahnungen nicht reagiert. Mit weiteren Abmahnungen wegen der Nutzung von Google Fonts ist nach dem Vorgehen der Generalstaatsanwaltschaft Berlin nicht zu rechnen.

Ähnliche Fälle sind allerdings wegen des in der DSGVO normierten Schadensersatzanspruchs – auch für immaterielle Schäden – künftig nicht auszuschließen.

2. Aufgaben der Zentralen Stelle – Zahlen, Daten, Fakten

Der behördliche Datenschutz nimmt in Personalunion drei Aufgaben der LHM als verantwortliche Stelle wahr:

- die Meldung von Datenschutzverletzungen an die zuständige Aufsichtsbehörde,
- die Koordinierung der Erfüllung von Betroffenenrechten sowie
- die Führung des Verzeichnisses über sämtliche in der Stadtverwaltung vorgenommene Verarbeitungstätigkeiten.

Diese Aufgaben wurden bei der „Zentralen Stelle“ gebündelt, welche bei der behördlichen Datenschutzbeauftragten angesiedelt ist. So können v.a. die kurzen gesetzlichen Fristen bei der Erfüllung von Betroffenenrechten und bei der Meldung von Datenpannen sichergestellt werden. Gleichzeitig vereinfacht dies die parallel oft notwendige datenschutzrechtliche Beratung der örtlichen Datenschutzbeauftragten und der betreffenden Fachdienststellen.

2.1. 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.

Im Zeitraum vom 01.01.2021 bis 31.12.2022 sind folgende Datenpannen bearbeitet worden:

Datenpannen gesamt, soweit an Zentrale Stelle gemeldet	Davon an die Aufsichtsbehörde gemeldet	Davon nicht meldepflichtig	Rückfragen der Aufsichtsbehörde	Beanstandung durch die Aufsichtsbehörde
155	39	116	In 10 Fällen	0

Der überwiegende Teil der Datenschutzverletzungen betraf dabei Fehlversendungen von Schreiben aufgrund versehentlicher Fehladressierung oder -kuvertierung (bei maschineller Kuvertierung), sowie aufgrund versehentlicher Falscheingabe von Empfänger*innen bei E-Mails. Aufgrund der hohen Zahl der täglich von der Stadtverwaltung versandten Papierpost und Mails werden sich derartige Vorkommnisse trotz ausreichender technisch-organisatorischer Maßnahmen auch in Zukunft nicht vollständig vermeiden lassen.

Sämtliche an die Zentrale Stelle gemeldeten Datenschutzverletzungen wurden zum Anlass genommen, die Beschäftigten der betroffenen Bereiche zu sensibilisieren und Prozesse weiter zu optimieren. Diese Maßnahmen wurden von den Aufsichtsbehörden entsprechend wahrgenommen, so dass es in keinem Fall zu einer aufsichtsbehördlichen Beanstandung der LHM kam.

2.2. 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 nicht (mehr) benötigte Daten gelöscht werden, wenn die gesetzlichen Voraussetzungen dafür vorliegen (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 zahlreichen Fachverfahren, Datenbanken, lokalen Speicherorten und Aktenablagen der städtischen Referate und Dienststellen gesucht werden. Die Monatsfrist kann daher nur mit einem gut organisierten, stadtweiten Prozess eingehalten werden. Dieser hat dazu geführt, dass im Berichtszeitraum sämtliche der über 40 Anträge fristgerecht beantwortet werden konnten.

2.3. Verzeichnis von Verarbeitungstätigkeiten

Im Verzeichnis von Verarbeitungstätigkeiten werden alle Datenverarbeitungsvorgänge bei der LHM aufgelistet und beschrieben (vgl. Art. 30 DSGVO).

Die Führung des Verzeichnisses ist bei der Zentralen Stelle bei der behördlichen Datenschutzbeauftragten angesiedelt. Die Pflege des Verzeichnisses obliegt den jeweils datenschutzrechtlich verantwortlichen Fachdienststellen und Referaten (d.h. inhaltliche Richtigkeit, Aktualität usw.). Für die kontinuierliche Pflege des Verzeichnisses steht ein Datenschutz-Management-Tool zur Verfügung.

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 abgebildet werden.

Das Verzeichnis enthält – Stand Dezember 2022 – rund 1.600 Einträge. Zum Ende des vorangehenden Berichtszeitraums 2019/2020 betrug die Anzahl 1.300 Verarbeitungstätigkeiten.

3. Stellensituation und Erfüllung der gesetzlichen Aufgaben

Die Aufgaben der Datenschutzbeauftragten wurden durch die DSGVO deutlich 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.

Die behördliche Datenschutzbeauftragte ist personell wie folgt ausgestattet:

- 2 VZÄ für Volljurist*innen, davon eine für die Funktion der behördlichen Datenschutzbeauftragten und Leitung der Zentralen Stelle
- 1 VZÄ für den technisch-organisatorischen Datenschutz
- 1 VZÄ für Vorzimmer und Assistenz.

Erfreulicherweise wurde vom Stadtrat im Rahmen des Beschlusses zum HH 2023 eine zusätzliche Stelle für den behördlichen Datenschutz bewilligt. Das Stellenbesetzungsverfahren mit Aufgabenbeschreibung etc. ist derzeit in Arbeit.

In den Referaten sind jeweils örtliche Datenschutzbeauftragte (größtenteils mit Stellvertretungen) benannt. Die örtlichen Datenschutzbeauftragten nehmen für ihren Zuständigkeitsbereich die gleichen Aufgaben wahr wie die behördliche Datenschutzbeauftragte. Sie sind die erste Anlaufstelle bei Beratungsbedarf innerhalb ihres Referats und binden die behördliche Datenschutzbeauftragte im Einzelfall beratend mit ein. Die örtlichen Datenschutzbeauftragten sind jedoch ganz überwiegend mit geringen bis unterhälftigen Stundenanteilen für den Datenschutz ausgestattet.

Die Erfüllung der gesetzlich vorgeschriebenen Pflichten der Datenschutzbeauftragten kann angesichts dieser personellen bzw. zeitlichen Ausstattung nicht immer in ausreichendem Umfang 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 in kleinem Umfang nachgekommen werden. Eine regelmäßige, anlasslose Auditierung einzelner Fachbereiche oder IT-Verfahren ist darüber hinaus nicht leistbar.

Proaktive Information, Beratung oder gar Sensibilisierung und Schulung der Beschäftigten oder einzelner Beschäftigtengruppen ist darüber hinaus nur eingeschränkt möglich. 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, 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 hintan, solange die Pflichtaufgaben der Datenschutzbeauftragten nicht umfänglich erfüllt werden.

Hinzu kommt, dass das Datenschutzrecht ein sehr dynamisches Rechtsgebiet ist, das durch die zunehmende Digitalisierung, aber auch die stärkere Berücksichtigung in der Rechtsprechung immer mehr an Bedeutung gewinnt.

Um all diese Aufgaben im erforderlichen Maß erfüllen und damit die Landeshauptstadt München datenschutzrechtlich optimal aufstellen zu können, müssen für die örtlichen Datenschutzbeauftragten als auch für den behördlichen Datenschutz ausreichend Kapazitäten zur Verfügung stehen. Eventuelle Stellenbedarfe für den Datenschutz sind von den Referaten für ihren Bereich im Rahmen des Eckdatenbeschlussverfahrens anzumelden.

4. Berichte aus den Referaten

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

- Kommunalreferat
- Kulturreferat
- Personal- und Organisationsreferat

Die Stellungnahmen hängen der Bekanntgabe als Anlagen an.

Beteiligung der Referate

Die Stellungnahmen sind der Beschlussvorlage als Anlagen 1 – 3 beigefügt.

Eine Mitzeichnung erfolgte durch das Direktorium, das Personal- und Organisationsreferat, das Referat für Bildung und Sport, das Gesundheitsreferat und die Stadtkämmerei.

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**
   An
   An
   z. K.

   Am