Bayerisches Staatsministerium des
Innern, für Sport und Integration

Arbeitshilfen

zur praktischen Umsetzung der Datenschutz-Grundverordnung, der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei Polizei und Justiz) und des Bayerischen Datenschutzgesetzes für bayerische öffentliche Stellen

Stand: März 2022

Inhalt

1.	**Vorwort**	**5**
2.	**Einführung**	**7**
2.1	Der Anwendungsbereich von DSGVO und der Richtlinie zum Datenschutz bei Polizei und Justiz	7
2.2	Anwendungsbereich des Bundesdatenschutzgesetzes	8
2.3	Der Anwendungsbereich des Bayerischen Datenschutzgesetzes	8
2.4	Schwerpunkt der Änderungen	10
2.4.1	Datenschutzrechtliche Begriffe	10
2.4.2	Neue zentrale Rolle des Verantwortlichen nach der Datenschutz-Grundverordnung	10
2.4.3	Zulässigkeit der Verarbeitung personenbezogener Daten	11
2.4.4	Verfahrensvorschriften	14
2.4.5	Aufgaben und Stellung des / der behördlichen Datenschutzbeauftragten	16
2.5	Wie gehe ich vor, um die richtige Rechtsgrundlage für die Lösung einer datenschutzrechtlichen Frage zu finden?	17
2.6	Welcher praktische Handlungsbedarf besteht?	18
2.6.1	Zuständigkeiten für die am Datenschutz Beteiligten festlegen	18
2.6.2	Den Bestand an Verarbeitungen erfassen	18
2.6.3	Aufgaben und Stellung des / der behördlichen Datenschutzbeauftragten festlegen	18
3.	**Maßnahmenplan für den Verantwortlichen zur Umsetzung der DSGVO**	**19**
4.	**Datenschutz-Geschäftsordnung**	**21**
4.1	Muster einer Datenschutz-Geschäftsordnung	23
4.2	Erläuterungen zur Datenschutz-Geschäftsordnung	30
4.3	Anlage 1 (zu § 2)	38
4.4	Anlage 2 (zu § 6)	39
4.5	Anlage 4 (zu § 10)	43
5.	**Schulungen der Beschäftigten und der behördlichen Datenschutzbeauftragten**	**45**
5.1	Schulung von Beschäftigten	45
5.2	Schulung des / der behördlichen Datenschutzbeauftragten	46
6.	**Das Verzeichnis der Verarbeitungstätigkeiten**	**49**
6.1	Welche öffentlichen Stellen müssen ein Verarbeitungsverzeichnis führen?	50
6.2	Weiterverwendung vorhandener Verfahrensverzeichnisse	50
6.3	Keine Veröffentlichungspflicht, kein Recht auf Einsichtnahme	50

6.4 Muster einer Beschreibung einer Verarbeitungstätigkeit nach Art. 30 Abs. 1 DSGVO und Art. 31 BayDSG 51
6.5 Erläuterungen zum Muster 53

7. Die Informationspflichten des Verantwortlichen nach Art. 13 und 14 DSGVO 59
7.1 Allgemeines 59
7.2 Wann ist zu informieren? 59
7.3 Wann werden personenbezogene Daten „erhoben“? 60
7.4 Ausnahmen von der Informationspflicht 60
7.5 Die Informationspflichten bei der Erhebung bei der betroffenen Person 62
7.5.1 Erhebungen auf Papierformularen 62
7.5.2 Erhebungen im Internet 63
7.5.3 Mündliche Datenerhebungen 63
7.6 Die Informationspflichten bei der Erhebung nicht bei der betroffenen Person 64
7.7 Die Informationspflichten bei einer Zweckänderung 65
7.8 Sonderfall: Informationspflicht bei einer Videoüberwachung 66
7.9 Die Informationspflichten in Art. 13 und 14 DSGVO im Einzelnen 67
7.10 Muster für Datenschutzinformationen 74

8. Datenschutzverletzungen und Datenpannen – was tun? 76
8.1 Was sind Datenschutzverletzungen oder Datenpannen? 76
8.2 Meldepflicht bei der Aufsichtsbehörde, Dokumentationspflicht 77
8.3 Benachrichtigungspflicht an die betroffenen Personen bei hohem Risiko 80
8.4 Interne Meldewege, Sensibilisierung der Mitarbeiterinnen und Mitarbeiter 80
8.5 Konsequenzen aus Auftreten einer Datenschutzverletzung ziehen 82

9. Foto- und Filmaufnahmen 83
9.1 Einleitung 83
9.2 Mustereinwilligungserklärung 85
9.3 Musterhinweis für Veranstaltungen 87

10. Auftragsverarbeitung 88
10.1 Wesentliche Rechtsgrundlagen 88
10.2 Inhaltliche Vorgaben für die Auftragsverarbeitung 89
10.2.1 Auswahl des Auftragsverarbeiters 89
10.2.2 Form des Vertrags zur Auftragsverarbeitung 89
10.2.3 Wesentliche Vertragsinhalte 89
10.3 Gesetzliche Pflichten des Auftragsverarbeiters 91
10.4 Welche Fragen sind zu klären? 92
10.5 Muster einer Vereinbarung zur Auftragsverarbeitung 93

11. Muster einer Vereinbarung zur Regelung gemeinsamer Verantwortlichkeit 103

12. Datenschutz-Folgenabschätzung und Risikoanalyse nach der DSGVO 113

12.1 Wozu dient die Datenschutz-Folgenabschätzung? 113

12.2 Für welche Verarbeitungen ist eine DSFA durchzuführen? 114

12.2.1 Ausnahmen 114

12.2.2 Schwellwertanalyse 116

12.2.3 Regelbeispiele in Art. 35 Abs. 3 DSGVO 117

12.2.4 „Blacklist“ im Sinne von Art. 35 Abs. 4 DSGVO 117

12.2.5 Alt- bzw. Bestandsverfahren 118

12.3 Durchführung der DSFA 119

12.4 Personelle Rahmenbedingungen hinsichtlich der Durchführung 120

12.5 Beteiligung der betroffenen Personen oder ihrer Vertreter 121

12.6 Beteiligung des / der behördlichen Datenschutzbeauftragten 122

12.7 Vorherige Konsultation der Aufsichtsbehörde 122

12.8 Regelmäßige Überprüfung 123

13. Muster einer Zweckvereinbarung für die Zusammenarbeit im Datenschutz 124

14. Muster für ein Impressum und eine Datenschutzerklärung im Internetauftritt einer Behörde 129

14.1 Impressum 129

14.2 Datenschutzerklärung 131

15. Weiterführende Informationen 143

16. Mitwirkende 144

Letzte Änderungen im Dokument:

Dezember 2018:

Überarbeitung Nr. 6, Einfügung Nrn. 7.1 – 7.4 und Nr. 10.

März 2019:

Einfügung von Nr. 7.5.

März 2022:

Überarbeitung Nr. 1 – 4, Nr. 6, Nr. 7, Nr. 10, Nr. 12, Nr. 14, Einfügung Nr. 4.5, Nr. 5, Nr. 7.10, Nr. 8, Nr. 9, Nr. 11, Nr. 15

1. Vorwort

Seit dem 25. Mai 2018 hat die von der Europäischen Union erlassene Datenschutz-Grundverordnung (DSGVO) für die bayerischen Behörden unmittelbare Geltung. Bis zum gleichen Zeitpunkt war auch die Richtlinie (EU) 2016/680 der Europäischen Union (Richtlinie zum Datenschutz bei Polizei und Justiz) in das Recht der Mitgliedstaaten umzusetzen.

Das Datenschutzrecht des Bundes und Bayerns war an die beiden Rechtsakte der EU anzupassen. Denn entgegenstehende Regelungen der Mitgliedsstaaten waren ab diesem Zeitpunkt nicht mehr anzuwenden, soweit der europäische Gesetzgeber den nationalen Gesetzgeber nicht über Öffnungsklauseln in der DSGVO zu der jeweiligen Regelung ermächtigt hat (sogenannter „Anwendungsvorrang des Europarechts“). Der Bund hat insbesondere ein neues Bundesdatenschutzgesetz (BDSG) erlassen und die Datenschutzvorschriften im Zehnten Buch Sozialgesetzbuch (SGB X) und in der Abgabenordnung (AO) neu gefasst. Der bayerische Gesetzgeber hat eine Neufassung des Bayerischen Datenschutzgesetzes (BayDSG) und Anpassungen anderer Gesetze verabschiedet (vgl. GVBl. 2018 S. 230).

Seit dem 25. Mai 2018 gilt damit eine neue Struktur im Datenschutzrecht. Ergänzend zur DSGVO als (außer im Polizei- und Strafrechts-/ Ordnungswidrigkeitenbereich) direkt anwendbarem Recht haben die bayerischen Behörden das neu gefasste BayDSG anzuwenden. Zusätzlich müssen sie – je nach Verwaltungsbereich – weiterhin auch datenschutzrechtliche Fachvorschriften beachten. Trotz der Strukturveränderungen bleiben die wesentlichen materiellen Kernelemente und damit viele bekannte und handhabbare Regelungen wie z. B. zur Zweckbindung und Datenübermittlung erhalten. Gleichwohl brachte die DSGVO Verfahrensänderungen mit sich, die in die Organisationsstrukturen und Verwaltungsabläufe öffentlicher Stellen einzupassen waren. Die DSGVO richtet sich in erster Linie an den für die jeweilige Datenverarbeitung Verantwortlichen. Ihre ordnungsgemäße Umsetzung in bayerischen öffentlichen Stellen erfordert ein umfassendes Zusammenspiel von Organisationsverantwortlichen, IT-Beauftragten, Fachabteilungen und der / dem Datenschutzbeauftragten[1] als den zentralen Datenschutzexperten vieler Organisationseinheiten.

Die vorliegenden Arbeitshilfen sollen bayerische öffentliche Stellen bei der ordnungsgemäßen Durchführung des Datenschutzrechts unterstützen. Sie wurden mit Unterstützung einer Arbeitsgruppe aus Vertretern der staatlichen und kommunalen Datenschutzpraxis und unter

[1] Aufgrund der Vielzahl weiblicher Datenschutzbeauftragten wird für deren Bezeichnung im Folgenden die Paarform verwendet. Im Übrigen wird sich an den Formulierungen der DSGVO orientiert.

der Beteiligung des Bayerischen Landesbeauftragten für den Datenschutz und der Kommunalen Spitzenverbände erstellt und weiterentwickelt.

Wegen der Vielzahl der mit einer grundlegenden Rechtsreform unvermeidbar verbundenen Fragestellungen werden die Arbeitshilfen kontinuierlich überprüft und bei Bedarf fortgeschrieben.

Die neueste Aktualisierung der Arbeitshilfen, Stand März 2022, enthält

- ein Musterinhaltsverzeichnis für den Datenschutzbericht,
- Hinweise zur Schulung von Beschäftigten und des / der behördlichen Datenschutzbeauftragten,
- ein Muster für Informationspflichten nach Art. 13 und 14 DSGVO
- ein neues Kapitel zu Datenschutzverletzungen und Datenpannen und den daraus resultierenden Meldepflichten nach Art. 33 und 34 DSGVO,
- Hinweise zu Foto- und Filmaufnahmen sowie eine Mustereinwilligungserklärung und einen Musterhinweis für Veranstaltungen,
- ein Muster einer Vereinbarung gemeinsamer Verantwortlichkeit
- eine grundsätzliche Überarbeitung und Fortschreibung des Kapitels zur Datenschutz-Folgenabschätzung

Für den Bereich der Bayerischen Polizei werden gesonderte Hilfestellungen bereitgestellt.

2. Einführung

2.1 Der Anwendungsbereich von DSGVO und der Richtlinie zum Datenschutz bei Polizei und Justiz

Der Anwendungsbereich der DSGVO und der Richtlinie zum Datenschutz bei Polizei und Justiz schließen sich gegenseitig aus (Art. 2 Abs. 2 Buchst. d DSGVO):

- Die DSGVO gilt unmittelbar für alle öffentlichen Stellen, soweit diese keine Tätigkeit im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz ausüben.
- Die Richtlinie zum Datenschutz bei Polizei und Justiz gilt für die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Betroffen sind die Polizei, die Gerichte in Strafsachen und die Staatsanwaltschaften, die Strafvollstreckungs- und Justizvollzugsbehörden, die Behörden des Maßregelvollzugs und alle Behörden bei der Verfolgung und Ahndung von Ordnungswidrigkeiten.
- Nach Art. 2 und Art. 28 Abs. 2 und 3 BayDSG wird auch in diesem Bereich weitgehend auf die Anwendung der Vorschriften der DSGVO verwiesen, um Abgrenzungsprobleme zwischen dem Geltungsbereich der Richtlinie und der DSGVO zu vermeiden. Allerdings enthält die Strafprozessordnung (StPO) – und im Falle der Polizei auch das Polizeiaufgabengesetz (PAG) – vorrangige Sondervorschriften für Polizei, Staatsanwaltschaften sowie alle Behörden bei der Ordnungswidrigkeitenverfolgung und -ahndung. Zu beachten ist insbesondere, dass sowohl die Informationspflichten der Art. 13 und 14 DSGVO als auch die Betroffenenrechte gemäß Art. 15 ff. DSGVO nicht für den Bereich der Ordnungswidrigkeitenverfolgung und -ahndung gelten, vgl. Art. 28 Abs. 2 und 3 BayDSG. So findet sich in Art. 28 Abs. 2 BayDSG keine Verweisung auf Kapitel III der Datenschutz-Grundverordnung, wodurch die Art. 12 bis 23 DSGVO insgesamt von einer Anwendung ausgenommen sind. In Art. 28 Abs. 3 Nr. 2 BayDSG wird Teil 2 Kapitel 3 des Bayerischen Datenschutzgesetzes - Rechte der betroffenen Person - ebenfalls vollumfänglich ausgeschlossen. Hintergrund ist, dass die Informationspflichten sowie die Betroffenenrechte, deren Gewährleistung auch die Richtlinie zum Datenschutz bei Polizei und Justizfordert (in deren Art. 12 ff.), in den jeweiligen Fachgesetzen geregelt sind. Für den Bereich der Ordnungswidrigkeitenverfahren ist vor allem **§ 500 StPO** (in Kraft seit dem 26. November 2019, eingeführt durch Gesetz vom 20. November 2019 [BGBl. I S. 1724]) von Bedeutung. Dieser ist über die Verweisung in § 46 Abs. 1 OWiG anwendbar. Konsequenterweise müssen

über die Verweisung nach § 500 Abs. 1 StPO in Ordnungswidrigkeitenverfahren neben der Strafprozessordnung (welche über § 46 Abs. 1 OWiG Anwendung findet) auch die §§ 45 ff. Bundesdatenschutzgesetz (BDSG) beachtet werden. Dies gilt allerdings nur, soweit die Strafprozessordnung nicht etwas anderes bestimmt, vgl. § 500 Abs. 2 Nr. 1 StPO.

2.2 Anwendungsbereich des Bundesdatenschutzgesetzes

Das BDSG gilt für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes sowie öffentliche Stellen der Länder, soweit diese Bundesrecht ausführen oder als Organe der Rechtspflege außerhalb des Verwaltungsbereichs tätig werden und der Datenschutz nicht durch Landesgesetz geregelt ist (§ 1 Abs. 1 Satz 1 BDSG).

Weiter findet das BDSG auf nicht öffentliche Stellen Anwendung (§ 1 Abs. 1 Satz 2 BDSG). Zu beachten sind im Übrigen die Ausführungen unter 2.1.

2.3 Der Anwendungsbereich des Bayerischen Datenschutzgesetzes

Wie bereits dargestellt, kann das BayDSG in Umsetzung der DSGVO nur in den Bereichen Regelungen treffen, in denen die DSGVO dafür Öffnungsklauseln enthält. Zur besseren Lesbarkeit ist unter jedem Artikel des BayDSG angegeben, welche Vorschrift der DSGVO damit ausgestaltet werden soll.

Das BayDSG gilt für die Behörden und sonstigen öffentlichen Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts (Art. 1 Abs. 1 BayDSG).

Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht öffentliche Stellen – ergänzend zu den Vorschriften der DSGVO also insbesondere die Vorschriften des allgemeinen Teils des BDSG, d.h. ohne §§ 45 ff. BDSG, entsprechend. Die Zuständigkeit des Bayerischen Landesbeauftragten für den Datenschutz für die Aufsicht bleibt hiervon unberührt (Art. 1 Abs. 3 Satz 2 BayDSG). Zudem kann der Bayerische Landesbeauftragte gegen diese Stellen – anders als gegen andere öffentliche Stellen – ein Bußgeld verhängen (Art. 22 BayDSG i.V.m. Art.83 Abs. 7 DSGVO).[2]

---

[2] Dazu die Aktuelle Kurz-Information (im Folgenden AKI) 17 des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/aki17.html.

Wettbewerbsunternehmen sind beispielsweise die kommunalen Energieversorgungs- und Verkehrsbetriebe sowie Krankenhäuser. Keine Wettbewerbsunternehmen in diesem Sinne sind die Einrichtungen der Kinderbetreuung, Schulen und Hochschulen.

Soweit möglich, hat der Bayerische Gesetzgeber den von der DSGVO eröffneten Regelungsspielraum genutzt. Das betrifft auch Regelungen zum Anwendungsbereich. Wesentliche Regelungen des BayDSG sind insoweit:

- Regelungen zum Datenschutz in Bereichen, die weder der DSGVO noch der Richtlinie zum Datenschutz bei Polizei und Justiz unterliegen. Für diese Bereiche wird weitgehend auf die Regelungen der DSGVO verwiesen (Art. 2 BayDSG).
- Regelungen zur Verarbeitung personenbezogener Daten zur Vorbereitung und Durchführung staatlicher und kommunaler Auszeichnungen und Ehrungen. (Art. 27 BayDSG).
- Regelungen zur Umsetzung allgemeiner und organisationsrechtlicher Anforderungen der Richtlinie zum Datenschutz bei Polizei und Justiz in das bayerische Landesrecht (Art. 28 bis 37 BayDSG). Nach Art. 2 und Art. 28 Abs. 2 und 3 BayDSG wird auch in diesem Bereich weitgehend auf die Anwendung der Vorschriften der DSGVO verwiesen. Das PAG und die StPO enthalten vorrangige Sondervorschriften für die Polizei sowie die StPO für die Staatsanwaltschaften.

  Auf die Tätigkeit der Gemeinden und sonstigen Behörden außerhalb des Polizei- und Strafverfolgungsbereichs sind die Art. 28 bis 37 BayDSG nur dann anwendbar, wenn Ordnungswidrigkeiten verfolgt oder geahndet werden und keine spezialgesetzlichen Vorschriften (z. B. im OWiG) bestehen (Art. 28 Abs. 1 Satz 2 BayDSG). Zu beachten ist, dass seit Ende November 2019 die StPO in § 500 StPO einen Verweis auf die Vorschriften der §§ 45 ff. BDSG enthält. Über § 46 OWiG ist dieser Verweis auch für Behörden, die Ordnungswidrigkeiten verfolgen, von Relevanz (siehe bereits unter 2.1).

- Die in Art. 38 BayDSG enthaltene Regelung zur Datenverarbeitung zu journalistischen, künstlerischen und literarischen Zwecken gilt grundsätzlich auch für nicht öffentliche Stellen.

2.4 Schwerpunkt der Änderungen

2.4.1 Datenschutzrechtliche Begriffe

Art. 4 DSGVO enthält Begriffsbestimmungen, die teils den schon früher im Datenschutzrecht verwendeten Begriffen entsprechen, sich teilweise aber auch von diesen unterscheiden. So umfasst der Begriff der „Verarbeitung“ nach Art. 4 Nr. 2 DSGVO jeglichen Umgang mit personenbezogenen Daten; die Norm enthält eine umfassende beispielhafte Aufzählung von Verarbeitungsschritten. Art. 4 DSGVO gilt auch bei präventivpolizeilichem Tätigwerden (Art. 28 Abs. 2 Satz 1 Nr. 1 BayDSG). Für die Verfolgung von Ordnungswidrigkeiten finden sich entsprechende Bestimmungen in § 46 BDSG.

2.4.2 Neue zentrale Rolle des Verantwortlichen nach der Datenschutz-Grundverordnung

Die DSGVO weist dem „Verantwortlichen“ bei der Verarbeitung personenbezogener Daten eine zentrale Rolle zu. „Verantwortlicher“ ist nach Art. 4 Nr. 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Art. 26 DSGVO sieht darüber hinaus die gemeinsame Verantwortlichkeit mehrerer Stellen vor, wenn diese gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.

Art. 3 Abs. 2 BayDSG stellt klar, dass Verantwortlicher für die Verarbeitung personenbezogener Daten im Sinne der DSGVO die für die Verarbeitung zuständige öffentliche Stelle ist, soweit nichts anderes[3] bestimmt ist. Im öffentlichen Bereich ist damit weiterhin die Behörde oder sonstige öffentliche Stelle gemeint (z. B. die Gemeinde oder das Landratsamt), die eine Datenverarbeitung zur Erfüllung ihrer Aufgaben durchführt.

[3] So etwa im Anwendungsbereich des Sozialgesetzbuchs, siehe § 67 Abs. 4 Satz 2 SGB X. Handelt es sich bei einem Sozialleistungsträger um eine Gebietskörperschaft, ist jede Organisationseinheit, die eine Aufgabe nach einem der Besonderen Teile des Sozialgesetzbuchs wahrnimmt, jeweils als eigener Verantwortlicher einzuordnen (ausführlicher mit Beispiel, siehe Arbeitspapier des Bayerischen Landesbeauftragten für den Datenschutz „Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung“, Stand: 1. März 2021, Rn. 17, online abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf).

Der Verantwortliche hat sicherzustellen, dass

- die materiellen Vorschriften über die Zulässigkeit der Verarbeitung personenbezogener Daten durch die öffentliche Stelle eingehalten werden,
- die Verfahrensvorschriften der DSGVO beachtet werden. Dies gilt z. B. für die Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO, die Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und die Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und Art. 14 BayDSG sowie die Vorgaben des Art. 28 DSGVO bei Einschaltung eines Auftragsverarbeiters,
- die datenschutzrechtlichen Informationspflichten nach Art. 13 und 14 DSGVO i.V.m. Art. 9 BayDSG und die sonstigen Rechte der Betroffenen beachtet werden (z. B. das Auskunftsrecht nach Art. 15 DSGVO und Art. 10 BayDSG, das Recht auf Löschung nach Art. 17 DSGVO und das Widerspruchsrecht nach Art. 21 DSGVO) und
- geeignete technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten getroffen werden (Art. 24 Abs. 1 und Art. 32 DSGVO), bspw. in Form von Datenschutzrichtlinien oder sonstigen Datenschutzanweisungen.

Wer die vielfältigen Pflichten des Verantwortlichen innerhalb der öffentlichen Stelle konkret erfüllt, ist von der Leitung der öffentlichen Stelle festzulegen. Regelmäßig ist dabei zwischen zentralen Ansprechpartnern für IT, Organisation und Datenschutz sowie den Fachabteilungen zu unterscheiden. Außerdem sind die Verwaltungsabläufe so zu gestalten, dass die Einhaltung datenschutzrechtlicher Bestimmungen sichergestellt ist. Die Letztverantwortlichkeit verbleibt bei der Behördenleitung. **Kapitel 4 dieser Arbeitshilfen** enthält ein Muster für eine Datenschutz-Geschäftsordnung, in der diese Aufgabenzuweisungen und Verfahrensabläufe beschrieben werden.

2.4.3 Zulässigkeit der Verarbeitung personenbezogener Daten

Öffentliche Stellen bedürfen für die Datenverarbeitung einer Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO). Hierbei dürften zunächst regelmäßig die Regelungen des Art. 6 Abs. 1 Unterabs. 1 Buchst. c, e, Abs. 3 Satz 1 Buchst. b DSGVO einschlägig sein. Insoweit ist allerdings darauf hinzuweisen, dass diese selbst **keine Befugnis** zur Datenverarbeitung darstellen, sondern **nur eine Öffnungsklausel** für die Mitgliedstaaten. Diese erlaubt es dem nationalen Gesetzgeber, die Datenverarbeitung durch öffentliche Stellen zu regeln. Hiervon hat der bayerische Gesetzgeber im Rahmen des BayDSG für öffentliche Stellen insbesondere durch Erlass der **allgemeinen Datenverarbeitungsbefugnisse nach Art. 4 und 5 BayDSG** Gebrauch gemacht.

Die allgemeinen Datenverarbeitungsbefugnisse können jedoch durch **vorrangige bereichsspezifische Befugnisse** verdrängt werden.
So gibt es beispielsweise im Anwendungsbereich des Sozialgesetzbuchs spezialgesetzliche Regelungen wie etwa in § 69 SGB X.[4]

Neben den vorrangigen fachgesetzlichen Befugnisnormen, die sich beispielsweise im Schul-, Arbeits- und Krankenhausrecht finden lassen, enthält der bereits erwähnte Art. 4 Abs. 1 BayDSG eine allgemeine Befugnisnorm für die Verarbeitung personenbezogener Daten durch bayerische öffentliche Stellen:
„Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist."
Für die Datenübermittlung an andere öffentliche Stellen gibt es in Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG eine allgemeine Verarbeitungsbefugnis:
„Eine Übermittlung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist."

Selbst wenn keine spezialgesetzliche Rechtsgrundlage existiert, kann ein Rückgriff auf die allgemeinen Datenverarbeitungsbefugnisse jedoch ggf. ausgeschlossen sein, weil der Gesetzgeber eine bewusste Lücke im Fachrecht vorgesehen hat.

Ergänzend kommen als Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch bayerische öffentliche Stellen Art. 6 Abs. 1 Unterabs. 1 Buchst. a (Einwilligung[5] der betroffenen Person, vgl. dazu allerdings einschränkend DSGVO-Erwägungsgrund 43), Buchst. b (Verarbeitung für die Erfüllung eines Vertrags) oder Buchst. d DSGVO (Verarbeitung, um lebenswichtige Interessen der betroffenen Person oder anderer Personen zu schützen) in Betracht. Diese Regelungen enthalten (anders als die Buchst. c und e) unmittelbar geltende Befugnisnormen, die keiner Umsetzung durch den nationalen Gesetzgeber bedürfen.

Eine besondere Einschränkung gilt dann, wenn besondere Kategorien personenbezogener Daten (sog. **sensible Daten**) gemäß Art. 9 Abs. 1 DSGVO betroffen sind. Zu beachten ist,

---

[4] Allgemein zum Datenschutz im Sozialleistungsbereich LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.html.
[5] Detaillierte Informationen zu den Voraussetzungen einer wirksamen Einwilligung finden sich in der Orientierungshilfe „Die Einwilligung nach der Datenschutzgrundverordnung" abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf.

dass für die Verarbeitung solcher Daten immer zusätzlich zu einer Verarbeitungsbefugnis nach Art. 6 Abs. 1 DSGVO ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO erfüllt sein muss. Für bestimmte Konstellationen ergibt sich eine solche Ausnahme von dem Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO bereits unmittelbar aus Art. 9 Abs. 2 DSGVO, für andere Konstellationen ist eine ausdrückliche Regelung im nationalen Recht erforderlich, wie sie allgemein formuliert Art. 8 Abs. 1 Satz 1 BayDSG bereithält. Etwaige Spezialregelungen im jeweiligen Bereich gehen allerdings diesen Vorschriften wiederum vor (beispielsweise Art. 30, 31 Gesundheitsdienst- und Verbraucherschutzgesetz oder Art. 47 Bayerisches Rettungsdienstgesetz sowie Art. 27 Bayerisches Krankenhausgesetz). Schließlich enthält Art. 10 DSGVO Einschränkungen für Daten aus Strafverfahren.

Neben den jeweiligen Erlaubnistatbeständen müssen bei Datenverarbeitungen zu anderen Zwecken, als denen, die der Datenerhebung zu Grunde lagen, zusätzlich die Voraussetzungen für eine **Zweckänderung** gem. Art. 6 Abs. 4 DSGVO und Art. 6 BayDSG beachtet werden.[6]

Bei der Prüfung der Zulässigkeit einer **Datenübermittlung** ist außerdem zu beachten, dass regelmäßig eine Datenverarbeitung sowohl bei der öffentlichen Stelle, die Daten übermittelt, als auch bei der öffentlichen Stelle, die Daten erhält (insoweit: regelmäßig eine Datenerhebung), vorliegt. Dies betrifft insbesondere Datenübermittlungen zwischen öffentlichen Stellen aufgrund von Auskunftsersuchen (sog. Frage – Antwort – Konstellationen). Sowohl nach der DSGVO als auch nach dem sog. Doppeltürmodell des Bundesverfassungsgerichts[7] benötigen beide öffentliche Stellen in diesen Konstellationen jeweils eine eigene Rechtsgrundlage für die Datenverarbeitung (also für die Übermittlung bzw. für die Erhebung).

Schließlich setzt die Zulässigkeit der Datenverarbeitung neben dem bereits erwähnten Erfordernis einer Rechtsgrundlage freilich voraus, dass auch die weiteren Vorgaben des Datenschutzrechts, etwa die allgemeinen Grundsätze des Art. 5 Abs. 1 DSGVO einschließlich der Zweckbindung (vgl. Art. 6 Abs. 4 DSGVO, Art. 6 BayDSG) sowie die sog. Datensicherheit nach Art. 32 DSGVO, beachtet werden.

---

[6] Dazu Überblick des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/ueberblick.pdf S. 13.
[7] BVerfGE 130, 151, 184.

2.4.4 Verfahrensvorschriften

Die DSGVO enthält formelle Vorgaben, welche insbesondere durch den Verantwortlichen, teilweise auch durch einen Auftragsverarbeiter, umgesetzt werden müssen. Insbesondere muss ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO geführt werden, die Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO müssen beachtet werden und teilweise muss eine Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und Art. 14 BayDSG durchgeführt werden. Art. 28 DSGVO enthält formelle Vorgaben für die Einschaltung eines Auftragsverarbeiters.

- Das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO ist vom Verantwortlichen – und (soweit vorhanden) gemäß Art. 30 Abs. 2 DSGVO zusätzlich auch vom Auftragsverarbeiter – zu führen. **Kapitel 6 dieser Arbeitshilfen enthält dazu nähere Ausführungen und ein Muster.**
- Dem / der behördlichen Datenschutzbeauftragten ist nach Art. 12 Abs. 1 Satz 1 Nr. 2 BayDSG Gelegenheit zur Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens zu geben, mit dem personenbezogene Daten verarbeitet werden. Hinzuweisen ist darauf, dass die datenschutzrechtliche Freigabe durch den / die behördlichen Datenschutzbeauftragten seit 25. Mai 2018 entfallen ist.
- Vor dem Einsatz (voraussichtlich) „hochrisikoträchtiger“ und eingriffsintensiver Verarbeitungen ist das Verfahren einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO[8] durchzuführen (vgl. auch Art. 14 BayDSG). Der Bayerische Landesbeauftragte für den Datenschutz hat hierzu ergänzend eine – nicht abschließende – Liste von Verarbeitungen veröffentlicht, für die ein solches Verfahren durchzuführen ist („Bayerische Blacklist“[9]). Für Datenverarbeitungen, die am 25. Mai 2018 bereits durchgeführt wurden (sog. Bestandsverfahren) und in die Kategorie „hochrisikoträchtiger“ Verarbeitungen im Sinne des Art. 35 DSGVO einzustufen wären, ist eine Datenschutz-Folgenabschätzung nach den unter 12.2.5 dargestellten Voraussetzungen durchzuführen.
  Kapitel 12 dieser Arbeitshilfen enthält nähere Ausführungen zu diesem Verfahren.

---

[8] Dazu Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz, https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf sowie Working Paper 248 rev. 01 der Artikel 29-Gruppe, https://www.ldi.nrw.de/mainmenu_Service/submenu_Newsarchiv/Inhalt/Leitlinien_der_Art__29-Gruppe_zur_EU_DSGVO/wp248-rev_01.pdf. Weitere Hilfestellungen finden sich auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter https://www.datenschutz-bayern.de/dsfa/.

[9] Abrufbar unter: https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf.

- Der Bayerische Landesbeauftragte für den Datenschutz hat als Aufsichtsbehörde für die bayerischen öffentlichen Stellen verstärkte Befugnisse bis hin zur Untersagung einzelner Datenverarbeitungen (Art. 57 und 58 DSGVO, Art. 16 Abs. 4 BayDSG) erhalten. Er ist von allen öffentlichen Stellen umfassend zu unterstützen. Der Bayerische Landesbeauftragte für den Datenschutz hat neben den Befugnissen aus der DSGVO das Recht, Datenschutzverstöße, einschließlich einer mangelnden Unterstützung seiner Tätigkeit, förmlich zu beanstanden (Art. 16 Abs. 4 BayDSG). Eine gewisse Einschränkung dieser Befugnisse sieht Art. 34 Abs. 2 BayDSG im Rahmen von Strafverfahren vor; diese Einschränkung gilt allerdings insb. nicht für Ordnungswidrigkeitenverfahren.
- Verletzungen des Schutzes personenbezogener Daten (Datenpannen), die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, sind dem Bayerischen Landesbeauftragten für den Datenschutz in der Regel binnen 72 Stunden zu melden und alle relevanten Informationen hierzu einschließlich getroffener Abhilfemaßnahmen zu dokumentieren (Art. 33 DSGVO). Der Bayerische Landesbeauftragte für den Datenschutz stellt dafür ein Meldeformular auf seiner Internetseite unter https://www.datenschutz-bayern.de/service/data_breach.html zur Verfügung.[10] Geht von der Verletzung voraussichtlich ein *hohes* Risiko für die Rechte und Freiheiten natürlicher Personen aus, sind auch die betroffenen Personen zu benachrichtigen (Art. 34 DSGVO). Für Sozialbehörden ist außerdem § 83a SGB X zu beachten.[11] **Kapitel 8 enthält nähere Ausführungen zu Datenschutzverletzungen bzw. Datenpannen sowie zu den Pflichten nach Art. 33 und 34 DSGVO**.
- Die von der Datenverarbeitung betroffene Person hat verschiedene Rechte.
  Dies gilt insbesondere für die Information der betroffenen Person bei einer Datenerhebung (z. B. mittels eines Formulars). **Kapitel 7 dieser Arbeitshilfen enthält dazu nähere Ausführungen und Beispiele für mögliche Formulierungen**.
  Die DSGVO gibt der betroffenen Person ferner weitere Rechte wie das Recht auf Auskunft (Art. 15 DSGVO, Art. 10 BayDSG), welche durch ablauforganisatorische Vorgaben wie beispielsweise eine in der Regel einmonatige Beantwortungsfrist (Art. 12 Abs. 3 und 4 DSGVO) gestärkt werden.[12]

---

[10] Einzelheiten können auf der Internetpräsenz des LfD unter https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf sowie in den Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 (WP 250 rev.01), https://www.datenschutz-bayern.de/datenschutzreform2018/wp250rev01_de.pdf, außerdem für den Richtlinienbereich (2016/680) in AKI 9, https://www.datenschutz-bayern.de/datenschutzreform2018/aki09.html nachgelesen werden.

[11] Dazu AKI 18 des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/aki18.html sowie allgemein zum Datenschutz im Sozialleistungsbereich https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.html.

[12] Ausführlich dazu Orientierungshilfe LfD, https://www.datenschutz-bayern.de/verwaltung/OH_Recht_auf_Auskunft.pdf.

Das Recht auf Auskunft der betroffenen Person umfasst auch das Recht auf die Bereitstellung einer kostenlosen Kopie (Art. 15 Abs. 3 DSGVO).

2.4.5 Aufgaben und Stellung des / der behördlichen Datenschutzbeauftragten

Nach Art. 37 Abs. 1 Buchst. a DSGVO hat jede öffentliche Stelle eine(n) Datenschutzbeauftragte(n) zu benennen. Die Stellung und die Aufgaben des / der behördlichen Datenschutzbeauftragten ergeben sich aus Art. 37 bis 39 DSGVO und Art. 12, 24 Abs. 5 BayDSG.

Der / die behördliche Datenschutzbeauftragte ist auf der Grundlage seiner / ihrer beruflichen Qualifikation und insbesondere seines / ihres datenschutzrechtlichen Fachwissens zu benennen (Art. 37 Abs. 5 DSGVO). Dazu gehören Rechtskenntnisse bezüglich der einschlägigen datenschutzrechtlichen Regelungen sowie Grundkenntnisse der eingesetzten IuK-Technik.

Der / die behördliche Datenschutzbeauftragte ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden (Art. 38 Abs. 1 DSGVO). Er / Sie muss Zugang zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO erhalten (Art. 12 Abs. 1 Satz 1 Nr. 1 BayDSG).

Der / die behördliche Datenschutzbeauftragte ist berechtigt und verpflichtet, der Behördenleitung unmittelbar zu berichten (Art. 38 Abs. 3 Satz 3 DSGVO). Wesentliche Aufgaben des / der behördlichen Datenschutzbeauftragten sind insbesondere

- die Unterrichtung und Beratung des Verantwortlichen über dessen datenschutzrechtliche Pflichten,
- die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften,
- die Zusammenarbeit mit der Aufsichtsbehörde,
- die Stellungnahme zu einem beabsichtigten Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden
- die Stellungnahme zu geplanten Videoüberwachungsanlagen und
- die Beratung des Verantwortlichen bei Datenschutz-Folgenabschätzungen und Anlaufstelle für betroffene Personen[13].

(Art. 39 Abs. 1 DSGVO, Art. 12 Abs. 1 Nr. 2 und Art. 24 Abs. 5 BayDSG).[14]

---

[13] Dazu AKI 12 des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/aki12.html.
[14] Ausführlich Orientierungshilfe des LfD, https://www.datenschutz-bayern.de/6/bdsb.pdf sowie Leitlinien in Bezug auf Datenschutzbeauftragte ("DSB"), WP 243 rev.01, https://www.datenschutz-bayern.de/datenschutzreform2018/wp243rev01_de.pdf.

Die Führung des Verzeichnisses der Verarbeitungstätigkeiten und die Durchführung der Datenschutz-Folgenabschätzung sind keine gesetzlichen Pflichtaufgaben des / der behördlichen Datenschutzbeauftragten.

2.5 Wie gehe ich vor, um die richtige Rechtsgrundlage für die Lösung einer datenschutzrechtlichen Frage zu finden?

Den Einstieg in die Frage der Zulässigkeit einer Datenverarbeitung bildet stets die DSGVO. Auf Grundlage und im Rahmen der dort vorgesehenen Öffnungsklauseln zu den einzelnen, bereits oben dargestellten Prüfungskomplexen (insbesondere generelle Rechtsgrundlage nach Art. 6 Abs. 1 bis 3 DSGVO, Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO, Zweckänderung nach Art. 6 Abs. 4 DSGVO) ist zu prüfen, ob das Fachrecht eine einschlägige Regelung der Verarbeitung (also eine gesetzliche Befugnis zur Datenverarbeitung) enthält. Wenn dies nicht der Fall ist, ist zu prüfen, ob auf Art. 4 Abs. 1 bzw. Art. 5 Abs. 1 BayDSG als Auffanggesetz zurückgegriffen werden kann, oder ob ggf. eine bewusste Lücke im Fachrecht vorliegt, welche den Rückgriff auf die allgemeinen Datenverarbeitungsbefugnisse ausschließt.

Die Regelungen der DSGVO und die Regelungen im Allgemeinen sowie gegebenenfalls auch im bereichsspezifischen nationalen Datenschutzrecht (sei es im Landes- oder Bundesrecht) sind im Zusammenhang zu lesen und anzuwenden.

Das BayDSG macht in den Überschriften verschiedener Vorschriften deutlich, auf welche Artikel der DSGVO sie sich beziehen.

Für Polizeibehörden und sonstige Stellen bei der Verfolgung von Ordnungswidrigkeiten empfiehlt sich, zu Beginn einen Blick in Art. 28 BayDSG zu werfen, der die in Art. 2 BayDSG angeordnete umfassende Geltung der DSGVO teilweise wieder einschränkt. Dabei muss auf den unterschiedlichen Wortlaut in Abs. 2 (Vorschriften der DSGVO finden „nur“ Anwendung) und Abs. 3 (Vorschriften des BayDSG finden „keine“ Anwendung) geachtet werden. Weitere, insbesondere materiell-rechtliche Regelungen zur Umsetzung der Richtlinie zum Datenschutz bei Polizei und Justiz finden sich im Fachrecht z. B. im PAG, im BayStVollzG, der StPO oder im OWiG sowie insbesondere über § 500 StPO im BDSG.

2.6 Welcher praktische Handlungsbedarf besteht?

2.6.1 Zuständigkeiten für die am Datenschutz Beteiligten festlegen

Die DSGVO und das BayDSG weisen dem Verantwortlichen, also der öffentlichen Stelle, bestimmte Aufgaben zu. Es ist festzulegen, wer die Pflichten des Verantwortlichen nach der DSGVO und dem BayDSG in der Behörde erfüllt. Davon abzugrenzen sind die Aufgaben und Befugnisse des / der behördlichen Datenschutzbeauftragten. **Kapitel 4 dieser Arbeitshilfen enthält ein Muster für eine Datenschutz-Geschäftsordnung.**

2.6.2 Den Bestand an Verarbeitungen erfassen

Das Verzeichnis der Verarbeitungstätigkeiten ist zentraler Ausgangspunkt für die Erfüllung der Aufgaben des Verantwortlichen, des / der behördlichen Datenschutzbeauftragten und der Aufsichtsbehörde: dieser ist das Verzeichnis auf Anfrage zur Verfügung zu stellen, Art. 30 Abs. 4 DSGVO. Als Ausgangspunkt für die Erstellung dieses Verzeichnisses und die Ermittlung der einzelnen Verarbeitungstätigkeiten kann das bisher geführte Verfahrensverzeichnis herangezogen werden. **Kapitel 6 dieser Arbeitshilfen enthält ein Muster für ein Verzeichnis der Verarbeitungstätigkeiten.**

2.6.3 Aufgaben und Stellung des / der behördlichen Datenschutzbeauftragten festlegen

Die Aufgaben und Stellung des / der behördlichen Datenschutzbeauftragten ergeben sich unmittelbar aus Art. 37 bis 39 DSGVO und Art. 12 BayDSG.

Besteht über die gesetzlich zugewiesenen Aufgaben hinaus ein Bedarf, dem / der Datenschutzbeauftragten weitere Aufgaben, beispielsweise die Führung des Verzeichnisses der Verarbeitungstätigkeiten, nach Art. 38 Abs. 6 DSGVO zu übertragen, so muss dies ausdrücklich geregelt werden.

3. Maßnahmenplan für den Verantwortlichen zur Umsetzung der DSGVO

Die folgende Tabelle enthält einen Überblick über die Maßnahmen zur Umsetzung der datenschutzrechtlichen Verpflichtungen in bayerischen Behörden und sonstigen öffentlichen Stellen.

Maßnahmen	Anmerkungen
1. Festlegung, wer in der Behörde welche Aufgaben nach der DSGVO übernimmt.	
2. Benennung / Bestellung eines / einer behördlichen Datenschutzbeauftragten (bDSB) und einer Stellvertretung gem. Art. 37 DSGVO und Art. 12 BayDSG	*(1) Öffentliche Stellen haben in jedem Fall eine(n) bDSB zu benennen (Art. 37 Abs. 1 Buchst. a DSGVO)* *(2) Auswahl geeigneter Personen im Sinne von Art. 37 Abs. 5 DSGVO.* *(3) DSB muss nicht zwingend ein(e) Beschäftigte(r) des Verantwortlichen sein.* *(4) Die Benennung eines/r gemeinsamen bDSB / Stellvertretung für mehrere Verantwortliche ist möglich (Art. 37 Abs. 3 DSGVO; **siehe hierzu auch das Muster einer Zweckvereinbarung für die Zusammenarbeit im Datenschutz in Kapitel 13 dieser Arbeitshilfen**).* *(5) Bestellung/Benennung dokumentieren, ggf. zuvor eine Benennung vom Gemeinde-/ Stadtrat beschließen lassen. **Kapitel 4 dieser Arbeitshilfen enthält ein Muster für ein Benennungsschreiben.*** *(6) Aufgabenbereich des/der DSB festlegen (Art. 39 Abs. 1 DSGVO, Art. 12 Abs. 1 BayDSG, **Kapitel 4 dieser Arbeitshilfen enthält eine Übersicht zu den Aufgaben des/der DSB**).* *(7) Kontaktdaten des/der DSB veröffentlichen (Art. 37 Abs. 7 DSGVO) und der Aufsichtsbehörde melden.*[15]

[15] Internetformular https://www.datenschutz-bayern.de/service/bdsb.html.

3. Erlass einer Geschäftsordnung zum Datenschutz	*Datenschutzrechtliche Zuständigkeiten müssen konkret einzelnen Organisationseinheiten oder Personen innerhalb der öffentlichen Stelle zugewiesen und notwendige Verfahrensabläufe festgelegt werden.* ***Näheres hierzu im Kapitel 4 dieser Arbeitshilfen.***
4. Erstellen des Verzeichnisses der Verarbeitungstätigkeiten (VV) gem. Art. 30 DSGVO	*(1) Ausgangspunkt kann das bisherige Verfahrensverzeichnis für automatisierte Verfahren sein.* *(2) Verwendung des Formblatts* ***Siehe Kapitel 6 dieser Arbeitshilfen.***
5. Erstellen von Datenschutzhinweisen auf Vordrucken und im Internet (Art. 12, 13 und 14 DSGVO)[16]	***Siehe hierzu Kapitel 7 und 14 dieser Arbeitshilfen zu den Informationspflichten.***
6. Abschluss von Verträgen mit geeigneten Auftragsverarbeitern	*Die formellen Vorgaben nach Art. 28 und 29 DSGVO müssen beachtet werden.* ***Siehe Kapitel 10 dieser Arbeitshilfen**.*
7. (Normen-) Screening	*Überprüfung (soweit noch nicht geschehen) von kommunalen Satzungen oder Verordnungen sowie von Dienstvereinbarungen und sonstigen Dienstanweisungen, ob diese mit der DSGVO vereinbar sind.*
8. Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, insbesondere sind Verfahren auf datenschutzfreundliche Voreinstellungen zu überprüfen	*Abstimmung der Schnittmengen mit der IT-Sicherheit:* *Vermeidung von doppelten Strukturen hinsichtlich des „technischen" Datenschutzes; bei technisch-organisatorischen Maßnahmen kann auf ein vorhandenes IT-Sicherheitskonzept hingewiesen werden, wenn dieses die datenschutzrechtlichen Anforderungen erfüllt.*

[16] Vgl. Fragen und Antworten des LfD, Arbeitspapier des LfD zu offenkundig unbegründeten und exzessiven Anträgen (Art. 12 Abs. 5 DSGVO), https://www.datenschutz-bayern.de/datenschutzreform2018/AP_ExzessiveAntraege.pdf sowie speziell für die Datenverarbeitung im Sozialleistungsbereich auch LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.html.

4. Datenschutz-Geschäftsordnung

Die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften trägt nach der DSGVO nicht der / die behördliche Datenschutzbeauftragte, sondern der „Verantwortliche“ (vgl. hierzu Einführung unter 2.4.2). Der Verantwortliche ist auch Adressat der Rechte der betroffenen Personen nach Art. 12 ff. DSGVO. Er hat nicht nur die Rechtmäßigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten zu gewährleisten, sondern muss auch den Nachweis dafür erbringen, dass die Datenverarbeitung im Einklang mit den Vorgaben der DSGVO erfolgt (sog. Rechenschaftspflicht, Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Auch die Richtlinie zum Datenschutz bei Polizei und Justiz sieht formelle und organisatorische Pflichten des Verantwortlichen vor, die denen der DSGVO weitgehend entsprechen und im BayDSG sowie im Fachrecht in nationales Recht umgesetzt wurden.

Im öffentlichen Bereich ist der Verantwortliche nicht eine einzelne handelnde Person, sondern die für die Datenverarbeitung zuständige öffentliche Stelle, d.h. die Behörde oder sonstige öffentliche Stelle, z. B. die Gemeinde oder das Landratsamt (Art. 4 Nr. 7 DSGVO, Art. 3 Abs. 2 BayDSG).[17] Der Leitung der jeweiligen öffentlichen Stelle obliegt es insbesondere, ein Datenschutzkonzept aufzustellen, mit dem sichergestellt wird, dass im Zuständigkeitsbereich der öffentlichen Stelle die datenschutzrechtlichen Pflichten erfüllt und datenschutzrechtliche Bestimmungen eingehalten werden (Art. 24 Abs. 2 DSGVO). Dies setzt voraus, dass datenschutzrechtliche Zuständigkeiten konkret einzelnen Organisationseinheiten oder Personen innerhalb der öffentliche Stelle zugewiesen und notwendige Verfahrensabläufe festgelegt werden.

> Mit anderen Worten: Die Leitung der jeweiligen öffentlichen Stelle muss dafür Vorsorge treffen, dass innerhalb ihres Zuständigkeitsbereichs eine datenschutzrechtliche Aufbau- und Ablauforganisation zur Verfügung steht, welche die Einhaltung der Vorgaben der datenschutzrechtlichen Vorschriften gewährleistet.

Die Dokumentation des Datenschutzkonzepts dient auch der Erfüllung der Rechenschaftspflicht.

Die Mindestaufgaben des / der behördlichen Datenschutzbeauftragten sind in Art. 39 Abs. 1 DSGVO, Art. 12 und Art. 24 Abs. 5 BayDSG gesetzlich festgelegt. Darüber hinaus können

---

[17] Vgl. für Verwaltungsgemeinschaften AKI 2 des LfD, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki02.html.

auf den / die behördliche(n) Datenschutzbeauftragte(n) einzelne Aufgaben und Pflichten des Verantwortlichen übertragen werden, sofern dies nicht zu einem Interessenkonflikt bei der Wahrnehmung seiner / ihrer übrigen Kernaufgaben führt (Art. 38 Abs. 6 DSGVO).[18]

Das nachfolgende Muster einer Datenschutz-Geschäftsordnung enthält Vorschläge, wie innerhalb einer öffentlichen Stelle datenschutzrechtliche Zuständigkeiten verteilt und verfahrensrechtliche Abläufe geregelt werden können. Das Muster ist für mittlere und große staatliche Verwaltungsbehörden konzipiert. Es kann eine Hilfestellung für eigenverantwortlich zu treffende Regelungen der Gemeinden, Landkreise, Bezirke und sonstigen öffentlichen Stellen sein. Abhängig von Größe und Struktur der einzelnen öffentlichen Stellen kann sich auch eine andere Zuständigkeitsverteilung oder die Festsetzung abweichender Verfahrensabläufe als sinnvoll erweisen.

Hinweis: Die Regelungen der DSGVO finden grundsätzlich auch bei Datenverarbeitungen im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz entsprechende Anwendung (vgl. Art. 2 Satz 1 i.V.m. Art. 28 ff. BayDSG). Aus Teil 2 Kapitel 8 des BayDSG sowie aus dem jeweiligen Fachrecht können sich jedoch Abweichungen, Modifikationen oder Ergänzungen (z. B. zusätzliche Angaben, die in das Verarbeitungsverzeichnis nach Art. 30 DSGVO aufgenommen werden müssen, vgl. Art. 31 BayDSG) ergeben, die bei der Anwendung der einzelnen Regelungen der DSGVO zu beachten sind. Bei Datenverarbeitungen zum Zwecke der Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten gelten vorrangig die Vorgaben des BDSG (§ 46 Abs. 1 OWiG i.V.m. § 500 StPO). Mit § 4 Buchst. c, § 12 Abs. 3 Satz 5 sowie § 14 enthält die Geschäftsordnung Regelungen, die nur bei Verarbeitungen im Anwendungsbereich des Art. 28 BayDSG zu beachten sind. Zur besseren Lesbarkeit des Musters nimmt die Geschäftsordnung ansonsten nur auf die Vorschriften der DSGVO Bezug. Auf Modifikationen zu einzelnen Regelungen der DSGVO für Datenverarbeitungen im Anwendungsbereich des Art. 28 BayDSG wird in den Erläuterungen hingewiesen.

[18] Ergänzende Informationen hierzu enthält die AKI 7: Datenschutzbeauftragte kreisangehöriger Gemeinden in Bayern: Inkompatibilitäten, Qualifikation, Zeitbudget des Landesbeauftragten, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki07.html.

4.1 Muster einer Datenschutz-Geschäftsordnung

Datenschutz-Geschäftsordnung[19] der … (*Behörde*) …. vom….

Inhaltsverzeichnis:

Erster Teil: Allgemeine Regelungen
§ 1 Geltungsbereich

Zweiter Teil: Datenschutzrechtliche Zuständigkeiten
§ 2 Behördenleitung
§ 3 Organisationssachgebiet
§ 4 IT-Sachgebiet
§ 5 Fachsachgebiete
§ 6 Behördliche(r) Datenschutzbeauftragte(r)

Dritter Teil: Zusammenarbeit
§ 7 Zusammenarbeit und gegenseitige Information

Vierter Teil: Datenschutzrechtliche Ablauforganisation
Abschnitt 1: Allgemeine Grundsätze zur Gewährleistung des Datenschutzes
§ 8 Information der Beschäftigten
§ 9 Beteiligung des / der behördlichen Datenschutzbeauftragten
§ 10 Datenschutzbericht
§ 11 Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses
Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen
§ 12 Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO
§ 13 Auftragsverarbeitung
§ 14 Vertrauliche Meldung von Datenschutzverstößen

Fünfter Teil: Schlussvorschriften
§ 15 Inkrafttreten

4 Anlagen

[19] Im kommunalen Bereich kann sich die Bezeichnung als „Dienstanweisung“ anbieten.

Erster Teil: Allgemeine Regelungen

§ 1 Geltungsbereich

Die Geschäftsordnung gilt für die Verarbeitung personenbezogener Daten durch alle Organisationseinheiten/Dienststellen der <*Behörde/Kommune*>.

Zweiter Teil: Datenschutzrechtliche Zuständigkeiten

§ 2 Behördenleitung[20]

(1) Die Behördenleitung stellt mit Unterstützung der nachfolgend genannten Organisationseinheiten sicher, dass die Verarbeitung personenbezogener Daten im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt

(2) [1]Die Behördenleitung benennt einen / eine behördliche(n) Datenschutzbeauftragte(n) und dessen / deren Vertretung, soweit gesetzlich oder in dieser Geschäftsordnung nichts anderes bestimmt ist. [2]Für die Benennung kann das als Anlage 1 beigefügte Schreiben verwendet werden

§ 3 Organisationssachgebiet[21]

(1) [1]Das Organisationssachgebiet erarbeitet im Benehmen mit dem / der behördlichen Datenschutzbeauftragten und dem IT-Sachgebiet geeignete Datenschutzvorkehrungen nach Art. 24 Abs. 2 DSGVO. [2]Hierzu gehören insbesondere Datenschutz-Richtlinien und fachverfahrensspezifische Anweisungen an die Beschäftigten.

(2) Soweit nichts anderes bestimmt[22] ist, führt das Organisationssachgebiet das Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO.

§ 4 IT-Sachgebiet[23]

Das IT-Sachgebiet legt in Abstimmung mit den nach §§ 3 und 5 zuständigen Organisationseinheiten

a. geeignete technische und organisatorische Maßnahmen zum Schutz der zu verarbeitenden Daten nach Art. 24 Abs. 1, Art. 25 und Art. 32 DSGVO,

b. angemessene und spezifische Maßnahmen zum Schutz besonderer Kategorien personenbezogener Daten nach Art. 8 Abs. 2 BayDSG,

---

[20] Im gemeindlichen Bereich z. B. der erste Bürgermeister/ Bürgermeisterin / Oberbürgermeister / Oberbürgermeisterin.
[21] Ggf. konkretisieren.
[22] Vgl. § 6 dieser Geschäftsordnung.
[23] Ggf. konkretisieren. Mit „IT-Sachgebiet“ wird die für IT verantwortliche Organisationseinheit bezeichnet.

c. ggf. geeignete Maßnahmen nach Art. 32 Abs. 2 BayDSG[24]

fest.

§ 5 Fachsachgebiete[25]

(1) Die Fachsachgebiete tragen für ihren Zuständigkeitsbereich die Verantwortung für die Beachtung der jeweils maßgeblichen datenschutzrechtlichen Vorschriften.

(2) Im Benehmen mit dem / der behördlichen Datenschutzbeauftragten stellen die Fachsachgebiete für ihren Zuständigkeitsbereich sicher, dass die Rechte der betroffenen Personen nach Art. 12, Art. 15 bis Art. 22 DSGVO sowie die Informationspflichten nach Art. 13 und Art. 14 DSGVO erfüllt werden.

(3) [1]Die Personalvertretung gilt als Fachsachgebiet. [2]Der besonderen Stellung der Personalvertretung ist Rechnung zu tragen.

§ 6 Behördliche(r) Datenschutzbeauftragte(r)[26,27]

Ergänzend zu den durch Art. 39 Abs. 1 DSGVO sowie Art. 12 und 24 Abs. 5 BayDSG zugewiesenen Aufgaben nach Anlage 2 werden dem / der behördlichen Datenschutzbeauftragten die nachfolgenden Aufgaben übertragen[28]:

☐ Führung des Verarbeitungsverzeichnisses nach Art. 30 DSGVO

☐ Koordinierung der Erfüllung der Rechte der betroffenen Personen nach Art. 12, Art. 15 bis 22 DSGVO durch das jeweilige Fachsachgebiet einschließlich Beteiligung bei deren abschließenden Entscheidungen über Betroffenenrechte

☐ Begleitung der Durchführung der Datenschutz-Folgenabschätzung nach Art. 35 f. DSGVO

☐ Schulungen von Beschäftigten

☐ Umsetzung der Meldung bzw. Benachrichtigung bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO

☐ _____

---

[24] Entfällt, soweit die öffentliche Stelle nicht dem Anwendungsbereich des Art. 28 BayDSG unterliegt.
[25] Ggf. anpassen z. B. „Fachreferat".
[26] Zur eingeschränkten Zuständigkeit des / der behördlichen Datenschutzbeauftragten in Gerichten vgl. Art. 37 Abs. 1 Buchstabe a DSGVO.
[27] Zur Gewährleistung der Erreichbarkeit des / der behördlichen Datenschutzbeauftragten wird empfohlen, ihm / ihr ein Funktionspostfach einzurichten z. B. datenschutzbeauftragter@behörde.de
[28] Die Übertragung zusätzlicher Aufgaben muss mit der in der DSGVO enthaltenen Rollenbeschreibung des / der Datenschutzbeauftragten vereinbar sein; insbesondere darf die Aufgabenübertragung nicht zu einem Interessenkonflikt führen, vgl. Erläuterungen zu § 6.

Dritter Teil: Zusammenarbeit

§ 7 Zusammenarbeit und gegenseitige Information

(1) [1]Das Organisationssachgebiet, das IT-Sachgebiet und der / die behördliche Datenschutzbeauftragte arbeiten zur Gewährleistung des Datenschutzes vertrauensvoll zusammen und informieren sich gegenseitig. [2]Hierzu schaffen sie geeignete Verfahren der kontinuierlichen Zusammenarbeit. [3]Sie unterrichten die Behördenleitung zeitnah über alle wesentlichen Vorgänge.

(2) [1]Jede(r) Beschäftigte meldet seinem / seiner jeweiligen Vorgesetzten unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen. [2]Die Fachsachgebiete informieren den / die behördliche(n) Datenschutzbeauftragte(n) über den Verstoß.

Vierter Teil: Ablauforganisation

Abschnitt 1: Allgemeine Grundsätze zur Gewährleistung des Datenschutzes

§ 8 Information der Beschäftigten

Die Beschäftigten sind durch Richtlinien zum Datenschutz und auf sonstige Art und Weise für den Umgang mit personenbezogenen Daten zu sensibilisieren.

§ 9 Beteiligung des / der behördlichen Datenschutzbeauftragten

(1) Der / die behördliche Datenschutzbeauftragte wird frühzeitig in alle wesentlichen Datenschutzfragen eingebunden und vom Organisationssachgebiet, dem IT-Sachgebiet, den Fachsachgebieten und den Beschäftigten bei der Erfüllung seiner / ihrer Aufgaben unterstützt.

(2) Ihm / ihr ist vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben.

(3) [1]Vor dem Einsatz einer Videoüberwachung sind dem behördlichen Datenschutzbeauftragten der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, der betroffene Personenkreis, die Maßnahmen nach Art. 24 Abs. 2 BayDSG und die vorgesehenen Auswertungen mitzuteilen. [2]Ihm / ihr ist Gelegenheit zur Stellungnahme zu geben.

(4) Der / die behördliche Datenschutzbeauftragte ist im Vorfeld von Vergabeverfahren und neuer Fachverfahren sowie vor der Beschaffung von IT-Systemen (IT-Hard- und Software) und IT-Diensten zu beteiligen, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden.

§ 10 Datenschutzbericht[29]

[1]Der / die behördliche Datenschutzbeauftragte erstellt regelmäßig, mindestens alle zwei Jahre, einen Bericht zum Datenschutz. [2]In diesem sind die in der Behörde/Kommune zur Gewährleistung des Datenschutzes eingesetzten technischen und organisatorischen Maßnahmen darzustellen sowie ggf. festgestellte Datenschutzverstöße und Schutzlücken aufzuführen. [3]Der Bericht enthält eine Bewertung, ob die eingesetzten technischen und organisatorischen Maßnahmen ausreichend sind, dem Stand der Technik entsprechen und in welchem Umfang datenschutzrechtliche Risiken bestehen. [4]Die Ergebnisse des Berichts werden mit der Behördenleitung und den zuständigen Organisationseinheiten erörtert und Verbesserungsmöglichkeiten geprüft. [5]Der Bericht wird nicht veröffentlicht.

§ 11 Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses

(1) Die Fachsachgebiete melden der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit[30] unaufgefordert die neu aufgenommenen Verarbeitungstätigkeiten sowie wesentliche Änderungen bereits gemeldeter Verarbeitungstätigkeiten.

(2) Für diese Meldung ist das als Anlage 3 beigefügte Formblatt zu verwenden.

(3) [1]Die für die Führung des Verarbeitungsverzeichnisses zuständige Organisationseinheit[31] übersendet den Fachsachgebieten jährlich eine Liste der von diesen gemeldeten Verarbeitungstätigkeiten. [2]Die Fachsachgebiete prüfen die Liste auf Richtigkeit und Vollständigkeit, aktualisieren sie und leiten sie der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit[32] zu.

---

[29] Die Erstellung eines Datenschutzberichts ist eine von mehreren Möglichkeiten, um die Erfüllung der Pflichten des Verantwortlichen nach Art. 24 Abs. 1 Satz 2 DSGVO sowie des / der behördlichen Datenschutzbeauftragten nach Art. 38 Abs. 3 Satz 3, Art. 39 Abs. 1 Buchst. b DSGVO verfahrensrechtlich abzusichern. Anstelle eines schriftlichen Berichts kann auch ein anderes geeignetes Verfahren zur regelmäßigen Beurteilung des Datenschutzes vorgesehen werden, das die Einhaltung der oben genannten Pflichten sicherstellt.

[30] Ggf. konkretisieren: hierbei kann es sich z. B. um das Organisationssachgebiet (vgl. § 4 Abs. 2) oder bei einer Aufgabenübertragung nach § 6 um den / die behördliche(n) Datenschutzbeauftragte(n) handeln.

[31] Ggf. konkretisieren.

[32] Ggf. konkretisieren.

Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen

§ 12 Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO

(1) [1]Im Fall einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO informiert die jeweilige Organisationseinheit, der die Datenschutzverletzung bekannt geworden ist, unverzüglich den / die behördliche(n) Datenschutzbeauftragte(n) hierüber.

(2) [1]Soweit dem Organisationssachgebiet und dem IT-Sachgebiet der Verstoß noch nicht bekannt ist, unterrichtet der / die behördliche Datenschutzbeauftragte diese. [2]Er / sie teilt ihnen dabei seine / ihre Einschätzung mit, ob eine Meldepflicht nach Art. 33 DSGVO und/oder eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. [3]Die Einschätzung ist schriftlich zu begründen.

(3) [1]Die für die Umsetzung der Meldung zuständige Organisationseinheit[33] meldet im Einvernehmen mit dem Organisationssachgebiet und dem IT-Sachgebiet die Verletzung des Schutzes personenbezogener Daten unverzüglich dem Bayerischen Landesbeauftragten für den Datenschutz mit dem nach Art. 33 DSGVO vorgegebenen Mindestinhalt, möglichst innerhalb einer Frist von 72 Stunden. [2]Ist eine Meldung innerhalb von 72 Stunden nicht möglich, sind die Gründe hierfür zu dokumentieren und die Meldung unverzüglich nachzuholen. [3]Die Meldung unterbleibt, wenn das Organisationssachgebiet und das IT-Sachgebiet unter Berücksichtigung der Einschätzung des / der behördlichen Datenschutzbeauftragten nach Abs. 2 der Auffassung sind, dass die Voraussetzungen des Art. 33 DSGVO nicht vorliegen. [4]Die Gründe hierfür sind zu dokumentieren. [5]Im Anwendungsbereich der Art. 28 bis 37 BayDSG sind, soweit von einer Verletzung des Schutzes personenbezogener Daten solche Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, die in Art. 33 Abs.3 DSGVO genannten Informationen unverzüglich auch an diesen zu melden (Art. 33 BayDSG bzw. bei der Ordnungswidrigkeitenverfolgung § 46 Abs. 1 OWiG i.V.m. § 500 StPO, § 65 Abs. 6 BDSG). [6]Im Einzelfall erforderliche zusätzliche Meldungen (z. B. nach § 83a SGB X an die Rechts- oder Fachaufsicht von Sozialbehörden oder nach Art. 11 Abs. 2 BayEGovG bzw. Art. 43 Abs. 2 BayDiG-E an das Landesamt für Sicherheit in der Informationstechnik) bleiben davon unberührt.

---

[33] Ggf. konkretisieren: Die Meldung erfolgt z. B. durch den / die behördliche(n) Datenschutzbeauftragte(n), wenn ihm / ihr diese Aufgabe gemäß § 6 übertragen worden ist. Ist dies nicht der Fall und wurde diese Aufgabe auch keiner anderen Organisationseinheit (z. B. IT-Sachgebiet, Organisationssachgebiet) zugewiesen, verbleibt es bei der Verantwortlichkeit des zuständigen Fachsachgebiets nach § 5 Abs. 1.

(4) [1]Das Organisationssachgebiet und das IT-Sachgebiet entscheiden auf der Grundlage der Einschätzung des / der behördlichen Datenschutzbeauftragten nach Abs. 2, ob eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat und somit eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. [2]Die Benachrichtigung der betroffenen Person erfolgt unverzüglich durch die für die Umsetzung der Benachrichtigung zuständige Organisationseinheit. [3]Unterbleibt eine Benachrichtigung nach Art. 34 DSGVO, sind die Gründe hierfür zu dokumentieren.

(5) Nach Bekanntwerden des Verstoßes leiten das Organisationssachgebiet und das IT-Sachgebiet in Abstimmung mit dem / der behördlichen Datenschutzbeauftragten unverzüglich Abhilfemaßnahme ein.

§ 13 Auftragsverarbeitung

[1]Das Organisationssachgebiet prüft vor Abschluss eines Vertrages über die Auftragsverarbeitung, ob der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO und den zu ihrer Ergänzung erlassenen europäischen, bundes- und landesrechtlichen Regelungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. [2]Hierzu lässt sich das Organisationssachgebiet entsprechende Nachweise/Zertifikate vorlegen und holt die Stellungnahme des / der behördlichen Datenschutzbeauftragten sowie des IT-Sachgebiets ein.

§ 14 Vertrauliche Meldung von Datenschutzverstößen

[1]Erlangt ein Mitarbeiter oder eine Mitarbeiterin von einem Datenschutzverstoß Kenntnis, kann er oder sie sich jederzeit unmittelbar an den / die behördliche(n) Datenschutzbeauftragte(n) wenden. [2]Postalische Sendungen, welche im Adressfeld den Zusatz „Datenschutzbeauftragte(r)“ enthalten, dürfen nur von dem / der behördlichen Datenschutzbeauftragten oder der Vertretung[34] geöffnet werden.[35] [3]Der/ die behördliche Datenschutzbeauftragte behandelt die Meldung vertraulich. [4]Er / sie darf Tatsachen, die ihm / ihr in Ausübung der Funktion anvertraut wurden, und die Identität der mitteilenden Person nicht ohne deren Einverständnis offenbaren.

§ 15 Inkrafttreten

Diese Geschäftsordnung tritt am … in Kraft.

---

[34] Vgl. dazu AKI 30 des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/aki30.html.
[35] Vgl. dazu AKI 25 des LfD, https://www.datenschutz-bayern.de/datenschutzreform2018/aki25.html.

4.2 Erläuterungen zur Datenschutz-Geschäftsordnung

Erster Teil: Allgemeine Regelungen

Zu § 1 (Geltungsbereich)

§ 1 bestimmt den Adressatenkreis, an den sich die Datenschutz-Geschäftsordnung richtet.

Zweiter Teil: Datenschutzrechtliche Zuständigkeiten

Der zweite Teil enthält aufbauorganisatorische Regelungen und legt konkret fest, welche Organisationseinheit innerhalb der öffentlichen Stelle für die Wahrnehmung bestimmter datenschutzrechtlicher Pflichten zuständig ist. Fehlt eine Zuständigkeitszuweisung an eine konkrete Organisationseinheit, sieht das vorliegende Muster eine allgemeine Zuständigkeit der jeweiligen Fachsachgebiete vor (siehe § 5).

Zu § 2 (Behördenleitung)

Zu Abs. 1: Die Leitung der öffentlichen Stelle hat zu gewährleisten, dass innerhalb ihres Zuständigkeitsbereichs die datenschutzrechtlichen Bestimmungen eingehalten werden.
Zu den maßgeblichen datenschutzrechtlichen Bestimmungen, die bei der Verarbeitung personenbezogener Daten zu beachten sind, gehören in erster Linie die Regelungen der DSGVO sowie die sie ergänzenden bundes- oder landesrechtlichen Datenschutzregelungen. Daneben unterfallen Verwaltungsbehörden, die in der Regel auch personenbezogene Daten zu Zwecken der Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten verarbeiten, insoweit auch dem Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz und haben die zur Umsetzung der Richtlinie erlassenen Datenschutzregelungen im Bundes- und Landesrecht zu beachten (vgl. Art. 28 Abs. 1 Satz 2 BayDSG).

Die Behördenleitung hat zum einen sicherzustellen, dass alle Verarbeitungen der öffentlichen Stelle im Einklang mit den materiell-rechtlichen Anforderungen dieser Vorschriften stehen, zum anderen, dass die Verfahrenspflichten in der öffentlichen Stelle umgesetzt werden. Diese Aufgabe kann die Behördenleitung nur erfüllen, wenn sie hierbei von verschiedenen Organisationseinheiten innerhalb der öffentlichen Stelle unterstützt wird. Jedes Fachsachgebiet hat in seinem Zuständigkeitsbereich die Vorschriften des Datenschutzes umzusetzen. Bei der Umsetzung organisatorischer und technischer Datenschutzmaßnahmen sind insbesondere das für die innerbehördliche Organisation zuständige Sachgebiet sowie das für IT

verantwortliche Sachgebiet gefordert. Darüber hinaus ist die Behördenleitung auf die Unterstützung des / der behördlichen Datenschutzbeauftragten angewiesen, zu dessen / deren Aufgaben u.a. die Unterrichtung und Beratung des Verantwortlichen im Hinblick auf datenschutzrechtliche Regelungen gehört (vgl. Art. 39 Abs. 1 Buchst. a DSGVO). Dem / der behördlichen Datenschutzbeauftragten können vom Behördenleiter einzelne Aufgaben und Pflichten des Verantwortlichen zur Durchführung übertragen werden, allerdings nur, soweit dies mit dem in der Datenschutz-Grundverordnung vorgesehenen Rollenbild des / der Datenschutzbeauftragten vereinbar ist und auch nicht zu einem Interessenkonflikt bei der Wahrnehmung seiner / ihrer übrigen Datenschutz-Kernaufgaben führt (Art. 38 Abs. 6 DSGVO).

Unterstützung im Sinne des § 2 bedeutet, dass die genannten Organisationseinheiten in ihrem Zuständigkeitsbereich der Behördenleitung zuarbeiten und für diese datenschutzrechtliche Pflichten wahrnehmen. Die Weisungs- und Entscheidungshoheit verbleibt dabei bei der Behördenleitung.

Zu Abs. 2: Die Benennung des / der behördlichen Datenschutzbeauftragten gehört in der Regel zu den Aufgaben der Behördenleitung. Ein Muster für ein mögliches Benennungsschreiben findet sich in Anlage 1 der Geschäftsordnung.

Zu § 3 (Organisationssachgebiet)

Zu Abs. 1: Das Organisationssachgebiet ist in einer öffentlichen Stelle für die Leitung aller innerorganisatorischen Angelegenheiten zuständig und schlägt der Leitung der öffentlichen Stelle Organisationsverfügungen vor.

Datenschutzrechtliche Aufgaben des Verantwortlichen, die im Zusammenhang mit innerorganisatorischen Fragestellungen stehen, sollten auf das Organisationssachgebiet übertragen werden. Hierzu gehört die in Art. 24 Abs. 2 DSGVO genannte Aufgabe des Verantwortlichen, geeignete Datenschutzvorkehrungen vorzusehen. Unter diesem Begriff sind insbesondere fachverfahrensspezifische Anweisungen an die Beschäftigten sowie interne oder externe Datenschutz-Richtlinien mit konkreten Handlungsanweisungen zum Umgang mit personenbezogenen Daten zu verstehen. Aufgabe des Organisationssachgebiets ist es entsprechende organisatorische Maßnahmen im Benehmen mit dem / der behördlichen Datenschutzbeauftragten und dem IT- Sachgebiet zu erarbeiten und der Behördenleitung vorzuschlagen.

Zu Abs. 2: Je nach Größe und Struktur der Behörde kann es sich empfehlen, weitere Aufgaben auf das Organisationssachgebiet zu übertragen, wie beispielsweise die Führung des

Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO. Bei Datenverarbeitungen im Anwendungsbereich des Art. 28 BayDSG sind nach Art. 31 BayDSG ergänzende Angaben im Verarbeitungsverzeichnis aufzunehmen. Die Führung des Verarbeitungsverzeichnisses bedeutet in diesem Zusammenhang die reine Verwaltung des Verarbeitungsverzeichnisses, nicht die Erstellung der einzelnen Beschreibungen der Verarbeitungstätigkeiten (vgl. zur Übertragungsmöglichkeit auf den / die behördliche(n) Datenschutzbeauftragte(n) § 6).

Zu § 4 (IT-Sachgebiet)

Aufgaben des Verantwortlichen im Zusammenhang mit der Gewährleistung der Sicherheit einschließlich der Vertraulichkeit, Verfügbarkeit und Integrität der Daten, die durch IT-Systeme und IT-Dienste verarbeitet werden, sollten innerhalb einer Behörde auf das IT-Sachgebiet übertragen werden. Hierzu gehört insbesondere die Einrichtung geeigneter technischer Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung sowie die Pflicht, Technik datenschutzfreundlich einzusetzen und Voreinstellungen so zu wählen, dass nur die für den konkreten Zweck erforderlichen personenbezogenen Daten verarbeitet werden (Art. 24 Abs. 1, Art. 25 und Art. 32 DSGVO). Besondere Kategorien personenbezogener Daten sind als sensible Daten durch angemessene und spezifische Maßnahmen zu schützen (Art. 8 Abs. 2 BayDSG). Bei Verarbeitungen im Anwendungsbereich der Art. 28 bis 37 BayDSG müssen im Fall von automatisierten Datenverarbeitungen besondere Schutzmaßnahmen nach Art. 32 Abs. 2 BayDSG getroffen werden, Art. 32 Abs. 3 und 4 DSGVO sind nicht anwendbar, vgl. Art. 32 Abs. 1 BayDSG. Beabsichtigte Maßnahmen müssen vor ihrem Erlass mit dem Organisationssachgebiet und den jeweils betroffenen Fachsachgebieten bzw. der Behördenleitung abgestimmt werden.

Das bisher nach Art. 11 Abs. 1 des Bayerischen E-Government-Gesetzes (BayEGovG) sowie künftig nach Art. 43 Abs. 1 des Bayerischen Digitalgesetzes (BayDiG-E) zu erstellende Informationssicherheitskonzept kann in diesem Zusammenhang wichtige Grundlagen und Anhaltspunkte liefern.

Zu § 5 (Fachsachgebiete)

Zu Abs. 1: Die Fachsachgebiete sind innerhalb ihres Fachbereichs dafür verantwortlich, dass personenbezogene Daten im Einklang mit datenschutzrechtlichen Vorgaben verarbeitet werden. Findet sich in der Geschäftsordnung keine ausdrückliche Zuständigkeitszuweisung an eine andere Organisationseinheit, sind die jeweiligen Fachsachgebiete für die Wahrnehmung der datenschutzrechtlichen Aufgabe zuständig.

Zu Abs. 2: Darüber hinaus liegt die Zuständigkeit für die Erfüllung der Rechte der betroffenen Personen nach Art. 15 bis Art. 22 DSGVO bei den Fachsachgebieten. Die Fachsachgebiete müssen in ihrem Fachbereich dafür Sorge tragen, dass Anträge der betroffenen Personen zügig bearbeitet und hierüber rechtzeitig innerhalb der europarechtlich vorgegebenen Fristen nach Art. 12 Abs. 3 DSGVO entschieden wird. Der / die behördliche Datenschutzbeauftragte ist vor der abschließenden Entscheidung über die Betroffenenrechte in aller Regel zu beteiligen. Bei Datenverarbeitungen im Anwendungsbereich des Art. 28 BayDSG sind die Rechte der betroffenen Personen im jeweiligen Fachrecht geregelt (zum Beispiel in Art. 65 PAG, Art. 23 BayVSG).

Zu Abs. 3: Als Teil der öffentlichen Stelle unterliegt auch der Personalrat grundsätzlich datenschutzrechtlichen Anforderungen und sollte deshalb wie ein Fachsachgebiet behandelt werden. Hierbei ist jedoch die besondere Stellung des Personalrats zu berücksichtigen. Es empfiehlt sich, die Regelung jeweils im Vorfeld der Verabschiedung der Geschäftsordnung mit der zuständigen Personalvertretung im Wege der vertrauensvollen Zusammenarbeit abzustimmen.[36]

Sollten weitere Stellen datenschutzrechtlich mit einbezogen werden, ist das bereits in § 1 aufzuführen.

Zu § 6 (Behördliche(r) Datenschutzbeauftragte(r))

Dem / der behördlichen Datenschutzbeauftragten werden in DSGVO und im BayDSG eine Reihe von Aufgaben zugewiesen. Diese Mindestaufgaben sind in der als Anlage 2 beigefügten Übersicht aufgeführt und mit konkretisierenden Beispielen versehen. Hinzu können ferner fachgesetzlich geregelte Aufgaben kommen.

Bei Gerichten erstreckt sich die Zuständigkeit des / der behördlichen Datenschutzbeauftragten nicht auf Verarbeitungen im Rahmen ihrer justiziellen Tätigkeit (Art. 37 Abs. 1 Buchst. a DSGVO).

[36] Ausführliche Informationen zur Frage, ob der Personalrat ein eigenständiger datenschutzrechtlicher Verantwortlicher ist. finden sich in der AKI 23: Der Personalrat - Verantwortlicher im Sinne des Datenschutzrechts?, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki23.html.

Neben den gesetzlich zugewiesenen Aufgaben können auf den / die behördliche(n) Datenschutzbeauftragte(n) weitere Aufgaben übertragen werden. Von einer Übertragung ist abzusehen, wenn diese nicht mit der in der DSGVO enthaltenen Rollenbeschreibung des / der Datenschutzbeauftragten vereinbar ist; insbesondere darf die Aufgabenübertragung nicht zu einem Interessenkonflikt führen (Art. 38 Abs. 6 DSGVO).

Neben der Übertragung von Koordinationsaufgaben bei der Erfüllung der Rechte der betroffenen Personen und der Begleitung der Durchführung einer Datenschutz-Folgenabschätzung, dem Abhalten von Schulungen sowie Umsetzung von Meldungen und Benachrichtigungen nach Art. 33 f. DSGVO kommt insbesondere die Übertragung der Führung des Verarbeitungsverzeichnisses nach Art. 30 DSGVO auf den / die behördliche(n) Datenschutzbeauftragte(n) in Betracht. Die Führung des Verarbeitungsverzeichnisses bedeutet in diesem Zusammenhang die reine Verwaltung des Verarbeitungsverzeichnisses. Für die Erstellung der einzelnen Beschreibungen der Verarbeitungstätigkeiten sowie für die Richtigkeit, Vollständigkeit und Aktualität des Verarbeitungsverzeichnisses bleiben die Behördenleitung, das Organisationssachgebiet bzw. die Fachsachgebiete zuständig.

Im Anwendungsbereich des Art. 28 BayDSG sind die Rechte der betroffenen Person im Fachrecht geregelt. Die Regelungen nach Art. 30 und Art. 33 DSGVO werden ergänzt durch die Bestimmungen in Art. 31 und Art. 33 BayDSG.

Dritter Teil: Zusammenarbeit

Zu § 7 (Zusammenarbeit und gegenseitige Information)

§ 7 Abs. 1 dient der Sicherstellung des gegenseitigen Austausches und Informationsflusses zwischen dem Organisationssachgebiet, dem IT-Sachgebiet und dem / der behördlichen Datenschutzbeauftragten. Als geeignetes Verfahren der Zusammenarbeit kommt beispielsweise die Einrichtung eines Jour Fixe in Betracht.
Zugleich wird mit der Regelung die Unterrichtung der Behördenleitung von wesentlichen datenschutzrechtlich relevanten Vorgängen gewährleistet.

Abs. 2 stellt zudem den Informationsfluss sicher für den Fall, dass einem Beschäftigten oder einer Beschäftigten ein Datenschutzverstoß bekannt wird. Handelt es sich bei dem Verstoß um eine Datenschutzverletzung im Sinne von Art. 4 Nr. 12 DSGVO, regelt § 12 das weitere Verfahren.

Vierter Teil: Datenschutzrechtliche Ablauforganisation

Der vierte Teil enthält ablauforganisatorische Regelungen, die die Einhaltung datenschutzrechtlicher Vorschriften in verfahrensrechtlicher Hinsicht absichern sollen. §§ 8 bis 11 enthalten allgemeine Verfahrensregelungen, §§ 12 ff. regeln besondere Verfahrensbestimmungen zur Gewährleistung besonderer datenschutzrechtlicher Pflichten, die durch die DSGVO neu begründet oder modifiziert wurden.

Zu § 8 (Information der Beschäftigten)

Die Beschäftigten sollten für den Umgang mit personenbezogenen Daten sensibilisiert werden. Dies kann beispielsweise über Richtlinien zum Datenschutz erfolgen, die konkrete Handlungsanweisungen zum Umgang mit personenbezogenen Daten vorsehen oder durch Informationsmaterial sowie Schulungen zum Datenschutz etc.

Zu § 9 (Beteiligung des / der behördlichen Datenschutzbeauftragten)

§ 9 gewährleistet die frühzeitige Einbindung des / der behördlichen Datenschutzbeauftragten bei allen wesentlichen datenschutzrechtlich relevanten Verfahrensabläufen (vgl. Art. 38 Abs. 1 DSGVO). Insbesondere wenn in der Behörde grundsätzliche oder schwierige datenschutzrechtliche Fragestellungen auftreten, ist der / die behördliche Datenschutzbeauftragte hierüber zu informieren und es ist ihm / ihr Gelegenheit zur Stellungnahme einzuräumen sowie ggf. die Teilnahme an Besprechungen zu ermöglichen. Vorlagen, die grundsätzliche oder schwierige datenschutzrechtliche Fragestellungen behandeln, sind ihm / ihr gleichfalls mit der Gelegenheit zur Stellungnahme zuzuleiten.

In jedem Fall ist dem / der behördlichen Datenschutzbeauftragten vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, sowie vor dem Einsatz einer Videoüberwachung Gelegenheit zur Stellungnahme zu geben (Art. 12, 24 Abs. 5 BayDSG).

Eine Beteiligung des / der behördlichen Datenschutzbeauftragten im Vorfeld der Beschaffung von IT-Systemen (IT-Hard- und Software) und IT-Diensten ist nur erforderlich, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden.

Zu § 10 (Datenschutzbericht)

Zu den Aufgaben des / der behördlichen Datenschutzbeauftragten gehört insbesondere die Überwachung der Einhaltung der Vorgaben der DSGVO nach Art. 39 Abs. 1 Buchst. b DSGVO. Der / die Datenschutzbeauftragte hat hierbei unmittelbar der Behördenleitung zu berichten (vgl. Art. 38 Abs. 3 Satz 3 DSGVO). Zugleich verpflichtet Art. 24 Abs. 1 Satz 2 DSGVO den Verantwortlichen, die umgesetzten technischen und organisatorischen Maßnahmen erforderlichenfalls zu überprüfen und zu aktualisieren. Durch den in § 10 vorgesehenen Bericht wird den beiden miteinander verschränkten Verpflichtungen des / der behördlichen Datenschutzbeauftragten und des Verantwortlichen durch ein Verfahren Rechnung getragen, das eine regelmäßige Beurteilung der Datenschutzorganisation einer Behörde gewährleistet. Soweit dies auch auf andere Weise sichergestellt wird, können die in § 10 vorgeschlagenen Berichtszeiträume verlängert oder der Bericht durch ein anderes geeignetes Verfahren zur regelmäßigen Beurteilung des Datenschutzes ersetzt werden (z. B. durch regelmäßige Besprechungen, in denen die in § 10 Satz 2 und 3 genannten Punkte erörtert werden).

Zu § 11 (Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses)

§ 11 enthält Verfahrensregelungen, die der Sicherstellung der Vollständigkeit und Aktualität des Verarbeitungsverzeichnisses dienen.

Zu § 12 (Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO)

§ 12 regelt das Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO und stellt die Beteiligung der zuständigen Organisationseinheiten sicher. Sowohl das Meldeverfahren nach Art. 33 DSGVO als auch das Benachrichtigungsverfahren nach Art. 34 DSGVO knüpfen an den Begriff der Datenschutzverletzung an. Eine Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO ist nicht schon bei jedem Datenschutzverstoß erforderlich, sondern nur bei Sicherheitsverletzungen, die, ob beabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten geführt haben, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (vgl. Art. 4 Nr. 12 DSGVO). Eine Benachrichtigung der betroffenen Person nach Art. 34 DSGVO ist nur bei Datenschutzverletzungen, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge haben, notwendig. Ausnahmen sind in Art. 13 BayDSG geregelt. Bei Datenverarbeitungen nach Art. 28 BayDSG ist ergänzend Art. 33 BayDSG zu berücksichtigen.

Die Umsetzung der Meldung der Datenschutzverletzung an die Aufsichtsbehörde sowie die Benachrichtigung der betroffenen Person kann auf den / die behördliche(n) Datenschutzbeauftragte(n) nach § 6 übertragen werden. Ein Online-Formular zur Meldung von Datenschutzverletzungen an den Bayerischen Landesbeauftragten für den Datenschutz, das auch eine Übersicht typisch vorkommender Datenschutzverletzungen beinhaltet, findet sich auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter https://www.datenschutz-bayern.de/service/data_breach.html.

Zu § 13 (Auftragsverarbeitung)

§ 13 trifft Verfahrensbestimmungen zur Auftragsverarbeitung nach Art. 28 DSGVO. Bei Datenverarbeitungen nach Art. 28 BayDSG sind die Maßgaben nach Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG zu beachten.

Zu § 14 (Vertrauliche Meldung von Datenschutzverstößen)

§ 14 enthält eine verfahrensrechtliche Bestimmung zur vertraulichen Meldung von Datenschutzverstößen. Bei Datenverarbeitungen im Anwendungsbereich der Art. 28 bis 37 BayDSG sind zusätzlich die Vorgaben des Art. 36 BayDSG zu beachten.

Fünfter Teil: Schlussvorschriften

Zu § 15 (Inkrafttreten)

Die Vorschrift legt das Inkrafttreten der Geschäftsordnung fest.

4.3 Anlage 1 (zu § 2)

Benennung als behördliche Datenschutzbeauftragte/behördlicher Datenschutzbeauftragter

(Bezeichnung der öffentlichen Stelle)

Benennung

Hiermit benenne ich

Frau/Herrn

(Amtsbezeichnung) *(Vorname)* *(Name)*

mit Wirkung vom (*Datum des Wirksamwerdens der Benennung)*

als behördliche Datenschutzbeauftragte/behördlichen Datenschutzbeauftragten der/des (Bezeichnung der öffentlichen Stelle)

Gleichzeitig übertrage ich ihr/ihm die in der Datenschutz-Dienstanweisung/Datenschutz-Geschäftsordnung der/des (Bezeichnung der öffentlichen Stelle) vom (Datum) festgelegten Aufgaben.

(Ort/Datum) (Bezeichnung der öffentlichen Stelle)
Unterschrift
(Name und Amtsbezeichnung der unterzeichnenden Behördenleitung)

4.4 Anlage 2 (zu § 6)

Aufgaben des / der behördlichen Datenschutzbeauftragten

	Die Aufgaben des / der Datenschutzbeauftragten umfassen: *(siehe Kennzeichnung)*	
	I. Gesetzliche Aufgaben	**Rechts-grundlage**
	I. 1. Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten, die sich aus dem Datenschutzrecht (DSGVO sowie allgemeine und bereichsspezifische nationale Datenschutzregelungen) ergeben. Dies umfasst insbesondere: I.1.1. Unterrichtung des Verantwortlichen, des Auftragsverarbeiters und der Beschäftigten der Behörde über die grundlegenden Bestimmungen des Datenschutzes und ihre jeweiligen Pflichten sowie Information bei gesetzlichen Neuerungen I.1.2. Datenschutzrechtliche Beratung hinsichtlich aller mit dem Schutz personenbezogener Daten zusammenhängenden Fragestellungen und Aktivitäten, u.a. (1) bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten (2) bei der Einführung neuer automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden sollen oder wesentlichen Änderungen (3) bei Planungen und Entwürfen von Verträgen zur Auftragsverarbeitung (4) hinsichtlich der Pflichten, insbesondere Informations- und Auskunftspflicht, in Bezug auf die Rechte betroffener Personen nach Art. 13 ff. DSGVO (5) hinsichtlich Meldungen bei Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) und Benachrichtigungen (Art. 34 DSGVO) I.1.3. Beantwortung von Anfragen und Einzelberatung von Beschäftigten in allen Fragen des Schutzes personenbezogener Daten I.1.4. Zusammenarbeit mit dem IT-Sicherheitsbeauftragten bzw. IT-Verantwortlichen I.1.5. Beratung des Verantwortlichen bei der Erstellung von Dienstanweisungen und Dienstvereinbarungen mit Bezug zum Schutz personenbezogener Daten	Art. 39 Abs. 1 Buchst. a DSGVO

	I.1.6. Beratung bei der Erstellung eines IT-Sicherheitskonzeptes der Behörde zu Anforderungen, die sich aus den Bestimmungen zum Schutz personenbezogener Daten ergeben	
	I.2. Überwachung der Einhaltung der DSGVO und nationaler Datenschutzvorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und diesbezügliche Überprüfungen Dies umfasst insbesondere: I.2.1. Überwachung der Einhaltung der Datenschutzvorschriften sowie der behördeninternen Vorgaben zum Schutz personenbezogener Daten (Datenschutz-Dienstanweisung) I.2.2. Überwachung und Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei der Ausführung der im Verzeichnis der Verarbeitungstätigkeiten dokumentierten Verarbeitungstätigkeiten I.2.3. Überwachung und Kontrolle der Einhaltung der im Verzeichnis der Verarbeitungstätigkeiten dokumentierten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten und zur Datensicherheit in Zusammenarbeit mit dem Verantwortlichen, der IT-Abteilung und dem IT-Sicherheitsbeauftragten I.2.4. Prüfung und Stellungnahme zur Einhaltung der gesetzlichen Bestimmungen zum Schutz personenbezogener Daten in Verträgen zur Auftragsverarbeitung (1) bei der Umstellung von bestehenden Verträgen auf die neuen gesetzlichen Grundlagen (2) bei vom Verantwortlichen geplanten Abschluss neuer Verträge zur Auftragsverarbeitung I.2.5. Überwachung und Kontrolle der Einhaltung der in den Verträgen zur Auftragsverarbeitung dokumentierten Vorgaben zum Schutz personenbezogener Daten, einschließlich der technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter in Zusammenarbeit mit dem Verantwortlichen, der IT-Abteilung und dem IT-Sicherheitsbeauftragten I.2.6 Fertigung von Stellungnahmen zu Datenschutzproblemen von Verwaltungsbereichen auf Anfrage oder in Eigeninitiative I.2.7 Überwachung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten, auch im Hinblick auf Sensibilisierung und Schulung derjenigen Beschäftigten, die an Verarbeitungsvorgängen beteiligt sind, bzw. diesbezügliche Überprüfungen	Art. 39 Abs. 1 Buchst. b DSGVO

	I.3. Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO I.3.1. Beratung auf Anfrage des Verantwortlichen hinsichtlich der Grundlagen und Erfordernisse von Datenschutz-Folgenabschätzungen I.3.2. Überwachung der ordnungsgemäßen Durchführung von Datenschutz-Folgenabschätzungen	Art. 39 Abs. 1 Buchst. c DSGVO
	I.4. Zusammenarbeit mit der Aufsichtsbehörde	Art. 39 Abs. 1 Buchst. d DSGVO
	I.5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und gegebenenfalls Beratung zu allen sonstigen Fragen	Art. 39 Abs. 1 Buchst. e DSGVO
	I.6. Beratung betroffener Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß DSGVO im Zusammenhang stehenden Fragen I.6.1. Beratung betroffener Personen – auf Anfrage I.6.2. Mit Zustimmung der betroffenen Person Weiterleitung von Anfragen, Auskunftsersuchen und Beschwerden an den Verantwortlichen und Überwachung der Erledigung/Beantwortung durch ihn	Art. 38 Abs. 4 DSGVO
	I.7. Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden. Zugang zum Verzeichnis nach Art. 30 DSGVO	Art. 12 BayDSG
	I.8.Stellungnahme vor dem Einsatz geplanter Videoüberwachungen, insbesondere hinsichtlich Zweck, räumlicher Ausdehnung, Dauer der Videoüberwachung, betroffenem Personenkreis, vorgesehener Maßnahmen zur Kenntlichmachung und vorgesehener Auswertungen	Art. 24 Abs. 5 BayDSG
	I.9. Erstellung von Berichten und Meldungen an die Behördenleitung I.9.1. Anlassbezogene Einzelmeldungen bei Feststellungen von Verletzungen des Schutzes personenbezogener Daten, insbesondere wenn die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt	Art. 38 Abs. 3 Satz 3 DSGVO

	I.9.2. Erstellung von regelmäßigen Berichten zur Datenschutz-Situation der Behörde an die Behördenleitung, zu den in der Dienstanweisung Datenschutz festgelegten Terminen	
	I.10. Regelmäßige eigene Fortbildung zum Datenschutz	

Ort, Datum
Unterschrift
Behördenleiter/in

Anlage 3 (zu § 11)
Siehe Muster unter Nummer 5.4 (Muster einer Beschreibung einer Verarbeitungstätigkeit nach Art. 30 Abs. 1 DSGVO und Art. 31 BayDSG).

4.5 Anlage 4 (zu § 10)
Datenschutzbericht – Musterinhaltsverzeichnis

Vorbemerkung:

Gemäß § 10 der Muster Datenschutz-Geschäftsordnung ist regelmäßig, mindestens alle zwei Jahre, ein Bericht zum Datenschutz zu erstellen. In diesem Bericht sind u. a. Maßnahmen zur Gewährleistung des Datenschutzes darzustellen und Datenschutzverletzungen aufzuführen. Durch den Bericht wird eine regelmäßige Beurteilung der Datenschutzorganisation der jeweiligen Behörde gewährleistet. Der Bericht ist kein Tätigkeitsbericht des / der behördlichen Datenschutzbeauftragten, durch den der / die Datenschutzbeauftragte Rechenschaft gegenüber der Behördenleitung abgelegt.

Der Bericht umfasst den gesamten Geltungsbereich der Geschäftsordnung und sollte mit Unterstützung des IT-Sicherheitsbeauftragten und der Organisationseinheiten erstellt werden. Die Verschwiegenheitspflicht des / der behördlichen Datenschutzbeauftragten nach Art. 38 Abs. 5 DSGVO, Art. 12 Abs. 2 BayDSG ist zu beachten.

Das nachfolgende Musterinhaltsverzeichnis enthält den sich aus der Geschäftsordnung ergebenden Mindestinhalt und kann beliebig erweitert und ergänzt werden.

Muster Inhaltsverzeichnis

1. Einleitung
2. Technisch-organisatorische Maßnahmen zu Gewährleistung des Datenschutzes
   - Technische Maßnahmen
     - z. B. sicherer Übertragungsweg von Mitteilungen, Nachrichten etc.
   - Organisatorische Maßnahmen
     - Schulungen der Mitarbeiterinnen und Mitarbeiter
     - Erlass von Dienstanweisungen
   - Auftragsverarbeitung
   - Sonstige Maßnahmen
3. Schutzlücken
   - Technisch
   - Organisatorisch
   - Sonstige

4. Datenschutzverstöße, Datenschutzverletzungen
    - Überwachung, Kontrolle
    - Feststellungen
    - Meldungen nach Art. 33 und 34 DSGVO
    - Vertrauliche Meldungen
5. Bewertung der datenschutzrechtlichen Risiken
6. Ausblick und Planung
    - Finanzieller, zeitlicher und personeller Bedarf

5. Schulungen der Beschäftigten und der behördlichen Datenschutzbeauftragten

5.1 Schulung von Beschäftigten

Damit die Vorgaben der DSGVO, des BayDSG und von fachgesetzlichen Datenschutzvorschriften von den Beschäftigten einer Behörde gesetzeskonform umgesetzt werden können, hat der Verantwortliche dafür Sorge zu tragen, dass die Beschäftigten für den Umgang mit personenbezogenen Daten ausreichend sensibilisiert und geschult sind.

Fast alle Beschäftigten einer Behörde verarbeiten so gut wie täglich personenbezogene Daten im Sinne der DSGVO, da dieser Begriff sehr weit zu verstehen ist: Unter ihn fallen nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, also beispielsweise Name und Adresse eines Petenten oder einer Petentin oder auch die dienstlichen Kontaktdaten eines Kollegen oder Kollegin einer anderen Behörde. Der Behördenleitung obliegt es nach § 2 Satz 1 der Muster-Datenschutz-Geschäftsordnung sicherzustellen, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt. Der Verantwortliche muss als solcher nach Art. 5 Abs. 2, Art. 24 Abs. 1 und Art. 32 Abs. 1 DSGVO einen Nachweis dafür erbringen können, dass er geeignete technische und organisatorische Maßnahmen getroffen hat, um die DSGVO-konforme Verarbeitung der personenbezogenen Daten sicherzustellen. Die Sensibilisierung und Schulung von Mitarbeitern und Mitarbeiterinnen gilt als eine entsprechende – wesentliche – Maßnahme (vgl. auch Art. 39 Abs. 1 Buchst. b DSGVO).

Mit welchem Konzept der Verantwortliche diese Schulungspflicht umsetzen kann, ist unter anderem von der Größe der Behörde, dem einhergehenden Stundenumfang sowie der Qualifikation des / der behördlichen Datenschutzbeauftragten abhängig. Sinnvoll ist ein gestuftes Konzept, mithilfe dessen die Beschäftigten auf mehreren Wegen fortlaufend beraten, geschult und sensibilisiert werden.

Als wichtiger Baustein eines solchen Konzeptes kommen je nach Bedarf der Beschäftigten vor allem themenbezogene und praxisorientierte Präsenz- sowie Online-Schulungen in Betracht. Zur Sensibilisierung tragen zudem regelmäßige datenschutzrechtliche Beiträge im Intranet, durch Newsletter oder in Hauszeitschriften bei. Teilweise kann hier auch mit einprägsamen Cartoons und Videoclips gearbeitet werden. Bisweilen werden im Rahmen von Fachschulungen bzw. Facharbeitskreisen auch spezifische Datenschutzthemen mit abgehandelt.

Nach Art. 39 Abs. 1 Buchst. b DSGVO obliegt es der / dem behördlichen Datenschutzbeauftragten zu überwachen, ob ein ausreichendes Schulungskonzept für die an den Verarbeitungsvorgängen beteiligten Beschäftigten vorliegt. Die Vorschrift verlangt nicht direkt, dass der / die behördliche Datenschutzbeauftragte die Schulungen selbst durchführt. Andererseits besteht laut Art. 39 Abs. 1 Buchst. a DSGVO aber auch die Pflicht zur Beratung aller Beschäftigten. Der Übergang von Beratung zur Schulung ist recht fließend. Selbstverständlich sollte der / die behördliche Datenschutzbeauftragte den Verantwortlichen hierbei unterstützen. Der / die behördliche Datenschutzbeauftragte sollte zumindest eine Mithilfe bei der Festlegung von Konzepten sowie bei der Auswahl von geeigneten Durchführenden leisten. Es bietet sich daher an, in der Datenschutz-Geschäftsordnung/Dienstanweisung festzulegen, wer die Aufgabe der Durchführung von Schulungen (generell oder in welchem Umfang) wahrnimmt. Neben dem / der behördlichen Datenschutzbeauftragten kommen auch hausinterne IT-Fachleute oder IT-(Sicherheits-)Beauftragte in Betracht. Wenn der / die behördliche Datenschutzbeauftragte interne Schulungen/Beratungen selbst durchführen soll, ist ihm/ihr natürlich ein entsprechendes Zeitkontingent zu geben. Sind Beauftragungen von Inhouse-Schulungen zur Sensibilisierung für die Beschäftigten unumgänglich, sollte bei der Auswahl der Schulenden auf eine hohe Erfahrung speziell im Bereich der bayerischen öffentlichen Verwaltung geachtet werden. Schulungsunterlagen sollten vorab auf ihre Tauglichkeit geprüft werden, insbesondere muss die Schulung auf den jeweiligen Adressatenkreis zugeschnitten sein und sie muss die Beschäftigten dort abholen, wo sie rechtlich stehen.

Durch den steten Wandel – sowohl im Beschäftigtenpool als auch aufgrund des technischen Fortschritts – sind die Schulungen stets zu wiederholen. Mindestens einmal im Jahr sollte eine Grundschulung (vor allem für neueingestellte Quereinsteiger, Anwärter und Azubis) und regelmäßig auch Auffrischungsschulungen für alle Beschäftigten angeboten werden.

5.2 Schulung des / der behördlichen Datenschutzbeauftragten

Der / die behördliche Datenschutzbeauftragte muss nach Art. 37 Abs. 5 DSGVO Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis vorweisen können. Dies ist nicht zuletzt unerlässlich, damit die Pflichten und Aufgaben in vollständiger Unabhängigkeit ausgeübt werden können.
Nach Art. 38 Abs. 2 DSGVO ist der Verantwortliche verpflichtet, dem / der behördlichen Datenschutzbeauftragten hierfür erforderliche Ressourcen bereit zu stellen.

Dies bedeutet, dem / der Datenschutzbeauftragten sowie der Stellvertretung die für die Aneignung und Erhaltung des Fachwissens erforderlichen Schulungen im Datenschutzrecht und der Datenschutzpraxis zu gewähren sowie die erforderlichen finanziellen Mittel (über Schulungen einschließlich Reisekosten hinaus auch für Gesetzeswerke, Fachzeitschriften usw.) bereit zu stellen.

Die Aufgabenstellung erfordert fortlaufende Schulungen und Erfahrungsaustausch, um neuartige Technologien und veränderte Gesetzesanforderungen zu überblicken.

Alternativ kann auch die externe Beratung durch erfahrene behördliche Datenschutzbeauftragte anderer öffentlicher Stellen in Betracht kommen. Dies bietet sich insbesondere an, wenn neue behördliche Datenschutzbeauftragte erst einer Einarbeitung bedürfen oder der Vollzug der DSGVO in der Behörde noch grundsätzliche Defizite aufweist (fehlende Datenschutzinformationen, kein oder nur bruchstückhaftes Verarbeitungsverzeichnis, fehlende Datenschutzdienstanweisung/-Geschäftsordnung, notwendige Datenschutz-Folgenabschätzungen o.ä.). Eine externe Beauftragung kann auch helfen, Akzeptanzprobleme zu minimieren.

Zusätzlich ist es für behördliche Datenschutzbeauftragte immer gewinnbringend, sich mit behördlichen Datenschutzbeauftragten anderer Behörden auszutauschen – insbesondere wenn sich diese mit gleichgelagerten Verarbeitungsvorgängen befassen. Hier ist die Bildung von regelmäßig tagenden Arbeitskreisen zur Erarbeitung gemeinsamer Lösungen hilfreich. Funktionierende Arbeitskreise gibt es beispielsweise seit Langem für die kreisfreien Städte in Bayern und seit kürzerer Zeit für die Landratsämter. Digitale Plattformen sind durchweg noch im Aufbau begriffen. Es bietet sich an, diese an die Arbeitskreise anzudocken. Beim Austausch mit anderen Behörden ist immer die Verschwiegenheitsverpflichtung des / der behördlichen Datenschutzbeauftragten nach Art. 12 Abs. 2 BayDSG zu beachten. Eine anonymisierte Fallbesprechung wird in jedem Fall ausreichen.

Viele Fragestellungen lassen sich durch einen Blick in die umfangreichen Informationen und Materialien lösen, die vom Bayerischen Landesbeauftragten für den Datenschutz auf dessen Webseite https://www.datenschutz-bayern.de (dort insbesondere unter den Rubriken „Datenschutzreform 2018“, „Themengebiete“ und „Tätigkeitsberichte“) bereitgestellt und regelmäßig aktualisiert werden.

Bei komplizierten Einzelfallfragen im Alltag bietet der Bayerische Landesbeauftragte für den Datenschutz über seinen gesetzlichen Auftrag hinaus im Rahmen seiner personellen Kapazi-

täten seine Unterstützung an. Dieser kann durch den / die behördliche(n) Datenschutzbeauftragte(n) schriftlich oder telefonisch kontaktiert werden. Vorausgesetzt wird allerdings, dass der / die behördliche Datenschutzbeauftragte neben der Ermittlung des Sachverhalts bereits eine eigene rechtliche Bewertung des konkreten datenschutzrechtlichen Problems vorgenommen hat, um diese mit dem Bayerischen Landesbeauftragten für den Datenschutz abzustimmen.

6. Das Verzeichnis der Verarbeitungstätigkeiten[37]

Die DSGVO verlangt von jeder öffentlichen Stelle den Nachweis, dass die von ihr oder in ihrem Auftrag vorgenommenen Verarbeitungen personenbezogener Daten im Einklang mit den datenschutzrechtlichen Vorschriften erfolgen („Rechenschaftspflicht", vgl. Art. 5 Abs. 2 DSGVO). Als ein wesentlicher Bestandteil dieser Rechenschaftspflicht sind alle „Verarbeitungstätigkeiten" einer öffentlichen Stelle in einem Verzeichnis (Verarbeitungsverzeichnis) schriftlich oder elektronisch zu dokumentieren (Art. 30 Abs. 1 DSGVO).

Das Verarbeitungsverzeichnis ist zentraler Ausgangspunkt für den Vollzug des Datenschutzrechts. In ihm wird dokumentiert, welche Kategorien von personenbezogenen Daten verarbeitet werden. Auskunftsersuchen der betroffenen Personen nach Art. 15 DSGVO können beispielsweise nur bearbeitet werden, wenn die öffentliche Stelle weiß, welche Daten sie über welche Personen verarbeitet. Auch für die Erstellung von Formularen, mit denen bei den Bürgern und Bürgerinnen Daten erhoben werden, sind die Angaben im Verarbeitungsverzeichnis hilfreich, da nach Art. 13 Abs. 1 und 2 DSGVO in Erhebungsformularen weitgehend gleiche Angaben zu machen sind, um der Informationspflicht gerecht zu werden.

Das Verarbeitungsverzeichnis ist nach Art. 30 Abs. 1 DSGVO vom Verantwortlichen zu führen, also von der öffentlichen Stelle, die personenbezogene Daten verarbeitet. Der / die behördliche Datenschutzbeauftragte hat nach Art. 12 Abs. 1 Satz 1 Nr. 1 BayDSG Zugang zu dem Verzeichnis. Dies kann auch durch einen Online-Zugriff auf ein elektronisch geführtes Verzeichnis geschehen.

Das Verarbeitungsverzeichnis ist aktuell zu halten. Insofern sollte die öffentliche Stelle dafür Sorge tragen, dass die das Verzeichnis führende Organisationseinheit von Änderungen bei bereits in das Verzeichnis aufgenommenen Verarbeitungstätigkeiten ebenso zeitnah erfährt wie von der Etablierung neuer Verarbeitungstätigkeiten, die einer Aufnahme in das Verzeichnis bedürfen. Die Zusammenarbeit der Fachsachgebiete mit der das Verzeichnis führenden Organisationseinheit sollte möglichst in der Datenschutz-Geschäftsordnung (siehe § 11 des Musters einer Datenschutz-Geschäftsordnung) geregelt werden.

---

[37] Eine ausführliche und detaillierte Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz findet sich unter https://www.datenschutz-bayern.de/datenschutzreform2018/verarbeitungsverzeichnis.html.

Dem Bayerischen Landesbeauftragten für den Datenschutz ist auf Anforderung das Verarbeitungsverzeichnis – bei einem elektronisch geführten Verzeichnis gegebenenfalls in Form von Ausdrucken – zur Verfügung zu stellen (Art. 30 Abs. 4 DSGVO).

6.1 Welche öffentlichen Stellen müssen ein Verarbeitungsverzeichnis führen?

Alle öffentlichen Stellen, die personenbezogene Daten ganz oder teilweise automatisiert verarbeiten oder bei denen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen, müssen ein Verarbeitungsverzeichnis führen. Unerheblich ist, ob die Verarbeitung durch die öffentliche Stelle selbst erfolgt oder von einem Auftragsverarbeiter durchgeführt wird. Die in Art. 30 Abs. 5 DSGVO enthaltene Ausnahme von der Pflicht zur Führung des Verzeichnisses für „Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen“ ist auf öffentliche Stellen nicht anwendbar.

6.2 Weiterverwendung vorhandener Verfahrensverzeichnisse

Die Angaben in den bisher für automatisierte Verfahren nach Art. 27 BayDSG a.F. geführten Verfahrensverzeichnissen **können regelmäßig nicht weiterverwendet werden**, da diese Verzeichnisse sich auf Verfahren und nicht auf Verarbeitungstätigkeiten beziehen und diese oft veraltet sein werden.

6.3 Keine Veröffentlichungspflicht, kein Recht auf Einsichtnahme

Eine Veröffentlichung des Verarbeitungsverzeichnisses ist von der DSGVO nicht vorgesehen. Im Hinblick auf die dort enthaltene Beschreibung der technischen und organisatorischen Maßnahmen könnte eine solche Veröffentlichung auch Geheimhaltungsinteressen berühren.

Ein Recht auf Einsichtnahme in das Verzeichnis enthält die DSGVO ebenfalls nicht. Auskunftsersuchen betroffener Personen, ob und ggf. welche Daten zu ihrer Person von der öffentlichen Stelle verarbeitet werden, sind nach Art. 15 DSGVO zu bearbeiten. Wie andere Behördeninformationen unterliegt das Verzeichnis allerdings auch den allgemeinen Informationszugangsrechten, so dass Auskunftsbegehren über den Inhalt der Verzeichnisse ab diesem Zeitpunkt nach Art. 39 BayDSG und ggf. nach Maßgabe der dort festgelegten Anspruchsbegrenzungen und Ausschlusstatbestände zu beurteilen sind.

6.4 Muster einer Beschreibung einer Verarbeitungstätigkeit nach Art. 30 Abs. 1 DSGVO und Art. 31 BayDSG

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	**Aktenzeichen**	**Stand:**
Verantwortlicher (Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer der öffentlichen Stelle)		
Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)		
Behördliche(r) Datenschutzbeauftragte(r) (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)		

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke
Rechtsgrundlagen

3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten

4. Kategorien der betroffenen Personen

Lfd. Nr.	Betroffene Personen

5. Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

Lfd. Nr.	Empfänger	Anlass der Offenlegung

6. Falls zutreffend: Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Lfd. Nr.	Drittland oder internationale Organisation	Geeignete Garantien im Falle einer Übermittlung nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr.	Löschungsfrist

8. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO, ggf. einschließlich der Maßnahmen nach Art. 8 Abs. 2 Satz 2 BayDSG

Weitere Angaben

9. Nur für Polizei- und Strafjustizbehörden

Erfolgt ein Profiling im Sinne von Art. 4 Nr. 4 DSGVO? ☐ Ja ☐ Nein
Falls ja: Welche Art von Profiling wird durchgeführt?
Besteht für die Verarbeitung eine Errichtungsanordnung? ☐ Ja, ☐ Nein Falls ja, bitte Datum und Aktenzeichen angeben

10. Verantwortliche Organisationseinheit

Dienststelle / Sachgebiet / Abteilung

11. Datenschutz-Folgenabschätzung

Ist für die Form der Verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich? ☐ Ja, ☐ Nein Falls ja, bis wann durchzuführen oder zu überprüfen
Begründung

12. Stellungnahme des / der behördlichen Datenschutzbeauftragten

Liegt eine Stellungnahme des behördlichen Datenschutzbeauftragten vor? ☐ Ja ☐ Nein
Ggf. nähere Erläuterung

6.5 Erläuterungen zum Muster

Welche Verarbeitungstätigkeiten sind in das Verzeichnis aufzunehmen?
Aufzunehmen sind alle *ganz oder teilweise automatisierten Verarbeitungstätigkeiten* – also alle Verarbeitungstätigkeiten, die ganz oder teilweise mit Hilfe von IT-Systemen erfolgen.

Nichtautomatisierte Verarbeitungstätigkeiten sind aufzunehmen, soweit die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO, Art. 2 Satz 2 BayDSG).

„Dateisystem" ist nach Art. 4 Nr. 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist. Diese Voraussetzung wird regelmäßig vorliegen, wenn eine strukturierte Verarbeitungstätigkeit schriftlich oder elektronisch dokumentiert und in einer Registratur gespeichert wird, wie dies bei Behörden üblich ist (vgl. z. B. §§ 12 ff. der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern – AGO). Insbesondere die Verwendung von Vordrucken für die Erhebung von Daten oder den Verwaltungsablauf ist ein Anhaltspunkt für die Pflicht zur Aufnahme in das Verarbeitungsverzeichnis.

Das Verarbeitungsverzeichnis soll einerseits alle Verarbeitungstätigkeiten ausreichend konkret darstellen, anderseits nicht zu kleinteilig sein. Der Begriff der „Verarbeitungstätigkeit" umfasst alle Verarbeitungsschritte, Vorgänge und Vorgangsreihen, die einem gemeinsamen, festgelegten Zweck dienen. Es ist daher nicht zu jedem einzelnen Verarbeitungsschritt bzw. Vorgang oder zu einer Vorgangsreihe ein eigener Verzeichniseintrag zu erstellen. Vielmehr ist ein zusammenfassender Verzeichniseintrag für die durch den Zweck gleichsam „verklammerte" Verarbeitungstätigkeit ausreichend. Insbesondere müssen Verarbeitungsschritte, die nur untergeordnete Hilfsfunktion haben und damit keinem eigenen neuen Zwecken, sondern letztlich nur dem Zweck der eigentlichen Verarbeitungstätigkeit dienen, nicht gesondert aufgeführt werden.

Beispiele für aufzunehmende Verarbeitungstätigkeiten:
- Personalaktenverwaltung
- Beihilfebearbeitung
- Wohngeldbearbeitung
- Bearbeitung von Bauanträgen
- Verwaltung der Zeiterfassung
- Einzelne Videoüberwachungen (auch mit mehreren Kameras, soweit an einem Ort)
- Durchführung von Wahlen und Abstimmungen

- Fahrerlaubnisverwaltung
- Kfz-Zulassung

Zu Nr. 1 (Allgemeine Angaben)
(Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO)

Die Bezeichnung der Verarbeitungstätigkeit soll allgemeinverständlich sein und den jeweiligen Zweck erkennen lassen. Beispiele siehe oben.
„Verantwortlicher" ist die Behörde oder sonstige öffentliche Stelle, die selbst oder mittels eines Auftragsverarbeiters die Verarbeitung durchführt. Die in Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO genannten „Vertreter" beziehen sich auf den Vertreter im Sinne von Art. 4 Nr. 17 DSGVO und sind damit für öffentliche Stellen nicht relevant.
„Gemeinsam für die Verarbeitung Verantwortliche" liegen vor, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen (Art. 26 Abs. 1 Satz 1 DSGVO).
Als „Anschrift" ist jeweils Postleitzahl, Ort, Straße und Hausnummer anzugeben.

Zu Nr. 2 (Zwecke und Rechtsgrundlagen der Verarbeitung)
(Art. 30 Abs. 1 Satz 2 Buchst. b DSGVO; Art. 31 Satz 1 BayDSG)

Die Angabe der Rechtsgrundlagen der Verarbeitungstätigkeit geht über die in Art. 30 Abs. 1 Satz 2 DSGVO aufgeführten Mindestangaben hinaus. Die Angabe dient dem Nachweis, dass diese Frage geprüft wurde. Für Verarbeitungen im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz (vgl. Art. 28 Abs. 1 BayDSG) ist die Angabe der Rechtsgrundlagen demgegenüber verpflichtend (Art. 31 Satz 1 BayDSG).
Soweit keine bereichsspezifische gesetzliche Regelung besteht, kommen als Rechtsgrundlagen die allgemeinen Verarbeitungsbefugnisse nach Art. 4 Abs. 1, Art. 5 Abs. 1 BayDSG, gegebenenfalls auch die unmittelbar geltenden Tatbestände nach Art. 6 Abs. 1 DSGVO in Betracht – bei besonderen Kategorien personenbezogener Daten in Verbindung mit Art. 9 Abs. 2 DSGVO und Art. 8 BayDSG.

Zu Nr. 3 (Kategorien der personenbezogenen Daten)
(Art. 30 Abs. 1 Satz 2 Buchst. c DSGVO)

Unter Kategorien sind aussagefähige Oberbegriffe zu verstehen, z. B. „Name und Vorname", „Anschrift", „Staatsangehörigkeit". Angaben rein technischer Art (z. B. Feldnummern, Schlüsselnummern usw.) sind nicht erforderlich. Die Bezugnahme auf beigefügte Beschreibungen

von Datensätzen ist zulässig, wenn aus diesen die personenbezogenen Daten eindeutig hervorgehen.

Zu Nr. 4 (Kategorien der betroffenen Personen)
(Art. 30 Abs. 1 Satz 2 Buchst. c DSGVO)

Zu beschreiben sind hier Personengruppen, die von der Verarbeitung betroffen sind. Beispiel: „Bauantragsteller" oder „Beihilfeberechtigte und deren Angehörige".
Anzugeben sind auch Personengruppen innerhalb der öffentlichen Stellen, deren Daten verarbeitet werden. Beispiel: „Sachbearbeiter im Bauamt".

Zu Nr. 5 (Kategorien der Empfänger)
(Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO)

Nach Art. 4 Nr. 9 DSGVO ist Empfänger „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht". Zu den Empfängern gehören daher auch Auftragsverarbeiter sowie Stellen innerhalb der Behörde mit anderen Aufgaben, denen die Daten regelmäßig weitergegeben werden oder die regelmäßig Zugriff auf die Daten haben.
Zu beachten ist ferner die Ausnahmeregelung des Art. 4 Nr. 9 Satz 2 DSGVO, wonach Behörden unter bestimmten, in dieser Vorschrift genannten Voraussetzungen nicht als Empfänger gelten.

Zu Nr. 6 (Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation)
(Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO)

Als Drittländer werden alle Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes bezeichnet. Im Falle einer Übermittlung an ein Drittland oder eine internationale Organisation nach Art. 44 DSGVO sind die entsprechenden Rechtsgrundlagen aus Kapitel V (Angemessenheitsbeschluss nach Art. 45 DSGVO, geeignete Garantien in Bezug auf den Schutz personenbezogener Daten nach Art. 46 DSGVO oder eine Ausnahme nach Art. 49 DSGVO) in Spalte 3 festzuhalten. Soweit erforderlich kann dazu auf ergänzende Dokumente verwiesen werden. [38]

[38] Ausführliche Informationen zum Internationalen Datenverkehr finden sich beim LfD, www.datenschutz-bayern.de.

Zu Nr. 7 (Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien)
(Art. 30 Abs. 1 Satz 2 Buchst. f DSGVO)

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke erforderlich ist, für die sie verarbeitet werden (Grundsatz der „Speicherbegrenzung", Art. 5 Abs. 1 Buchst. e DSGVO). Gespeicherte Daten sind daher unverzüglich zu löschen, sobald sie für die Aufgabenerfüllung der öffentlichen Stelle nicht mehr erforderlich sind (vgl. DSGVO-Erwägungsgrund 39). Der Verantwortliche sollte daher Fristen für die Löschung oder regelmäßige Überprüfung der personenbezogenen Daten vorsehen (vgl. DSGVO-Erwägungsgrund 39). Fachgesetzliche Regelungen sind zu beachten.
Über den eigentlichen Speicherungsanlass hinaus (z. B. zur Bearbeitung eines Antrags auf Baugenehmigung) kann eine Speicherung auch zur Erfüllung von Dokumentationspflichten oder von archivrechtlichen Anbietungspflichten (vgl. Art. 26 Abs. 6 BayDSG) erforderlich sein.
Anzugeben ist auch der Beginn der Löschungsfrist.

Zu Nr. 8 (Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO ggf. einschließlich der Maßnahmen nach Art. 8 Abs. 2 Satz 2 BayDSG)
(Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO; Art. 8 Abs. 2 Satz 2 BayDSG)

Hier sind die technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO allgemein zu beschreiben. Trotz der in Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO verwendeten Formulierung „wenn möglich" hat der Verantwortliche hier in aller Regel Angaben zu machen, da er ohnehin verpflichtet ist, „geeignete technische und organisatorische Maßnahmen" zu treffen. Entsprechende Informationen werden dem Verantwortlichen daher in aller Regel vorliegen.
Eine Beschreibung von Maßnahmen nach Art. 8 Abs. 2 Satz 2 BayDSG ist erforderlich, wenn besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden.
Aus datenschutzrechtlicher Sicht zentral ist insbesondere die Fähigkeit, die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Es ist zulässig und oft auch ausreichend, wenn dazu und im Hinblick auf die weiteren in Art. 32 Abs. 1 DSGVO genannten Maßnahmen auf ein vorhandenes Informationssicherheitskonzept verwiesen wird (vgl. den bisher geltenden Art. 11 Abs. 1 Satz 2 BayEGovG sowie den künftig geltenden Art. 43 Abs. 1 Satz 2 BayDiG-E).

Zu Nr. 9. (Nur für Verarbeitungen durch Polizei- und Strafjustizbehörden)
(Art. 31 Satz 1 BayDSG)

Angaben zum Profiling sind nur erforderlich, wenn bei Verarbeitungen im Sinne des Art. 28 Abs. 1 BayDSG im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz ein Profiling erfolgt. Relevant kann dies für Behörden der Polizei, Gerichte in Strafsachen und Staatsanwaltschaften, Strafvollstreckungs- und Justizvollzugsbehörden sowie Behörden des Maßregelvollzugs sein, soweit diese personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit verarbeiten. Sonstige Behörden können nur betroffen sein, soweit diese personenbezogene Daten verarbeiten, um Straftaten oder Ordnungswidrigkeiten zu verfolgen oder zu ahnden.

„Profiling“ ist nach Art. 4 Nr. 4 DSGVO „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.
Errichtungsanordnungen werden nach Art. 64 Abs. 1 PAG erstellt.

Zu Nr. 10 (Verantwortliche Organisationseinheit)

Hier ist die Dienststelle, das Referat oder die sonstige Organisationseinheit der öffentlichen Stelle anzugeben, in der die Verarbeitungstätigkeit erfolgt. Beispiele: „Personalreferat“ oder „Bauamt“.

Zu Nr. 11 (Datenschutz-Folgenabschätzung)

Die Angabe, ob eine Datenschutz-Folgenabschätzung für die Verarbeitungstätigkeit durchzuführen ist, geht über die in Art. 30 Abs. 1 Satz 2 DSGVO aufgeführten Mindestangaben für die Beschreibung von Verarbeitungstätigkeiten hinaus. Sie dient dem Nachweis, dass diese Frage in Abstimmung mit dem / der behördlichen Datenschutzbeauftragten geprüft wurde.

Welches Risiko für die Rechte und Freiheiten natürlicher Personen von einer beabsichtigten Verarbeitung personenbezogener Daten ausgeht und wie dieses Risiko bewältigt werden kann, ist vor jeder Verarbeitung zu prüfen. Eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 Satz 1 DSGVO ist dagegen nur durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. Diese Voraussetzung wird nur bei wenigen Verarbeitungstätigkeiten vorliegen. Für Polizeibehörden richtet sich die Datenschutz-Folgenabschätzung nach Art. 64 Abs. 2 PAG.

Die Datenschutz-Folgenabschätzung ist „vorab“, d.h. vor dem erstmaligen Einsatz einer Verarbeitung durchzuführen. Für bereits laufende Verarbeitungen, die ohne wesentliche Änderungen fortgeführt werden und die eine Datenschutz-Folgenabschätzung erfordern, ist diese **wie unter 12.2.5 dargestellt** nachzuholen.

Kapitel 12 dieser Arbeitshilfen enthält weitere Hinweise zu den Voraussetzungen und der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.

Zu Nr. 12 (Stellungnahme des / der behördlichen Datenschutzbeauftragten)

Dem / Der behördlichen Datenschutzbeauftragten ist vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben (Art. 12 Abs. 1 Satz 1 Nr. 2 BayDSG). Eine Stellungnahme des / der behördlichen Datenschutzbeauftragten ist nach Art. 24 Abs. 5 BayDSG auch vor dem Einsatz einer Videoüberwachung einzuholen.

7. Die Informationspflichten des Verantwortlichen nach Art. 13 und 14 DSGVO[39]

7.1 Allgemeines

Die DSGVO verpflichtet den Verantwortlichen zur Information der betroffenen Person

- wenn personenbezogene Daten bei der betroffenen Person selbst erhoben werden (Art. 13 Abs. 1 und 2 DSGVO),
- wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden (also z. B. bei Dritten oder aus öffentlich zugänglichen Quellen, Art. 14 Abs. 1 und 2 DSGVO) und
- vor einer Weiterverarbeitung von Daten zu einem anderen Zweck als dem, der bei der Erhebung zugrunde lag (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).

Es besteht keine generelle rechtliche Verpflichtung, unabhängig von einer solchen Erhebung oder Weiterverarbeitung für einen anderen Zweck die Betroffenen über die Verarbeitung ihrer Daten zu informieren.

Die Informationen sind nach Art. 12 Abs. 1 Satz 1 DSGVO in präziser, transparenter, verständlicher, leicht zugänglicher Form und in einer klaren und einfachen Sprache zu erteilen. Bei Informationen, die sich speziell an Kinder richten, ist eine für Kinder verständliche Sprache zu verwenden.

Im Fachrecht bestehen teilweise Sondervorschiften zu den Informationspflichten, so z. B. in §§ 32a, 32b und 32d AO, in §§ 82 und 82a des SGB X und in Art. 28 Abs. 3 Nr. 2 BayDSG bei der Verfolgung und Ahndung von Ordnungswidrigkeiten.

7.2 Wann ist zu informieren?

Im Fall der Erhebung bei der betroffenen Person selbst sind dieser die Informationen zum Zeitpunkt der Erhebung mitzuteilen (Art. 13 Abs. 1 DSGVO) bzw. zur Verfügung zu stellen (Art. 13 Abs. 2 DSGVO).

---

[39] Eine ausführliche und detaillierte Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz findet sich unter https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Informationspflichten.pdf; die „Leitlinien für Transparenz gemäß der Verordnung 2016/679“ der Art. 29-Gruppe (WP 260 rev.01) sind abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/wp260rev01_de.pdf.

Bei einer Erhebung nicht bei der betroffenen Person sind der betroffenen Person innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats die Informationen mitzuteilen bzw. zur Verfügung zu stellen (Art. 14 Abs. 3 Buchst. a DSGVO). Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen (etwa in einem Anschreiben), ist die Information spätestens zum Zeitpunkt der ersten Mitteilung zu erteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, ist die Information spätestens zum Zeitpunkt der ersten Offenlegung zu erteilen (Art. 14 Abs. 3 Buchst. b und c DSGVO).

Bei einer beabsichtigten Weiterverarbeitung von Daten zu einem anderen Zweck als dem, der bei der Erhebung zugrunde lag, ist die betroffene Person vor der Weiterverarbeitung zu informieren (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).

7.3 Wann werden personenbezogene Daten „erhoben“?

Eine Erhebung von Daten liegt grundsätzlich nur vor, wenn der Verantwortliche sich Daten zu einer oder mehreren Personen zielgerichtet beschafft. Auch das Bereitstellen eines Online-Formulars auf einer Internetseite oder eines Papierformulars, das die betroffene Person ausfüllt und an die öffentliche Stelle sendet oder bei der jeweiligen Dienststelle abgibt, ist als Erhebung anzusehen. Keine Erhebung liegt zunächst vor, wenn dem Verantwortlichen die Daten von der betroffenen Person selbst oder von Dritten ohne vorherige Aufforderung übermittelt werden.

7.4 Ausnahmen von der Informationspflicht

Allgemeine Ausnahmen von den Informationspflichten finden sich in Art. 13 Abs. 4, Art. 14 Abs. 5 DSGVO sowie in Art. 9 Abs. 1 BayDSG:

Eine Information der betroffenen Person ist nicht erforderlich, wenn und **soweit** die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4, 14 Abs. 5 Buchst. a DSGVO):

- In einem Verwaltungsverfahren ist es grundsätzlich ausreichend, die betroffene Person zu Beginn des Verfahrens – in der Regel bei Antragseinreichung – zu informieren. Sollten sich im weiteren Verfahren Rückfragen ergeben, die zu einer erneuten Datenerhebung bei der betroffenen Person führen, löst dies in der Regel keine neue Informationspflicht aus.

- Eine Information der betroffenen Person ist nicht erforderlich, **soweit** sich die Informationen eindeutig aus den Umständen der Erhebung ergeben.
- Auch bei wiederholten Erhebungen, die dem gleichen Zweck dienen, kann in der Regel vorausgesetzt werden, dass die betroffene Person bereits über die Information verfügt und eine Wiederholung der Information nicht erforderlich ist, z. B. bei wiederholten Lebensmittelkontrollen im gleichen Betrieb, bei wiederholten Hausbesuchen in der Jugend- und Familienhilfe usw.

Eine Pflicht zur Information der betroffenen Person besteht nach Art. 9 Abs. 1 i.V.m. Art. 6 Abs. 2 Nr. 3 Buchst. a, b und d BayDSG auch nicht, soweit und solange dies erforderlich ist

- zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung,
- zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen i.S. d. § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldbescheiden sowie
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person.

In Bezug auf die Informationspflicht nach Art. 14 Abs. 1 sieht Art. 14 Abs. 5 DSGVO noch weitere Ausnahmen von der Informationspflicht vor. Danach kann eine Information der betroffenen Person auch unterbleiben, wenn und soweit

- die Erteilung einer Information sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert, insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für Statistikzwecke (Art. 14 Abs. 5 Buchst. b DSGVO),
- die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen vorsehen, ausdrücklich geregelt ist (Art. 14 Abs. 5 Buchst. c DSGVO) oder
- die personenbezogenen Daten einem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen (z. B. für Notare, Art. 14 Abs. 5 Buchst. d DSGVO).

Weitere Ausnahmen können sich aus Fachgesetzen ergeben, z. B. aus §§ 32a ff. AO oder aus Art. 28 Abs. 3 Nr. 2 BayDSG bei der Verfolgung und Ahndung von Ordnungswidrigkeiten.

Sieht ein Verantwortlicher unter Berufung auf einen Ausschlusstatbestand von der Information der betroffenen Person ab, muss er im Rahmen seiner Rechenschaftspflicht (vgl. Art. 5 Abs. 2 DSGVO) nachweisen können, dass die Voraussetzungen des jeweiligen Ausschlusstatbestandes vorgelegen haben.

7.5 Die Informationspflichten bei der Erhebung bei der betroffenen Person

7.5.1 Erhebungen auf Papierformularen

Die betroffene Person kann über alle nach Art. 13 Abs. 1 und 2 DSGVO mitzuteilenden oder zur Verfügung zu stellenden Angaben auf dem jeweiligen Antrags- oder sonstigen Erhebungsformular oder durch ein zusätzliches Hinweispapier informiert werden. Dies ist allerdings rechtlich nicht erforderlich, sehr aufwendig und wird daher in der Regel nicht zweckmäßig sein.

Es ist daher eine Aufteilung zu empfehlen in Informationen, die direkt auf dem Erhebungsformular stehen bzw. aus diesem hervorgehen, und weitergehenden Informationen, die von der erhebenden Behörde im Internet oder auf sonstige Weise zur Verfügung gestellt werden:

- Der Verantwortliche und die Zwecke, für die die Daten erhoben werden, müssen aus einem Erhebungsformular hervorgehen. Aufgrund der Transparenzvorgabe des Art. 12 Abs. 1 DSGVO sollte die öffentliche Stelle regelmäßig den Verantwortlichen, dessen Kontaktdaten und den Zweck auf dem Formular explizit nennen.
- Ergänzend ist auf dem Erhebungsformular anzugeben, wo weitere Informationen erhältlich sind, z. B. auf einer konkret anzugebenden Internetseite oder beim zuständigen Sachbearbeiter / der zuständigen Sachbearbeiterin der Behörde. Zulässig ist auch eine Aufteilung dieser weiteren Informationen in allgemeine Informationen (z. B. auf einer Internetseite) verbunden mit dem Hinweis, wo konkrete Informationen zum Einzelfall erhältlich sind (z. B. beim zuständigen Sachbearbeiter / der zuständigen Sachbearbeiterin).
- Gemäß Art. 12 Abs. 1 Satz 1 DSGVO sind die Informationen in „leicht zugänglicher Form“ zur Verfügung zu stellen. Wird auf eine Internetseite verwiesen, ist somit in aller Regel die Angabe eines Direktlinks erforderlich, so dass sich eine betroffene Person nicht erst mühsam zu den für sie relevanten Informationen durchklicken muss. Da zudem nicht davon ausgegangen werden kann, dass jede betroffene Person über einen Internetzugang verfügt, ist eine alternative Bezugsmöglichkeit vorzuhalten bzw. anzugeben. Bei Verweis auf einen „zuständigen Sachbearbeiter“ muss zumindest aus den Umständen

eindeutig hervorgehen, wer der jeweils zuständige Sachbearbeiter ist bzw. wie dieser unmittelbar erreicht werden kann, damit die betroffene Person dies nicht erst aufwändig ermitteln muss.

Beispiel für die Formulierung einer Information nach Art. 13 DSGVO auf Erhebungsvordrucken:
„Verantwortlich für die Verarbeitung ist …Wir verarbeiten Ihre Daten um (Angabe des Verwendungszwecks).
Weitere Informationen über die Verarbeitung Ihrer Daten und Ihre Rechte bei der Verarbeitung Ihrer Daten können Sie im Internet unter … (Angabe einer Internetadresse) abrufen. Weitere Informationen erhalten Sie bei Bedarf von Ihrem zuständigen Sachbearbeiter / Ihrer zuständigen Sachbearbeiterin."

7.5.2 Erhebungen im Internet

Bei der Erhebung personenbezogener Daten auf einer Internetseite reicht es aus, wenn auf der Erhebungsseite ein deutlich sichtbarer Link auf die Informationen nach Art. 13 Abs. 1 und 2 DSGVO enthalten ist. Zu unterscheiden sind dabei

- Informationen über die Verarbeitung personenbezogener Daten des Internetnutzers / der Internetnutzerin durch den Betrieb der Internetseite allgemein (vgl. dazu die Ausführungen in Teil B des Musters einer Datenschutzerklärung, für Internetseiten staatlicher Behörden, Kapitel 14 dieser Arbeitshilfen) und
- falls zutreffend: Informationen zur Verarbeitung personenbezogener Daten, die auf der Internetseite für spezielle Verarbeitungen erhoben werden (z. B. Online-Anträge).

Beispiel:
„Informationen zur Verarbeitung Ihrer Daten und zu Ihren diesbezüglichen Rechten finden Sie auf unserer Datenschutzerklärung unter … (Angabe einer Internetadresse)."

7.5.3 Mündliche Datenerhebungen

Auch bei mündlichen Datenerhebungen besteht die Informationspflicht nach Art. 13 DSGVO. Die betroffene Person muss auch hier stets erkennen können, wer der Verantwortliche ist und für welchen Zweck die Daten erhoben werden. Sofern sich dies nicht aus den Umständen ergibt oder der betroffenen Person nicht ohnehin bekannt ist, ist dies mitzuteilen.
Der betroffenen Person gegenüber ist anzugeben, wo weitergehende Informationen zur Verfügung gestellt werden.

7.6 Die Informationspflichten bei der Erhebung nicht bei der betroffenen Person

Eine Erhebung von Daten nicht bei der betroffenen Person kann aus allgemein zugänglichen Quellen erfolgen (z. B. aus Zeitungen, dem öffentlich zugänglichen Internet oder durch Besichtigungen) oder durch Befragung von Dritten. Eine Erhebung von Daten nicht bei der betroffenen Person i.S.v. Art. 14 DSGVO liegt damit jedenfalls auch vor, wenn Daten von einer öffentlichen Stelle oder nicht öffentlichen Stelle auf Anfrage übermittelt werden.

Informationen über Dritte, die nicht am Verfahren beteiligt sind:
Werden anlässlich einer Erhebung von Daten zu einer Person auch Daten Dritter erhoben, löst dies jedenfalls dann keine Informationspflicht nach Art. 14 DSGVO gegenüber diesen Dritten aus, wenn dieser „Beifang" lediglich als unselbständiger Teil der Daten der betroffenen Person verarbeitet wird und eine Information dieser Dritter einen unverhältnismäßigen Aufwand im Sinn des Art. 14 Abs. 5 Buchst. b DSGVO verursachen würde.[40]

Beispiele:

- Für die Durchführung eines Verwaltungsverfahrens ist die Geburtsurkunde der betroffenen Person erforderlich. Auf dieser sind Daten der Eltern der betroffenen Person enthalten.
  Wenn und soweit eine Verarbeitung dieser Daten außerhalb dieses Verwaltungsverfahrens nicht erfolgt, besteht regelmäßig keine Informationspflicht gegenüber den Eltern.
- Bei der Einstellung eines Beamten oder Beschäftigten werden zur Berechnung des Familienzuschlags Angaben zum Ehepartner oder der Ehepartnerin / Lebenspartner oder der Lebenspartnerin und zu Kindern erhoben.
  Wenn und soweit eine Verarbeitung dieser Daten für einen anderen Zweck nicht erfolgt, besteht regelmäßig keine Informationspflicht gegenüber dem Ehepartner oder der Ehepartnerin / dem Lebenspartner oder der Lebenspartnerin oder den Kindern nach Art. 14 DSGVO.
- Bei der Vorlage eines Attests wird der Name des ausstellenden Arztes / der ausstellenden Ärztin erfasst.
  Eine Informationspflicht gegenüber dem Arzt / der Ärztin besteht unter der oben genannten Voraussetzung in der Regel nicht.

[40] Vgl. auch Nr. 62 der „Leitlinien für Transparenz gemäß der Verordnung 2016/679" (WP 260) der Art. 29-Gruppe, https://www.datenschutz-bayern.de/datenschutzreform2018/wp260rev01_de.pdf.

7.7 Die Informationspflichten bei einer Zweckänderung

Beabsichtigt der Verantwortliche, personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so hat er der betroffenen Person vor dieser Weiterverarbeitung Informationen über den anderen Zweck und weitere Informationen zur Verfügung zu stellen (Art. 13 Abs. 3 DSGVO bzw. Art. 14 Abs. 4 DSGVO).

Generell liegt keine Zweckänderung vor, wenn Daten für die in Art. 6 Abs. 1 BayDSG angegebenen Zwecke der Aufsicht und Kontrolle, Erstellung von Geschäftsstatistiken, Rechnungsprüfung, Prüfung oder Wartung automatisierter Verfahren der Datenverarbeitung und zur Gewährleistung der Netz- und Informationssicherheit sowie, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen, zu eigenen Ausbildungs- und Prüfungszwecken verwendet werden.
Diese Zwecke werden bei einer Verarbeitung personenbezogener Daten durch öffentliche Stellen als Ausfluss ihrer Funktion und organisationsrechtlichen Grundstrukturen neben dem jeweiligen aufgabenbezogenen Hauptzweck regelmäßig mitverfolgt und müssen nicht angegeben werden.

Keine Zweckänderung ist insbesondere auch die Weitergabe personenbezogener Daten an die in einem Verwaltungsverfahren beteiligten Dienststellen einer Behörde oder die zur Kostenabrechnung zuständigen Stellen. Auch die Beteiligung des örtlichen Personalrats im Rahmen dessen Mitbestimmungs- /Mitwirkungsrechte stellt keine Zweckänderung dar.
Bei einer Zweckänderung innerhalb der öffentlichen Stelle, die die Daten bei der betroffenen Person erhoben hat, ist die betroffene Person auf den beabsichtigten neuen Verarbeitungszweck hinzuweisen und es sind ihr die maßgeblichen Informationen nach Art. 13 Abs. 2 DSGVO zur Verfügung zu stellen. Bei einer Zweckänderung innerhalb der öffentlichen Stelle, die Daten nicht bei der betroffenen Person erhoben hat, ist die betroffene Person auf den beabsichtigten neuen Verarbeitungszweck hinzuweisen und es sind ihr die maßgeblichen Informationen nach Art. 14 Abs. 2 DSGVO zur Verfügung zu stellen. Auch diese Informationen können ggf. (teilweise) durch Angabe einer Internetadresse erfolgen, auf der die Informationen abrufbar sind.

Keine Informationspflicht besteht jedenfalls bei der Übermittlung von Daten an eine andere öffentliche Stelle auf deren Ersuchen, soweit damit keine Änderung des Erhebungszwecks verbunden ist. Eine solche Datenübermittlung löst keine Informationspflicht bei der datenabgebenden Stelle aus. In diesem Fall hat der Datenempfänger die Information der betroffenen Person nach Art. 14 DSGVO sicherzustellen und dabei unter Nr. 5 „Angabe der Quelle“ darzulegen, von welcher anderen Stelle die Daten übermittelt wurden.

7.8 Sonderfall: Informationspflicht bei einer Videoüberwachung[41]

Eine besondere Regelung der Informationspflicht enthält Art. 24 Abs. 2 BayDSG für die Videoüberwachung. Setzen bayerische öffentliche Stellen Anlagen zur Videoüberwachung ein, so sind diese durch geeignete Maßnahmen erkennbar zu machen (z. B. durch Hinweisschilder oder Piktogramme nach DIN 33450). Dabei ist der Verantwortliche anzugeben, wenn er nicht aus den Umständen hervorgeht (Art. 24 Abs. 2 Satz 2 BayDSG).
Zusätzlich ist eine Information der von einer Videoüberwachung betroffenen Personen nach Art. 13 bzw. 14 DSGVO erforderlich. Es bietet sich daher an, das Hinweisschild um eine verknüpfende Information zu ergänzen (z. B. einen Hinweis auf einen Schaukasten mit den vollständigen Datenschutzhinweisen, die Angabe einer Internetadresse und/oder eines QR-Codes).

[41] Eine Orientierungshilfe zur Videoüberwachung durch bayerische öffentliche Stellen des Bayerischen Landesbeauftragten findet sich unter https://www.datenschutz-bayern.de/3/oh_video.pdf.

7.9 Die Informationspflichten in Art. 13 und 14 DSGVO im Einzelnen

Wesentliche Angaben zur Erfüllung der Informationspflichten decken sich mit den Angaben im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO und können daher aus der jeweiligen Beschreibung der Verarbeitungstätigkeit übernommen werden. Textvorschläge für die einzelnen Informationspflichten sind:

Linke Spalte: Textvorschlag Rechte Spalte: Ausfüllhinweise

1. Bezeichnung der Verarbeitungstätigkeit

Datenschutzhinweise im Zusammenhang mit … (*Bauantrag, Beihilfeantrag usw.*)	*Entspricht regelmäßig der Bezeichnung der Verarbeitungstätigkeit in Nr. 1 des Verarbeitungsverzeichnisses.*

2. Name und Kontaktdaten des Verantwortlichen

Verantwortlich für die Verarbeitung ist … ***Name, Postanschrift, E-Mail-Adresse und Telefonnummer der öffentlichen Stelle*.**	*Entspricht der Angabe des Verantwortlichen im Verarbeitungsverzeichnis.* *Es ist ausreichend, wenn der Verantwortliche in allgemeiner Form bezeichnet wird, z. B.: „Verantwortlich für die Verarbeitung ist Ihr zuständiges Landratsamt / Ihre zuständige Gemeindeverwaltung“.* [42] *Kontaktdaten müssen gleichwohl eindeutig angegeben werden bzw. aus den Umständen hervorgehen.*

3. Kontaktdaten des / der Datenschutzbeauftragten

Dienstliche Anschrift, E-Mail-Adresse und Telefonnummer des / der behördlichen Datenschutzbeauftragten.	*Entspricht der Angabe im Verarbeitungsverzeichnis. Der Name des / der behördlichen Datenschutzbeauftragten muss hier nicht genannt werden* *Für den / die behördlichen Datenschutzbeauftragten wird die Einrichtung einer Funktions-E-Mail-Adresse empfohlen.*

[42] Ausnahme: § 67 Abs. 4 Satz 2 SGB X (siehe Fußnote 2); konkrete Benennung der verantwortlichen Organisationseinheit erforderlich.

4. Zwecke und Rechtsgrundlagen der Verarbeitung

4a) Zwecke der Verarbeitung: **Ihre Daten werden dafür erhoben, um ...** **(Zwecke aufzählen, ggf. mit Spiegelstrichen).**	*Entspricht Nr. 2 im Verarbeitungsverzeichnis.* *Es empfiehlt sich, hier möglichst alle (auch vorhersehbare zukünftige Zwecke) mit anzuführen, um eine erneute Informationspflicht nach Art. 13 Abs. 3 DSGVO bei Zweckänderungen zu vermeiden. Die Zwecke müssen hinreichend bestimmt und eindeutig bezeichnet sein (Art. 5 Abs. 1 Buchst. b DSGVO).*
4b) Rechtsgrundlagen der Verarbeitung **Rechtsgrundlage der Verarbeitung ist Art. …**	*Entspricht Nr. 2 im Verarbeitungsverzeichnis* *Soweit keine gesetzliche Regelung im bereichsspezifischen (z. B. SGB X) oder allgemeinen nationalen Datenschutzrecht (wie etwa auch Art. 4 Abs. 1 BayDSG) besteht, kommen als Rechtsgrundlagen die unmittelbar geltenden Tatbestände nach Art. 6 Abs. 1 DSGVO – bei besonderen Kategorien personenbezogener Daten in Verbindung mit Art. 9 Abs. 2 DSGVO, Art. 8 BayDSG in Betracht.* *Nach Art. 4 Abs.1 BayDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.* *Sind mehrere Rechtsgrundlagen einschlägig, so sollte der Verantwortliche alle nennen. Zu beachten ist, dass bereichsspezifische Rechtsgrundlagen dem BayDSG vorgehen.* *Die Rechtsgrundlage zur Verarbeitung im berechtigten Interesse des Verantwortlichen (Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO) kommt für Behörden im Rahmen ihrer hoheitlichen Aufgaben **nicht** in Betracht (Art. 6 Abs. 1 Unterabs. 2 DSGVO).*

5. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Ihre personenbezogenen Daten werden weitergegeben an: – **… (Empfänger innerhalb der Behörde/ Kommune)** – **… (Auftragsverarbeiter)** – **… (Dritte)**	*Entspricht Nr. 5 im Verarbeitungsverzeichnis* *Als Empfänger gelten:* – *andere Organisationseinheiten mit anderen Aufgaben innerhalb der öffentlichen Stelle,* – *Auftragsverarbeiter,* – *Dritte außerhalb der öffentlichen Stelle.*

, um …	*Es empfiehlt sich eine kurze Erläuterung, warum die Daten den Empfängern offengelegt werden. Evtl. ist darauf auch schon bei Nr. 4 einzugehen (Zwecke und Rechtsgrundlagen).*

6. Übermittlung von personenbezogenen Daten an ein Drittland

Es ist geplant, Ihre personenbezogenen Daten an … (*ein Drittland/eine internationale Organisation*) zu übermitteln. **Textvorschlag bei vorliegendem Angemessenheitsbeschluss (Art. 45 DSGVO):** **Die EU-Kommission hat am … beschlossen, dass die personenbezogenen Daten in … genauso geschützt sind wie in der Europäischen Union.**	*Entspricht Nr. 6 im Verarbeitungsverzeichnis* *Drittländer sind Länder außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums.* *Bei einer Datenübermittlung in Drittländer sind die Zulässigkeitsvoraussetzungen des Kapitel V, Art. 44 bis 50 der DSGVO zu beachten.* *Angemessenheitsbeschlüsse der EU-Kommission nach Art. 45 DSGVO sind auf der Website der EU-Kommission abrufbar (unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).* *Eine zulässige Veröffentlichung personenbezogener Daten im Internet ist keine Übermittlung von personenbezogenen Daten an ein Drittland in diesem Sinne.*

7. Dauer der Speicherung der personenbezogenen Daten

Ihre Daten werden nach der Erhebung … (*für 1 Jahr, längstens … Jahre, bis zur Volljährigkeit usw.*) gespeichert. **Alternative, falls keine Fristen benennbar sind:** **Ihre Daten werden von uns so lange gespeichert, wie dies unter Beachtung der gesetzlichen Aufbewahrungsfristen gemäß (*Angabe der Vorschriften*) für die jeweilige Aufgabenerfüllung erforderlich ist; in der Regel bewahren wir Ihre Daten … Jahre auf.**	*Entspricht Nr.7 im Verarbeitungsverzeichnis* *Anzugeben ist regelmäßig der Zeitpunkt, zu dem die Daten zur Erfüllung des Fachrechts einschließlich evtl. bestehender Dokumentations- oder Aufbewahrungspflichten nicht mehr erforderlich sind. Nicht ausreichend wäre eine Speicherdauer nur bis zum Abschluss des konkreten „Arbeitsschrittes", beispielsweise der Erteilung der Baugenehmigung. Die Erfüllung von Dokumentationspflichten ist regelmäßig Teil der Aufgabenerfüllung. Behörden und öffentliche Stellen haben daneben die Grundsätze der ordnungsgemäßen Aktenführung insbesondere der Aktenvollständigkeit zu berücksichtigen.* *Wenn für die Speicherdauer im konkreten Fall allgemein bekannte, gesetzliche Vorgaben bestehen, kann auf diese verwiesen werden.*

	Hier sind möglichst genaue Angaben zu machen. *Nur im Ausnahmefall sollte die allgemeine Formulierung (Alternative) verwendet werden.* *Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem Archiv anzubieten, darf eine Löschung erst erfolgen, nachdem die Unterlagen einem Archiv angeboten wurden (Art. 26 Abs. 6 BayDSG).*

8. Betroffenenrechte

Fehler! Linkreferenz ungültig.Hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten stehen Ihnen als einer betroffenen Person die nachfolgend genannten Rechte gemäß Art. 15 ff. DSGVO zu: **Sie können Auskunft darüber verlangen, ob wir personenbezogene Daten von Ihnen verarbeiten. Ist dies der Fall, so haben Sie ein Recht auf Auskunft über diese personenbezogenen Daten sowie auf weitere mit der Verarbeitung zusammenhängende Informationen (Art. 15 DSGVO). Bitte beachten Sie, dass dieses Auskunftsrecht in bestimmten Fällen eingeschränkt oder ausgeschlossen sein kann (vgl. insbesondere Art. 10 BayDSG).** **Für den Fall, dass personenbezogene Daten über Sie nicht (mehr) zutreffend oder unvollständig sind, können Sie eine Berichtigung und gegebenenfalls Vervollständigung dieser Daten verlangen (Art. 16 DSGVO).** **Bei Vorliegen der gesetzlichen Voraussetzungen können Sie die Löschung Ihrer personenbezogenen Daten (Art. 17 DSGVO) oder die Einschränkung der Verarbeitung dieser Daten (Art. 18 DSGVO) verlangen. Das Recht auf Löschung nach Art. 17 Abs. 1 und 2 DSGVO besteht jedoch unter anderem dann nicht, wenn die Verarbeitung personenbezogener Daten erforderlich ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher**	*Bei einzelnen Verarbeitungstätigkeiten können sich Einschränkungen der genannten Rechte ergeben. Schließen fachgesetzliche Vorschriften die in der linken Spalte genannten Rechte der betroffenen Person aus, sind die Formulierungen entsprechend anzupassen.* *Beispiel: kein Recht auf Berichtigung gem. Art. 16 DSGVO bei Verarbeitungen zu Archivzwecken (vgl. Art. 26 Abs. 4 Satz 1 BayDSG).* *Aufsichtsbehörde für bayerische öffentliche Stellen ist der Bayerische Landesbeauftragte für den Datenschutz (im Detail vgl. Art. 15 Abs. 1 BayDSG), sofern bereichsspezifisch nichts anderes bestimmt ist (vgl. etwa § 32h AO).* *Bezüglich des Widerspruchsrechts nach Art. 21 DSGVO kann der diesbezüglichen gesonderten Hinweispflicht des Art. 21 Abs. 4 DSGVO auch im Rahmen einer Information nach Art. 13 DSGVO nachgekommen werden. Da der Hinweis nach Art. 21 Abs. 4 DSGVO in einer „von anderen Informationen getrennten Form zu erfolgen" hat, ist in diesem Fall über das Widerspruchsrecht in einem eigenen und nach Möglichkeit (zum Beispiel mittels Fettdrucks) optisch hervorgehobenen Absatz zu informieren.*

Gewalt erfolgt (Art. 17 Abs. 3 Buchst. b DSGVO). **Aus Gründen, die sich aus Ihrer besonderen Situation ergeben, können Sie der Verarbeitung Sie betreffender personenbezogener Daten durch uns zudem jederzeit widersprechen (Art. 21 DSGVO). Sofern die gesetzlichen Voraussetzungen vorliegen, verarbeiten wir in der Folge Ihre personenbezogenen Daten nicht mehr.** **Weitere Einschränkungen, Modifikationen und gegebenenfalls Ausschlüsse der vorgenannten Rechte können sich aus der Datenschutz-Grundverordnung oder nationalen Rechtsvorschriften ergeben.** **Sie haben das Recht, sich bei einer Aufsichtsbehörde im Sinn des Art. 51 DSGVO über die Verarbeitung Ihrer personenbezogenen Daten zu beschweren. Zuständige Aufsichtsbehörde für bayerische öffentliche Stellen ist der Bayerische Landesbeauftragte für den Datenschutz, erreichbar unter Postfach 22 12 19, 80502 München oder https://www.datenschutz-bayern.de/service/complaint.html.**	

9. Widerrufsrecht bei Einwilligung

Wenn Sie in eine Verarbeitung personenbezogener Daten durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.	*Diese Information ist nur zu erteilen, wenn die Verarbeitung auf einer Einwilligung der betroffenen Person beruht (Art. 6 Abs.1 Unterabs. 1 Buchst. a oder Art. 9 Abs. 2 Buchst. a DSGVO).*

10. Pflicht/Keine Pflicht zur Bereitstellung der Daten

Sie sind dazu verpflichtet, Ihre Daten anzugeben. Diese Verpflichtung ergibt sich aus … (*Gesetz, Vertrag*). **Wir benötigen Ihre Daten, um … (*z. B. Ihren Antrag auf … zu bearbeiten, den Vertrag mit Ihnen abschließen zu können*).**	*Diese Information ist abhängig davon zu geben, ob die betroffene Person dazu **verpflichtet** ist, die personenbezogenen Daten anzugeben. Die Verpflichtung kann sich aus Gesetz oder Vertrag ergeben oder für einen Vertragsabschluss erforderlich sein.*

Wenn Sie die erforderlichen Daten nicht angeben, ... – **kann Ihr Antrag nicht bearbeitet werden,** – **kann der Vertrag mit Ihnen nicht abgeschlossen werden,** – **kann nach Art. … ein Bußgeld verhängt werden,** – **können folgende Maßnahmen ergriffen werden … (usw.)** **Oder** **Die Angaben Ihrer personenbezogenen Daten erfolgt freiwillig. Sofern Sie diese Daten nicht bereitstellen, kann dies allerdings zur Folge haben, dass [Angabe der Nachteile].**	*Bei Pflicht: Bitte ggf. verpflichtende Rechtsgrundlage einfügen und zutreffende Folgen bei Nichtangabe ergänzen.* *Soweit freiwillig: Nachteile angeben, die sich aus fehlender Bereitstellung ergeben (etwa, dass der Antrag nicht bearbeitet werden kann).*

11. Nur bei einer Erhebung nicht bei der betroffenen Person: Kategorien der personenbezogenen Daten, die verarbeitet werden und Quelle der Daten

Die Behörde/Kommune verarbeitet folgende personenbezogene Daten von Ihnen: – **...** – **...** – **...** **Ihre Daten haben wir bei … erhoben.**	*Unter Kategorien sind aussagefähige Oberbegriffe zu verstehen, z. B. „Name und Vorname“, „Anschrift“, „Staatsangehörigkeit“. Angaben rein technischer Art (z. B. Feldnummern, Schlüsselnummern usw.) sind nicht erforderlich.* *Anzugeben ist die Quelle, aus der die Datenstammen, ggf. auch, ob sie aus öffentlich zugänglichen Quellen stammen.* *Für eine verständliche und transparente Information sollten die Kategorien der verarbeiteten personenbezogenen Daten sowie die Quelle dieser Daten im Fall einer Erhebung nach Art. 14 DSGVO möglichst frühzeitig angegeben werden, etwa vor Nr. 4 (Zwecke und Rechtsgrundlagen).*

12. Sonderfall: Informationspflicht für den Fall einer späteren Zweckänderung

In diesem Fall ist der Text bei vorstehender Nr. 4a durch folgenden Text zu ersetzen. Im Übrigen sind mindestens die Informationen nach Art. 13 Abs. 2 bzw. Art. 14 Abs. 2 DSGVO im Hinblick auf den geänderten Zweck mitzuteilen (soweit die betroffene Person noch nicht über diese Informationen verfügt, vgl. Art. 13 Abs. 4, Art. 14 Abs. 5 Buchst. a DSGVO):	*Diese Information muss vor der beabsichtigten Weiterverarbeitung erfolgen.* *Der Zweck einer Verarbeitung ergibt sich regelmäßig aus den Angaben im Verarbeitungsverzeichnis und aus dem Erhebungsformular.* *Diese Informationspflicht gilt für Fälle, in denen die öffentliche Stelle die Daten im Nachhinein*

Wir haben Daten von Ihnen erhoben, um … (*ursprüngliche Zwecke nennen*). Wir beabsichtigen nun, diese Daten zu verarbeiten, um … (*neue Zwecke nennen).*	*für einen anderen Zweck weiterverarbeiten will, als bei der Erhebung angegeben wurde. Sie besteht nicht, wenn die Daten für den gleichen Zweck, der bei der Erhebung angegeben wurde an Dritte übermittelt werden.* *Wenn die Daten an einen Dritten bzw. einen anderen Verantwortlichen übermittelt werden ist ggf. auch der Empfänger informationspflichtig.*

7.10 Muster für Datenschutzinformationen[43]

Datenschutzinformationen gemäß Art. 13, 14 DSGVO im Zusammenhang mit [Thema ergänzen] **Stand: [Monat/Jahr]**	
1. Name und Kontaktdaten des Verantwortlichen	**Verantwortlich** für die Verarbeitung Ihrer Daten ist die XY, Straße Hs.Nr., PLZ Ort, Telefon (Vorwahl) Rufnummer-0, E-Mail: poststelle@lbehörde.de, ggf. sicheres Kontaktformular.
2. Kontaktdaten der / des behördlichen Datenschutzbeauftragten	Unsere/n **Datenschutzbeauftragte/n** erreichen Sie wie folgt: DSB, Straße Hs.Nr., PLZ Ort, Telefon (Vorwahl) Rufnummer-0, E-Mail: postfachDSB@lbehörde.de, ggf. sicheres Kontaktformular.
3. Betroffenenrechte	Nach der Datenschutz-Grundverordnung (DSGVO) stehen Ihnen folgende Rechte zu: • Sie können **Auskunft** verlangen, ob und ggf. welche personenbezogenen Daten wir von Ihnen verarbeiten und erhalten weitere mit der Verarbeitung zusammenhängende Informationen (Art. 15 DSGVO). Bitte beachten Sie, dass dieses Auskunftsrecht in bestimmten Fällen eingeschränkt oder ausgeschlossen sein kann. • Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf **Berichtigung** zu (Art. 16 DSGVO). • Liegen die gesetzlichen Voraussetzungen vor, so können Sie die **Löschung** Ihrer personenbezogenen Daten oder die **Einschränkung ihrer Verarbeitung** verlangen (Art. 17 und 18 DSGVO). Das Recht auf Löschung nach Art. 17 Abs. 1 und 2 DSGVO besteht jedoch unter anderem dann nicht, wenn die Verarbeitung personenbezogener Daten erforderlich ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 17 Abs. 3 Buchst. b DSGVO). • Erfolgt die Verarbeitung zur Wahrnehmung einer öffentlichen Aufgabe (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DSGVO), haben Sie das Recht, jederzeit gegen die Verarbeitung Ihrer Daten **Widerspruch** einzulegen, wenn Sie hierfür Gründe haben, die sich aus Ihrer besonderen Situation ergeben (Art. 21 Abs. 1 Satz 1 DSGVO). Sollten Sie von Ihren Rechten Gebrauch machen, prüfen wir, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind. Weitere Einschränkungen, Modifikationen und gegebenenfalls Ausschlüsse der vorgenannten Rechte können sich aus der Datenschutz-Grundverordnung oder nationalen Rechtsvorschriften ergeben.
4. Beschwerderecht bei der Aufsichtsbehörde	Ihnen steht weiterhin ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz zu. Diesen können Sie unter folgenden Kontaktdaten erreichen: Postanschrift: Postfach 22 12 19, 80502 München Hausanschrift: Wagmüllerstr. 18, 80538 München

[43] Das vorliegende komprimierte Muster für Datenschutzinformationen stellt ein Formulierungsbeispiel dar.

	Telefon: +49 89 212672-0 Telefax: +49 89 212672-50 Kontaktformular: https://www.datenschutz-bayern.de/service/complaint.html
5. Zwecke der Datenverarbeitung	*[aus VVT übernehmen]*
6. Rechtsgrundlagen der Datenverarbeitung	*[aus VVT übernehmen]*
7. Kategorien der personenbezogenen Daten, soweit der betroffenen Person noch nicht bekannt[44]	*Zusätzlich zu den von Ihnen angegebenen Daten verarbeiten wir folgende personenbezogene Daten von Ihnen:* – *[Kategorie einfügen]* – *[Kategorie einfügen]*
8. Quellen personenbezogener Daten, die nicht bei der betroffenen Person erhoben werden bzw. wurden[45]	*[Quelle angeben (z. B.: Ihre Daten haben wir bei … erhoben)]*
9. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten	*[Aus VVT übernehmen]*
10. Ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation	*[Aus VVT übernehmen; ggf. fehlende Angaben nach Art. 13 Abs. 1 Buchst. f bzw. Art. 14 Abs. 1 Buchst. f DSGVO ergänzen (bzgl. Angemessenheitsbeschluss bzw. geeigneter oder angemessener Garantien)]*
11. Ggfs. Widerrufsrecht bei Einwilligungen	*Formulierungsvorschlag, falls zutreffend:* *Ihre Einwilligung können Sie jederzeit widerrufen. Hieraus entstehen Ihnen keine Nachteile. Der Widerruf kann gegenüber [der Behörde] formlos erklärt werden. Die Rechtmäßigkeit der aufgrund Ihrer Einwilligung bis zum Widerruf erfolgten Verarbeitung wird dadurch nicht berührt.*
12. Dauer der Speicherung der personenbezogenen Daten	*[Aus VVT übernehmen]*
13. Pflicht / Keine Pflicht zur Bereitstellung der Daten	*Formulierungsvorschlag im Falle einer Bereitstellungspflicht:* *Sie sind gesetzlich verpflichtet, Ihre personenbezogenen Daten uns gegenüber anzugeben. Diese Verpflichtung ergibt sich aus [Angabe der Rechtsgrundlage]. Wenn Sie Ihre Daten nicht angeben, kann dies zur Folge haben, dass [Angabe der möglichen Nachteile].* *Formulierungsvorschlag im Fall freiwilliger Bereitstellung:* *Die Angaben Ihrer personenbezogenen Daten erfolgt freiwillig. Sofern Sie diese Daten nicht bereitstellen, kann dies allerdings zur Folge haben, dass [Angabe der Nachteile].*

[44] Nur in den Fällen des Art. 14 DSGVO: Soweit es für den Bürger aus dem Antragsformular nicht erkennbar ist, dass noch weitere Kategorien von personenbezogenen Daten verarbeitet werden, weil sie nicht bei der betroffenen Person erhoben werden, sind diese hier anzugeben.
[45] Nur in den Fällen des Art. 14 DSGVO.

8. Datenschutzverletzungen und Datenpannen – was tun?

Eine wichtige Neuerung der Datenschutzreform 2018 war die Einführung einer umfassenden Meldepflicht bei Datenschutzverletzungen an die Aufsichtsbehörde (Art 33 DSGVO) sowie einer Benachrichtigungspflicht gegenüber der betroffenen Person, wenn mit einer Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht (Art. 34 DSGVO).

Nachfolgend werden die aus diesen Regelungen hervorgehenden Handlungspflichten des Verantwortlichen in einer kurzen Übersicht erläutert. Ergänzend wird auf die ausführliche Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz zu diesem Thema hingewiesen[46].

Die Nichtbeachtung bestehender Melde- und Benachrichtigungspflichten kann aufsichtliche Maßnahmen nach sich ziehen, unter den Voraussetzungen der Art. 22 und 23 BayDSG kommt auch die Verhängung einer Geldbuße in Betracht.

Neben der Meldepflicht an den Bayerischen Landesbeauftragten für den Datenschutz können auch weitere fachgesetzliche Meldepflichten bestehen, z. B. nach § 83a SGB X an die Rechts- oder Fachaufsicht von Sozialbehörden oder nach Art. 11 Abs. 2 BayEGovG (künftig Art. 43 Abs. 2 BayDiG-E) an das Landesamt für Sicherheit in der Informationstechnik.

8.1 Was sind Datenschutzverletzungen oder Datenpannen?

Nach Art. 4 Nr. 12 DSGVO ist eine „Verletzung des Schutzes personenbezogener Daten“ (kurz: Datenschutzverletzung) eine „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

---

[46] https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf. Auf Besonderheiten bei Sozialbehörden bzw. im Bereich der Justiz (für Kommunen im Ordnungswidrigkeitenrecht relevant!) sind spezielle AKIs veröffentlicht: https://www.datenschutz-bayern.de/datenschutzreform2018/aki09.pdf und https://www.datenschutz-bayern.de/datenschutzreform2018/aki18.pdf. Daneben hat auch der Europäische Datenschutzausschuss ein Working Paper zu dieser Thematik veröffentlicht, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/wp250rev01_de.pdf.

Anders gesagt: Eine Datenschutzverletzung ist ein Verstoß gegen die Datensicherheit, bei dem Unberechtigten personenbezogene Daten vermutlich oder erwiesenermaßen bekannt werden und/ oder dem Verantwortlichen nicht mehr oder nur noch in veränderter Form zur Verfügung stehen. Die Ursachen dafür sind vielfältig, ein Verschulden ist nicht erforderlich. Dabei kann es sich beispielsweise um folgende Sachverhalte handeln:

- Hackerangriff
- Zugriff von Dritten auf persönliche Daten oder PIN-Codes
- Diebstahl, Verlust oder Sabotage von IT-Hardware (Notebook, Diensthandy o.ä.) oder auch von Papierakten
- unbefugtes Weitergeben von Daten durch Mitarbeiterinnen und Mitarbeiter durch eine Verletzung der Datensicherheit [auch behördenintern], Vortäuschen einer anderen Person am Telefon oder per E-Mail)
- Einbruch in Dienstgebäude bzw. Büro

8.2 Meldepflicht bei der Aufsichtsbehörde, Dokumentationspflicht

Gemäß Art. 33 Abs. 1 DSGVO sind Datenschutzverletzungen **„unverzüglich und möglichst binnen 72 Stunden“** nach Bekanntwerden der zuständigen Aufsichtsbehörde, für den öffentlichen Bereich in Bayern dem Bayerischen Landesbeauftragten für den Datenschutz, zu melden. Diese Meldung sollte dabei mittels des hierfür bereitgestellten Onlineformulars erfolgen.[47]

Im Anwendungsbereich des § 32h AO hat die Meldung in Steuersachen nicht an den Bayerischen Landesbeauftragten für den Datenschutz, sondern den Bundesbeauftragten für den Datenschutz als zuständiger Aufsichtsbehörde zu erfolgen. Die Meldung darf in Straf- oder Ordnungswidrigkeitenverfahren gegen den Verantwortlichen nur mit seiner Zustimmung verwendet werden, Art. 23 Abs. 4 BayDSG.

Eine Meldung ist gemäß Art. 33 DSGVO nur dann nicht erforderlich, wenn die Datenschutzverletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“.

---

[47] https://www.datenschutz-bayern.de/service/data_breach.html.

Um einen schnellen Umgang mit möglichen Datenschutzverletzungen gewährleisten zu können, müssen diesbezüglich behördenintern organisatorische Regelungen getroffen werden.

Hierzu ist, in der Regel mittels Dienstanweisung und im Geschäftsverteilungsplan, eine für die praktische Durchführung der Meldung verantwortliche Stelle festzulegen. Das Muster der Datenschutzgeschäftsordnung enthält in § 12 hierzu einen Formulierungsvorschlag. Diese Aufgabe kann, muss aber nicht zwingend dem / der Behördlichen Datenschutzbeauftragten übertragen werden.

Im Zusammenhang mit den Pflichten nach Art. 33 und 34 DSGVO sind folgende Arbeitsschritte zu beachten:

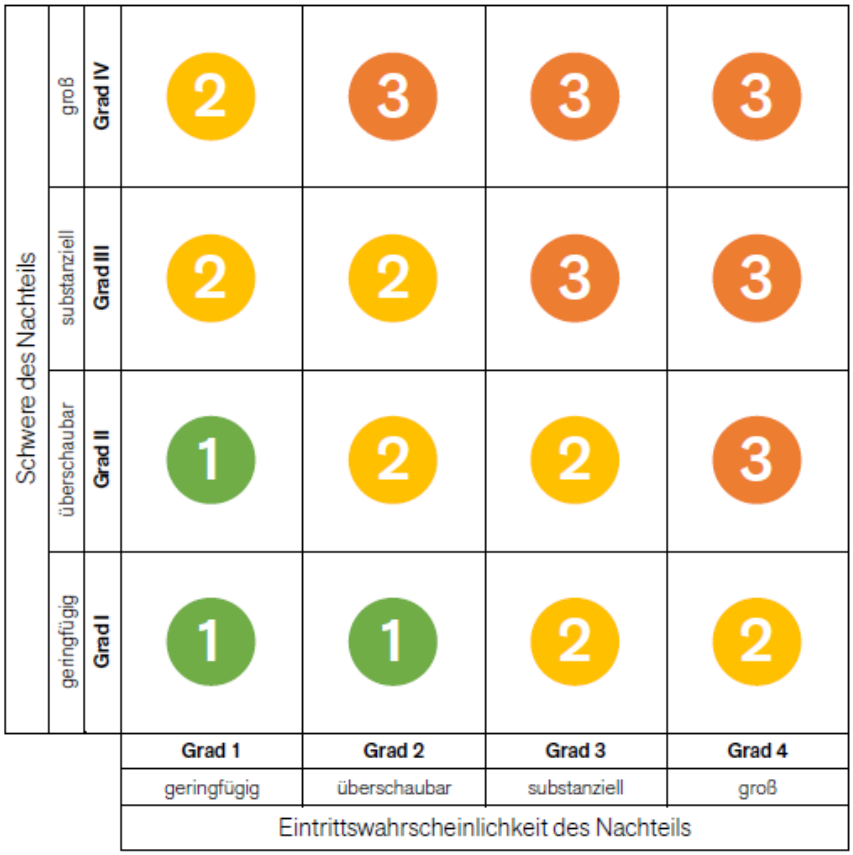
- Beurteilung des Risikos der Datenschutzverletzung

Jede festgestellte Datenschutzverletzung ist zunächst behördenintern daraufhin zu überprüfen, welches voraussichtliche Risiko für die Rechte und Freiheiten natürlicher Personen mit ihr einhergeht. Erst aus dieser **Risikobeurteilung** ergibt sich nämlich, ob

- eine **Meldepflicht** an die Aufsichtsbehörde gem. Art. 33 DSGVO (bei **„voraussichtlichem Risiko“**),
- zusätzlich eine **Benachrichtigungspflicht** an die betroffene Person gem. Art. 34 DSGVO (bei **„voraussichtlich hohem Risiko“**)
- oder (ausnahmsweise) **keine Meldepflicht** aufgrund **voraussichtlich geringfügigem Risiko**

gegeben ist.

Die Durchführung dieser Risikobeurteilung ist in der Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz ausführlich dargestellt, im Kern ist dabei folgende Bewertungsmatrix heranzuziehen. Ein voraussichtliches Risiko liegt hiernach dann vor, wenn die Gesamtbewertung der Einzelkriterien „Schwere des Nachteils für den Betroffenen“ sowie „Eintrittswahrscheinlichkeit des Nachteils“ einen Wert von 2 (= Risiko) oder 3 (= hohes Risiko) ergibt:



Bei Durchführung der Risikobeurteilung von Datenschutzverletzungen im IT- Bereich sollte grundsätzlich, soweit vorhanden, zusätzlich der oder die Informationssicherheitsbeauftragte mit einbezogen werden. Daneben kann die Hinzuziehung weiterer Beschäftigter, z. B. aus der IT, geboten sein.

- Entscheidung über Vorliegen einer Meldepflicht

Die Verantwortung für die Meldung, und damit auch die endgültige Entscheidung, ob ein meldepflichtiger Vorfall vorliegt, liegt beim Verantwortlichen; intern kann er die Entscheidungsbefugnis delegieren. Eine sachgerechte Delegation, z. B. des Bürgermeisters / der Bürgermeisterin an den Amtsleiter / die Amtsleiterin, ist hierbei möglich. Diese Entscheidung kann allerdings – anders als die Durchführung der Risikobeurteilung sowie die tatsächliche Abgabe der Meldung - nicht dem / der behördlichen Datenschutzbeauftragten übertragen werden, der/die insoweit ausschließlich eine Beratungs- und Überwachungsfunktion innehat.

- Dokumentation der Datenschutzverletzung

Festgestellte Datenschutzverletzungen sind grundsätzlich zu dokumentieren (Art. 33 Abs. 5 DSGVO), selbst wenn die Risikobeurteilung aufgrund voraussichtlich geringfügigen Risikos nicht zu einer Meldepflicht führen sollte. Zudem sollten ggf. ergriffene Abhilfemaßnahmen aufgeführt werden.

Die abgegebene Meldung über das Online-Formular ist als Dokumentation alleine nicht ausreichend, daneben ist zumindest die Risikobeurteilung in nachvollziehbarer Form festzuhalten.

Auch die Zuständigkeit für diese Aufgabe sollte in der Datenschutz-Geschäftsordnung und/oder der Dienstanweisung festgehalten sein.

8.3 Benachrichtigungspflicht an die betroffenen Personen bei hohem Risiko

Ergibt die Risikobeurteilung im Hinblick auf die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Person(en), hat der Verantwortliche die betroffenen Personen **unverzüglich** von der Datenschutzverletzung zu benachrichtigen (Art. 34 Abs. 1 DSGVO).

Auch hinsichtlich der Zuständigkeit für diese Aufgabe muss eine organisatorische Festlegung getroffen sein. Hierfür kann ebenfalls eine zentrale Stelle festgelegt werden ; im Regelfall sollte aufgrund der dienstlichen Nähe zu den betroffenen Personen jedoch hierfür diejenige Dienststelle verantwortlich sein, bei der die Datenschutzverletzung erfolgte.

8.4 Interne Meldewege, Sensibilisierung der Mitarbeiterinnen und Mitarbeiter

Damit die für die Risikobeurteilung, Dokumentation, und Meldung einer Datenschutzverletzung zuständige Stelle diese Aufgaben auch wahrnehmen kann, muss auch der Prozess, wie sie von einer solchen Verletzung Kenntnis erlangt, geregelt sein. Das Muster der Datenschutzgeschäftsordnung enthält in § 12 hierzu einen Vorschlag, wie ein solcher Prozess etabliert werden kann.

Auf jeden Fall ist dabei der / die Behördliche Datenschutzbeauftragte bzw. die für die Risikobeurteilung, Dokumentation und Meldung einer Datenschutzverletzung zuständige Stelle

möglichst unmittelbar und direkt sowie der/die unmittelbare Dienstvorgesetzte zu informieren. Aufgrund der knappen (72-Stunden-) Zeitvorgabe für die Meldung an die Aufsichtsbehörde sollten dabei parallele Meldewege möglich sein, um zu verhindern, dass sich die Meldung aufgrund von Abwesenheiten verzögert. Sollte im Einzelfall die 72-Stunden-Frist dennoch nicht eingehalten werden können, muss der Meldung eine Begründung für die Verzögerung beigefügt werden (Art. 33 Abs. 1 Satz 2 DSGVO).

Damit bereits die internen Meldungen strukturiert erfolgen und als Teil der Dokumentation verwendet werden können, kommt die Einführung eines internen Meldeformulars mit Laufweg, Hinweisen etc. in Betracht.

Nachdem eine Datenschutzverletzung grundsätzlich an jedem Arbeitsplatz vorkommen kann, müssen auch grundsätzlich alle Beschäftigten darüber informiert sein bzw. werden

- wann eine Datenschutzverletzung vorliegt,
- was bei Auftreten eines solchen Vorfalls zu tun ist und
- wer wie hierüber zu informieren ist.

Es ist daher zentral, in der gesamten öffentlichen Stelle ein Bewusstsein für datenschutzrechtliche Notwendigkeiten (nicht nur) im Hinblick auf das Auftreten einer Datenschutzverletzung zu schaffen und aufrecht zu erhalten.

Hierzu sind vom Verantwortlichen die entsprechenden Sensibilisierungsmaßnahmen durchzuführen, wie etwa

- Schulungen,
- Bekanntgabe entsprechender Vorschriften gegen Unterschrift,
- Information in Hauszeitschriften und/oder Intranet,
- Rundschreiben / Flyer / Serien-E-Mails.

Daneben sind die Beschäftigten in geeigneter Weise auf mögliche arbeits- und disziplinarrechtliche sowie ggf. strafrechtliche Folgen insb. bei bewussten Verstößen hinzuweisen. Denn anders als vielfach angenommen, können einzelne Beschäftigte über Art. 23 BayDSG bei datenschutzrechtlichen Verstößen belangt werden; das „Privileg“ des Art. 22 BayDSG bezieht sich nur auf die Behörde selbst, nicht aber auf einzelne Beschäftigte. Zudem können datenschutzrechtliche Verstöße von Beschäftigten zu Schadensersatzansprüchen gemäß Art. 82 DSGVO gegen den Dienstherren als Verantwortlichen führen, welche auf dem Zivilrechtsweg verfolgt werden können.

8.5 Konsequenzen aus Auftreten einer Datenschutzverletzung ziehen

Ist eine Datenschutzverletzung festgestellt worden, ist zu prüfen, wie deren Folgen möglichst geringgehalten werden können. Daneben sind Vorkehrungen zu treffen, die künftig einen vergleichbaren Vorfall ausschließen. Hierbei kommen beispielsweise folgende Maßnahmen in Betracht:

- Änderungen im Prozessablauf,
- Technische Änderungen im Fachverfahren/IT-System,
- Dienstanweisung,
- Sensibilisierung der Beschäftigten (ggf. durch Anleitung / FAQs zu bestimmten Themen),
- Aufnahme bestimmter datenschutzrechtlicher Aspekte in Schulungen bzw. in ein Handbuch für Fachverfahren.

9. Foto- und Filmaufnahmen

9.1 Einleitung

Foto- und Filmaufnahmen sind ein wichtiger Bestandteil in der Öffentlichkeitsarbeit bayerischer öffentlicher Stellen. Allerdings stellt jede Anfertigung sowie die nachfolgende Veröffentlichung von Aufnahmen, auf denen Personen identifizierbar sind, eine Verarbeitung personenbezogener Daten dar, so dass es einer Rechtsgrundlage dafür bedarf und die Verarbeitung mit den typischen datenschutzrechtlichen Verpflichtungen (Verarbeitungsverzeichnis, Informationspflichten etc.) einhergeht.[48]

Hinsichtlich Foto- und Filmaufnahmen im Zusammenhang mit kommunalen Auszeichnungen und Ehrungen besteht mit Art. 27 BayDSG eine spezielle Rechtsgrundlage.

Aktuell ist **nicht abschließend geklärt,** ob **Art. 4 Abs. 1 BayDSG** hinsichtlich der Aufnahme von Personenfotografien und -filmaufnahmen und **Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG** hinsichtlich der entsprechenden Veröffentlichung als **Rechtsgrundlage** herangezogen werden darf. Der Bayerische Landesbeauftragte für den Datenschutz weist in seiner „Aktuellen Kurz-Information 16: Fotografien in der Öffentlichkeitsarbeit bayerischer Kommunen“ auf die ungeklärte Rechtslage hin, empfiehlt bayerischen Kommunen, die Entwicklung zu beobachten, wendet sich aber ausdrücklich nicht gegen die Aufnahme und Veröffentlichung von Personenfotografien sowie von Filmaufnahmen auf Grundlage von Art. 4 Abs. 1, 5 Abs. 1 Satz 1 Nr. 1 BayDSG unter Berücksichtigung gewisser Maßgaben:

So hat der Verantwortliche vor jeder Aufnahme bzw. Veröffentlichung kritisch zu prüfen, ob sie in Bezug auf die kommunale Aufgabe der Öffentlichkeitsarbeit als **erforderlich** angesehen werden kann. Die Begleitung von Veranstaltungen mittels Öffentlichkeitsarbeit wird sich in der Regel auf Anlässe von einigem Rang – Repräsentationsveranstaltungen – beschränken. Der Bayerische Landesbeauftragte für den Datenschutz empfiehlt in diesem Zusammenhang, derartige Veranstaltungen der Kategorie nach durch einen Gemeinderatsbeschluss festzulegen. Regelmäßig nicht erforderlich wird es sein, eine Veranstaltung mittels Fotografien systematisch zu dokumentieren, sondern es genügt, hervorgehobene Funktions-

[48] Eine umfangreiche Kurzinformation des Bayerischen Landesbeauftragten für Datenschutz findet sich unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki16.html. Hinsichtlich kommunaler Schulen und Kindertageseinrichtungen ist ein Beitrag "Erstellung und Verwendung von Schülerfotos" https://www.datenschutz-bayern.de in der Rubrik "Themengebiete - Schulen" abrufbar.

und Würdenträger bzw. Ehrengäste zu fotografieren und dazu einige Übersichtsaufnahmen zu erstellen. Im Rahmen der Pressearbeit ist darauf zu verzichten, umfangreiche Bildarchive bereit zu stellen, vielmehr sollten allenfalls einige wenige, sorgsam ausgewählte Fotografien herausgegeben werden. Zudem fehlt es im Falle eines überraschenden oder heimlichen Ablichtens von Teilnehmern und Teilnehmerinnen der Veranstaltung an der Erforderlichkeit. Um dies zu vermeiden, sollte **auf der Einladung der Veranstaltung auf die Fertigung von Foto- und Filmaufnahmen hingewiesen** werden und während der Veranstaltung **Hinweisschilder** aufgestellt werden.[49] Abhängig von der Bedeutung des zu dokumentierten Ereignisses kann es zur Erfüllung der Öffentlichkeitsarbeit darüber hinaus nicht erforderlich sein, weltweite Öffentlichkeit (wie es bei der Veröffentlichung im Internet anzunehmen ist) herzustellen, so dass die Verwendung **örtlich begrenzter Medien**, wie die örtliche Tageszeitung oder das Gemeindeblatt oft ausreichen wird.

Besteht nach den dargestellten Grundsätzen eine Erforderlichkeit gemäß Art. 4 Abs. 1, 5 Abs. 1 Satz 1 Nr. 1 BayDSG für die Verarbeitung personenbezogener Daten, hat der Verantwortliche abschließend sein **Ermessen** auszuüben, ob er personenbezogene Daten verarbeiten will. Dafür hat er einzelfallbezogen das Publikationsinteresse mit dem Interesse der betroffenen Personen am Schutz ihrer personenbezogenen Daten abzuwägen. Bei dieser Abwägung ist insbesondere auch zu berücksichtigen, ob die jeweilige Foto- oder Filmaufnahme über das Offensichtliche (z. B. Hautfarbe, Nutzung einer Sehhilfe) hinaus Rückschlüsse auf Daten im Sinne von Art 9 Abs. 1 DSGVO (z. B. Gesundheitsdaten) zulässt.

Kann der Einsatz von Foto- und Filmaufnahmen nach den dargestellten Maßstäben nicht auf die Art. 4 Abs. 1, 5 Abs. 1 BayDSG gestützt werden, kann **ggf. auf eine Einwilligung zurückgegriffen** werden.

[49] Vgl. Musterhinweis für Veranstaltungen unter 9.3.

9.2 Mustereinwilligungserklärung

Einwilligungserklärung in die Erstellung und Veröffentlichung von Filmaufnahmen, Tonaufnahmen und Fotografien durch die ……

Hiermit erteilen wir / erteile ich gegenüber ……., die Einwilligung, von der nachstehend genannten Person (Zutreffendes bitte ankreuzen)

☐ Fotos ☐ Video- und Tonaufnahmen

in Zusammenhang mit ……..*(der Veranstaltung etc.)* zu erstellen.

In eine mögliche Veröffentlichung (Zutreffendes bitte ankreuzen)

☐ In der Presse *(bitte näher spezifizieren: örtliche Tagespresse, überregionale Zeitung etc.)*

☐ In Drucksachen
  ☐ der ….

☐ im Internetauftritt
  ☐ der …(www.….)

willige ich ein.

……..……..……..……..
Name und Vorname der abgebildeten Person

……..……..……..……..….
Geburtsdatum der abgebildeten Person (bei Minderjährigen)

……..……..……..……..….
Anschrift der abgebildeten Person

Für die Anfertigung und Veröffentlichung von Fotos von einzelnen, individuell erkennbaren Personen oder von Video- oder Tonaufnahmen ist im vorliegenden Fall eine Einwilligung erforderlich. Die Verarbeitung basiert auf Art. 6 Abs. 1 Buchst. a DSGVO. Sie erfolgt zum Zweck der Presse- und Öffentlichkeitsarbeit.

Die Rechteeinräumung an den Fotos und/oder Videos und Tonaufnahmen erfolgt ohne Vergütung und umfasst auch das Recht zur Archivierung und Bearbeitung, soweit die Bearbeitung nicht entstellend ist. Namen oder sonstige personenbezogene Daten werden von uns nicht veröffentlicht, auch nicht als Quelltext zu Bildern und/oder Videos.

Durch eine Verwendung im Internet können die Fotos und/oder Videos weltweit abgerufen und gespeichert werden. Entsprechende Daten können damit auch über so genannte „Suchmaschinen“ aufgefunden werden. Dabei kann nicht ausgeschlossen werden, dass andere Personen oder Unternehmen diese Bilder und/oder Videos verändern, zu anderen Zwecken nutzen oder mit weiteren im Internet verfügbaren Daten verknüpfen und ein Persönlichkeitsprofil erstellen. Über die Archivfunktion von Suchmaschinen sind die Daten zudem häufig auch dann noch abrufbar, wenn diese aus den oben genannten Internetseiten bereits entfernt oder geändert wurden.

Sie können die Einwilligung jederzeit schriftlich bei ……. mit Wirkung für die Zukunft widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Dies ist insbesondere relevant in Fällen, in denen der Druckauftrag bereits erteilt ist.

Soweit die Einwilligung nicht widerrufen wird, gilt sie zeitlich unbeschränkt.

Die Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile.

……..……..……..……..…

(Ort, Datum) (Unterschrift der abgebildeten Person)

Sofern die abgebildete Person das 18. Lebensjahr noch nicht vollendet hat, ist die Unterschrift der gesetzlichen Vertreter erforderlich, zusätzlich muss ab dem 14. Lebensjahr die abgebildete Person unterschreiben:

……..……..……..……..…

(Ort, Datum) (Unterschrift der/des Erziehungsberechtigten)

Weitere Informationen zum Datenschutz finden Sie unter:

(Link mit Datenschutzhinweisen des Verantwortlichen einfügen)

9.3 Musterhinweis für Veranstaltungen

Hinweis:

Hier wird fotografiert!

Wir möchten Sie darauf hinweisen, dass der Veranstalter – ohne zur Zahlung einer Vergütung verpflichtet zu sein – berechtigt ist, im Rahmen dieser Veranstaltung Fotoaufnahmen zu erstellen und zum Zwecke der Öffentlichkeitsarbeit und der Berichterstattung über die Veranstaltung zu veröffentlichen. Diese Rechte gelten räumlich und zeitlich unbegrenzt.

Die Fotos werden auf den Internetseiten der ….. und in der lokalen Presse verwendet.

Gemäß Art. 21 DSGVO haben Sie gegebenenfalls das Recht darauf, nicht fotografiert zu werden – bitte sprechen Sie unverzüglich mit dem/der Veranstalter/in oder Fotografen/in, wenn Sie dieses Recht geltend machen wollen.

Veranstalter und damit Verantwortlicher für die Erstellung von Fotoaufnahmen ist … Rechtsgrundlage ist Art. 4 Abs. 1 BayDSG i.V.m. der Aufgabe, die Öffentlichkeit und die Presse über die Veranstaltung zu informieren.

Weitere Informationen zum Datenschutz finden Sie unter:

xxx

10. Auftragsverarbeitung[50]

Die nachfolgenden Ausführungen beziehen sich auf Verarbeitungen im Anwendungsbereich der DSGVO. Für eine Auftragsverarbeitung, die der Richtlinie zum Datenschutz bei Polizei und Justiz unterfällt, ist die eingeschränkte Bezugnahme in Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG bzw. im Ordnungswidrigkeitenverfahren des § 62 BDSG zu beachten.

10.1 Wesentliche Rechtsgrundlagen

Die Beteiligten einer Auftragsverarbeitung werden als „Verantwortlicher“ und „Auftragsverarbeiter“ bezeichnet (Art. 4 Nr. 7, 8 DSGVO). Wesentliche Regelungen der Auftragsverarbeitung ergeben sich unmittelbar aus Art. 28 und 29 DSGVO. Der Mindestinhalt für den Vertrag über die Auftragsverarbeitung (AV-Vertrag) – oder gegebenenfalls des „anderen Rechtsinstruments“ – ist in Art. 28 Abs. 3 Unterabs. 1 DSGVO geregelt.
Die Zulässigkeit einer Auftragsverarbeitung kann im öffentlichen Bereich durch nationales Recht eingeschränkt sein. Beispiele für entsprechende fachspezifische Regelungen sind Art. 27 Abs. 4 Sätze 5 und 6 Bayerisches Krankenhausgesetz (BayKrG) sowie § 80 Zehntes Buch Sozialgesetzbuch (SGB X).

Der Verantwortliche ist als „Herr der Daten“ für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Der Auftragsverarbeiter wird ähnlich einer beim Verantwortlichen selbst beschäftigten Person privilegiert; bei der Weitergabe von Daten im Rahmen der Auftragsverarbeitung werden Verantwortlicher und Auftragsverarbeiter als Einheit behandelt. Insbesondere ist der Auftragsverarbeiter im Verhältnis zum Verantwortlichen nicht „Dritter“ im Sinne des Art. 4 Nr. 10 DSGVO (gleichwohl ist er jedoch „Empfänger“ im Sinne des Art. 4 Nr. 9 DSGVO). Für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtgrundlage als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt. Insbesondere § 203 StGB bleibt jedoch unberührt. Auftragsverarbeiter fallen selbst gemäß § 203 Abs. 3 StGB unter diese Strafbarkeit, darauf hat sie der Verantwortliche gemäß § 203 Abs. 4 StGB hinzuweisen und zur Verschwiegenheit zu verpflichten.

[50] Eine ausführliche und detaillierte Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz findet sich unter https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf.

Die Auftragsverarbeitung im Zusammenhang mit der dauerhaften rechtsverbindlichen Speicherung elektronischer Akten im **Ordnungswidrigkeitenverfahren** regelt § 497 StPO i.V.m. § 49d Abs. 1 OWiG. In den Anwendungsbereich des § 497 StPO fällt eine dauerhafte, rechtsverbindliche Speicherung elektronischer Akten i.S.d. § 110a OWiG, die in zentralen Rechenzentren erfolgen wird. Eine dauerhafte rechtsverbindliche Speicherung elektronischer Akten im Ordnungswidrigkeitenverfahren i.S.d. § 497 StPO ist nur dann zulässig, wenn die öffentliche Stelle den Zutritt und den Zugang zu den Datenverarbeitungsanlagen, in denen die elektronischen Akten rechtsverbindlich gespeichert werden, tatsächlich und ausschließlich kontrolliert. Ist dies nicht der Fall, ist ein Outsourcing nicht möglich.

10.2 Inhaltliche Vorgaben für die Auftragsverarbeitung

10.2.1 Auswahl des Auftragsverarbeiters

Der Auftragsverarbeiter muss „hinreichende Garantien" – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen (vgl. DSGVO-Erwägungsgrund 81) – für die Umsetzung der geeigneten technischen und organisatorischen Schutzmaßnahmen bieten (Art. 28 Abs. 1 DSGVO). Um hinreichende Garantien nachzuweisen, können gem. Art. 28 Abs. 5 DSGVO beispielsweise die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder genehmigte Zertifizierungsverfahren (Art. 42 DSGVO) als Faktoren herangezogen werden. Diese Möglichkeit besteht allerdings nicht im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz, da Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG die Regelung in Art. 28 Abs. 5 DSGVO für nicht anwendbar erklärt. Eine ausdrückliche Pflicht des Verantwortlichen, sich fortlaufend von der Einhaltung dieser Maßnahmen zu überzeugen, ist zwar nicht ausdrücklich geregelt, ergibt sich aber aus der Rechenschafts- und Nachweispflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 Satz 1 DSGSVO sowie dem Schutzziel des Art. 28 DSGVO.

10.2.2 Form des Vertrags zur Auftragsverarbeitung

Der Vertrag zur Auftragsverarbeitung ist schriftlich abzufassen; dies kann auch in einem elektronischen Format erfolgen (Art. 28 Abs. 9 DSGVO). Dieser Anforderung genügt die Textform im Sinne des § 126b BGB.

10.2.3 Wesentliche Vertragsinhalte

Bei einer Auftragsverarbeitung ist grundsätzlich (d. h., wenn diese nicht ausnahmsweise auf Grundlage eines „anderen Rechtsinstruments" im Sinne des Art. 28 Abs. 3 Unterabs. 1 S. 1 DSGVO erfolgt) der Abschluss eines AV-Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter erforderlich. Dies erfolgt meist als Ergänzung eines IT-Dienstleistungsvertrags. Der AV-Vertrag enthält gesetzlich festgelegte Vertragsinhalte, u.a. **Regelungen**

zum Gegenstand und zur Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen (vgl. Art. 28 Abs. 3 Unterabs. 1 DSGVO).

a) Weisungen

Personenbezogene Daten dürfen nur auf dokumentierte Weisung des Verantwortlichen verarbeitet werden (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. a, Art. 29 DSGVO).

b) Datengeheimnis

Die zur Datenverarbeitung befugten Personen müssen zur Einhaltung des Datengeheimnisses verpflichtet sein oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Eine ausdrückliche Regelung zum Datengeheimnis ist zwar in der DSGVO nicht vorgesehen; allerdings muss der Auftragsverarbeiter gewährleisten, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder gesetzlich zur Verschwiegenheit verpflichtet sind (Art. 28 Abs. 3 Unterabs. Satz 2 Buchst. b DSGVO). Für Beschäftigte öffentlicher Stellen gilt das Datengeheimnis nach Art. 11 BayDSG. Daher ist keine gesonderte Verpflichtung der Beschäftigten auf das Datengeheimnis erforderlich. Zusätzlich muss gewährleistet sein, dass alle beschäftigten Personen des Auftragsverarbeiters, welche die Daten erhalten, gemäß § 203 Abs. 3, 4 StGB über die Strafbarkeit nach § 203 StGB belehrt werden.

c) Gewährleistung der Sicherheit der Verarbeitung

Der Auftragsverarbeiter hat alle nach Art. 32 DSGVO erforderlichen Maßnahmen zur Sicherheit der Verarbeitung zu ergreifen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. c DSGVO). Je höher das Risiko der Verarbeitung zu bewerten ist, desto strengere Schutzmaßnahmen werden zu ergreifen sein. Die vom Auftragsverarbeiter vorgeschlagenen Maßnahmen sind vom Verantwortlichen inhaltlich zu prüfen und ggf. zu ergänzen.

d) Unterauftragsverarbeiter

Ferner sind in den AV-Vertrag auch Regelungen zum Einsatz weiterer Auftragsverarbeiter (Unterauftragsverarbeiter) aufzunehmen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. d DSGVO). Der Auftragsverarbeiter darf keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen. Im Fall einer allgemeinen schriftlichen Genehmigung ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren (Art. 28 Abs. 2

DSGVO). Hierdurch erhält der Verantwortliche die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.
Soll ein Unterauftragsverarbeiter eingesetzt werden, hat der Auftragsverarbeiter diesem dieselben Datenschutzpflichten aufzuerlegen, die auch für ihn aufgrund des AV-Vertrags mit dem Verantwortlichen gelten. Der Auftragsverarbeiter haftet für Verstöße des Unterauftragsverarbeiters gegenüber dem Verantwortlichen gemäß Art. 28 Abs. 4 S. 2 DSGVO.

e) Unterstützungspflichten bei Beantwortung von Anträgen
Der Auftragsverarbeiter hat den Verantwortlichen soweit möglich mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen von betroffenen Personen (z. B. Anträge auf Auskunft, Berichtigung oder Löschung von personenbezogenen Daten) zu unterstützen (Art. 28 Abs. 3 Unterabs. 1 S. 2 Buchst. e, Kapitel III DSGVO).

f) Unterstützungspflichten bei den Pflichten aus Art. 32–36 DSGVO
Der Verantwortliche muss mit dem Auftragsverarbeiter eine Unterstützungspflicht u.a. bzgl. der Sicherheit der Verarbeitung (Art. 32 DSGVO), der Meldung von Datenschutzverletzungen (Art. 33 DSGVO) und der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) vereinbaren (Art. 28 Abs. 3 Unterabs. 1 S. 2 Buchst. f DSGVO). Die Reichweite dieser Pflicht richtet sich nach der Art der Verarbeitung und dem Umfang der Informationen, die dem Auftragsverarbeiter zur Verfügung stehen.

g) Löschung nach Vertragsbeendigung
Nach Abschluss des Vertrags zur Erbringung einer Auftragsverarbeitung sind alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückzugeben oder, ggf. nach Ablauf von Aufbewahrungsfristen, einschließlich etwaig vorhandener Kopien zu löschen (Art. 28 Abs. 3 Unterabs. 1 S. 2 Buchst. g DSGVO).

h) Pflicht zur Bereitstellung von Informationen und Ermöglichung von Überprüfungen
Komplexe Datenverarbeitungsvorgänge sind für den Verantwortlichen häufig schwer nachvollziehbar. Der Auftragsverarbeiter hat den Verantwortlichen mit Nachweisen zur Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten und der Ermöglichung von Überprüfungen und Vor-Ort-Kontrollen zu unterstützen (Art. 28 Abs. 3 Unterabs. 1 S. 2 Buchst. h DSGVO).

10.3 Gesetzliche Pflichten des Auftragsverarbeiters

Auch der Auftragsverarbeiter muss ein eigenes Verarbeitungsverzeichnis nach Art. 30 Abs. 2 DSGVO führen und dieses auf Verlangen der Aufsichtsbehörde zur Verfügung stellen

(Art. 30 Abs. 4 DSGVO; Art. 28 Abs. 2 Satz 2, Art. 31 BayDSG). Ebenso wie der Verantwortliche ist der Auftragsverarbeiter ferner verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten (Art. 31 DSGVO) sowie ggf. einen / eine Datenschutzbeauftragte(n) zu bestellen (vgl. Art. 37 DSGVO). Erlangt der Auftragsverarbeiter Kenntnis von einer Datenschutzverletzung, hat er diese unverzüglich dem Verantwortlichen zu melden (Art. 33 Abs. 2 DSGVO).
Bei Verarbeitungen im Anwendungsbereich der DSGVO sind die Aufsichtsbehörden gem. Art. 58 DSGVO befugt, gegen den Auftragsverarbeiter direkt vorzugehen, auf Verstöße hinzuweisen, ihn anzuweisen oder Sanktionen zu verhängen (Art. 83 ff. DSGVO).
Auftragsverarbeiter und Verantwortliche haften gegenüber betroffenen Personen gesamtschuldnerisch auf Schadenersatz bei Datenschutzverstößen (Art. 82 Abs. 4 DSGVO). Der Verantwortliche oder der Auftragsverarbeiter können von betroffenen Personen auf Schadenersatz in Anspruch genommen werden (Art. 82 Abs. 1 DSGVO).

10.4 Welche Fragen sind zu klären?

Der Verantwortliche sollte entsprechend den Anforderungen des Art. 28 DSGVO mindestens folgende Fragen klären:

- Wurde der Auftragsverarbeiter hinreichend sorgfältig ausgewählt und liegen entsprechende Garantien vor?
- Werden dem Verantwortlichen wirksame Kontrollrechte eingeräumt (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. h DSGVO)?
- Werden dem Verantwortlichen wirksame Weisungsrechte eingeräumt?
- Wo findet die Auftragsverarbeitung konkret statt? Werden bei Übermittlungen von Daten an Drittländer ggf. zusätzlich Art. 44 ff. DSGVO beachtet?
- Ist die Beauftragung von Unterauftragsverarbeitern vertraglich geregelt (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst d, Art. 28 Abs. 2 und 4 DSGVO)?
- Hat der Auftragsverarbeiter einen / eine Datenschutzbeauftragte(n) und einen Ansprechpartner bei auftretenden Problemen?
- Bestehen ausreichende Mitwirkungspflichten des Auftragsverarbeiters bei der Erfüllung der Rechte der betroffenen Person (z. B. auf Auskunft, Löschung, Widerspruch, Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. e DSGVO), bei Verletzungen des Schutzes personenbezogener Daten und ggf. einer erforderlichen Datenschutz-Folgenabschätzung (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. f DSGVO)?
- Sind Haftungsbeschränkungen zum Nachteil des Verantwortlichen im Vertrag enthalten?

10.5 Muster einer Vereinbarung zur Auftragsverarbeitung

Das nachfolgende Muster einer Vereinbarung zur Auftragsverarbeitung ist möglichst universell gehalten. Je nach konkreter Fallgestaltung ist es daher anzupassen oder zu ergänzen. Das Muster zeigt, wie die Vorgaben von Art. 28 Abs. 3 DSGVO vertraglich umgesetzt werden können; es erhebt – insbesondere hinsichtlich zivilrechtlicher Aspekte – keinen Anspruch auf Vollständigkeit.

Mit dem Durchführungsbeschluss (EU) 2021/915 der Europäischen Kommission vom 4. Juni 2021 liegen erstmals sog. Standardvertragsklauseln i.S.d. Art. 28 Abs. 7 DSGVO vor, die von den Vertragsparteien als Muster herangezogen werden können. Deren Beachtung oder Übernahme ist jedoch nicht zwingend – die Vertragsparteien haben die freie Wahl, ob sie die Standardvertragsklauseln ganz oder auch nur zum Teil übernehmen, Art. 28 Abs. 6 DSGVO. Die Standardvertragsklauseln der Europäischen Kommission sind in manchen Punkten umfassender als das nachfolgende Muster, das aus Praktikabilitätsgründen schlanker gehalten ist – so finden sich dort etwa Klauseln spezifisch zum Umgang mit sensiblen Daten oder ausführliche Regelungen für die Fälle einer Verletzung des Schutzes personenbezogener Daten. Falls eine detailliertere Regelung solcher Fragestellungen angezeigt sein sollte, kann sich dafür an den o. g. Standardvertragsklauseln orientiert werden.

Die Standardvertragsklauseln sind abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2021:199:FULL Seite L199/21 ff.

Für den öffentlichen Bereich ist zudem zu beachten, dass die Zulässigkeit der Auftragsverarbeitung gesetzlich eingeschränkt bzw. an besondere Voraussetzungen geknüpft sein kann (vgl. etwa Art. 27 Abs. 4 Sätze 5 und 6 Bayerisches Krankenhausgesetz, § 80 Zehntes Buch Sozialgesetzbuch, § 62 BDSG im Ordnungswidrigkeitenverfahren sowie Art. 108 Abs. 3 Bayerisches Beamtengesetz). In einem solchen Fall sind die jeweiligen gesetzlichen Vorgaben bei der Vertragsgestaltung zu berücksichtigen und entsprechend abzubilden.

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen .....
- Verantwortlicher (nachfolgend Auftraggeber genannt) -

und

.....
- Auftragsverarbeiter (nachfolgend Auftragnehmer genannt) -

Präambel
Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO zum Schutz der personenbezogenen Daten betroffener Personen und ergänzt insoweit den Vertrag vom …… (im Folgenden „Auftrag" genannt). Sie findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen der Auftragnehmer oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten für den Auftraggeber verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Art, Zweck und Gegenstand der Verarbeitung

Dauer der Verarbeitung

Art der verarbeiteten personenbezogenen Daten

Kategorien der betroffenen Personen

1.2 Die in diesem Vertrag vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Rechte und Pflichten des Auftragnehmers

2.1 Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. a DSGVO). Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.
Sofern Weisungen des Auftraggebers zunächst mündlich erfolgen, sind sie unverzüglich schriftlich oder elektronisch zu bestätigen.

2.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Unterabs. 2 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragnehmer berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt der Auftragnehmer bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Auftraggebers zu gewährleisten (Art. 32 Abs. 1 DSGVO). Sofern personenbezogene Daten in Telearbeit und Heimarbeit verarbeitet werden, ist er verpflichtet, dies dem Auftraggeber mitzuteilen. Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus (*bitte ausführen - ggf. mit Verweisung -, z. B. aus der Anlage zu dieser Vereinbarung, dem Sicherheitskonzept etc.*). Ände-

rungen der getroffenen Maßnahmen durch den Auftragnehmer sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen und mit diesem abzustimmen.

2.4 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Unterabs. 1 Buchst. e DSGVO) nachzukommen und unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. f DSGVO).

2.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. b DSGVO). Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

2.7 Der Auftragnehmer nennt dem Auftraggeber Ansprechpartner für im Rahmen des Vertrages anfallende Weisungen sowie einen etwaige(n) Datenschutzbeauftragte(n). Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftraggeber die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. eines oder einer etwaigen Datenschutzbeauftragten unverzüglich anzuzeigen.

Ansprechpartner des Auftragnehmers:
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

Datenschutzbeauftragte(r) des Auftragnehmers
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

2.8 Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

2.9 Nach Auftragsende sind Daten (einschließlich vorhandener Kopien), Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. g DSGVO).

2.10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

3.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3.4 Der Auftraggeber nennt dem Auftragnehmer weisungsberechtigte Personen für im Rahmen des Vertrages anfallende Weisungen sowie den / die Datenschutzbeauftragte(n). Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftragnehmer unverzüglich die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. eines oder einer Datenschutzbeauftragten anzuzeigen.

Weisungsberechtigte Personen des Auftraggebers sind:
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

Datenschutzbeauftragte(r) des Auftraggebers
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

3.5 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragnehmer geltend, wird dieser die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte.

5. Kontrollrechte des Auftraggebers

5.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. h DSGVO*). Ggf.: Folgende Nachweise sind diesem Vertrag als Anlage beigefügt:*

☐ *Ergebnisse eines Selbstaudits (Anlage)*

☐ *Zertifikat zu Datenschutz- und / oder Informationssicherheit (z. B. ISO 27001) (Anlage)*

☐ *Genehmigte Verhaltensregeln (Art. 40 DSGVO) vom … (Datum) (Anlage)*

☐ *Zertifizierungen gemäß Art. 42 DSGVO (Anlage)*

☐ *Verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO) vom … (Datum). (Anlage)*

☐ *aktuelles Testat und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer/ Wirtschaftsprüferin, Revision, Datenschutzbeauftragte(r), IT-Sicherheitsabteilung, Datenschutzauditor / Datenschutzauditorin Qualitätsauditor / Qualitätsauditorin, Anlage)*

☐ *…. (Anlage).*

5.2 *Sofern einschlägig: Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.*

5.3 Der Auftraggeber ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Dies und Maßnahmen nach Nr. 5.4 werden nicht durch die Vorlage von Nachweisen nach Nr. 5.1 ausgeschlossen.

5.4 Inspektionen durch den Auftraggeber oder durch einen von diesem beauftragten Prüfer werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten durchgeführt. Der Auftragnehmer hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass der Auftraggeber oder ein von diesem beauftragte(r) Prüfer / Prüferin im Rahmen seiner / ihrer Inspektion auch Kenntnis von Daten erlangt, die der Auftragnehmer im Auftrag eines anderen Verantwortlichen verarbeitet. Der Auftraggeber stellt sicher, dass ein von ihm beauftragter Prüfer / Prüferin in keinem Wettbewerbsverhältnis zu dem Auftragnehmer steht.

6. Unterauftragsverarbeiter (weitere Auftragsverarbeiter)

6.1 Ein Unterauftragsverarbeitungsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.
Der Auftragnehmer trägt bei der Auswahl eines Unterauftragsverarbeiters insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt.
Nicht als Unterauftragsverarbeitungsverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Auftraggebers ausgeschlossen ist), Reinigungskräfte und Prüfer. Der Auftragnehmer trifft mit diesen Dritten im erforderlichen Umfang schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

6.2 Der Auftragnehmer nimmt keinen Unterauftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung in Anspruch. Der Auftragnehmer teilt dem Auftraggeber die bereits bei Abschluss dieses Vertrags bestehenden Unterauftragsverarbeitungsverhältnisse vorab mit. Die bei Vertragsbeginn bestehenden Unterauftragsverarbeitungsverhältnisse sind in *Anlage …* zu diesem Vertrag aufgeführt. Diese gelten als von Beginn des Auftrages an genehmigt.

6.3 Weitere Unterauftragsverarbeiter
Alternative 1:

☐ Gemäß den vorgenannten Regelungen erteilt der Auftraggeber dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO in Anspruch zu nehmen (Art. 28 Abs. 2 Satz 1 Alt. 2, Satz 2 DSGVO). Der Auftragnehmer informiert den Auftraggeber frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Einspruch ist innerhalb

von einem Monat nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragnehmer einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

Alternative 2:

☐ Der Auftragnehmer nimmt einen Unterauftragsverarbeiter nur in Anspruch, wenn der Auftraggeber dies zuvor gesondert schriftlich genehmigt hat (Art. 28 Abs. 2 Satz 1 Alt. 1 DSGVO). Der Auftragnehmer informiert den Auftraggeber frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern beabsichtigt.

6.4 Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Unterauftragsverarbeiter sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung diesem wirksam aufzuerlegen. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.5 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden (Art. 28 Abs. 4 Satz 2 DSGVO).

6.6 Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber vorab zustimmt.

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten des Auftraggebers durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragnehmer gefährdet werden. Der Auftragnehmer informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Auftraggeber liegt.

8.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

8.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

_____, den _____	_____, den _____
Ort *Datum*	*Ort* *Datum*
_____	_____
- Auftraggeber -	- Auftragnehmer -

11. Muster einer Vereinbarung zur Regelung gemeinsamer Verantwortlichkeit

Das nachfolgende Muster einer Vereinbarung zur Regelung gemeinsamer Verantwortlichkeit ist möglichst universell gehalten und erhebt keinen Anspruch auf Vollständigkeit. Je nach konkreter Fallgestaltung kann es daher anzupassen oder zu ergänzen sein. Insbesondere stellt sich eine Aufgliederung der Verarbeitungen in einzelne Abschnitte, die sog. Wirkbereiche, nicht in jedem Fall als praktikabel oder gar zwingend dar.

Vereinbarung über die Verarbeitung personenbezogener Daten in gemeinsamer Verantwortlichkeit (Art. 26 Datenschutz-Grundverordnung – DSGVO)

zwischen .....(Partei 1)

und

..... (Partei 2)

Ggf. weitere Verantwortliche

gemeinsam als **Parteien**

1. Verantwortliche

1.1 Diese Vereinbarung regelt die Rechte und Pflichten der Verantwortlichen (im Folgenden auch „Parteien“ genannt) bei der gemeinsamen Verarbeitung personenbezogener Daten im Rahmen der nachfolgend näher festgelegten Verarbeitungstätigkeiten. Diese Vereinbarung gilt für alle Tätigkeiten, bei denen Beschäftigte der Parteien oder ein durch sie beauftragter Auftragsverarbeiter personenbezogene Daten für die Verantwortlichen verarbeiten.

1.2 Die Parteien sind sich darüber einig, dass sie bei der/den nachfolgend näher beschriebenen Verarbeitungstätigkeit/en gemeinsam über Zwecke und Mittel der Verarbeitung bestimmen und insoweit eine gemeinsame Verantwortlichkeit für festgelegte Prozessabschnitte besteht.

1.3 Im Rahmen der Kooperation/ des Projekts ……. werden personenbezogene Daten verarbeitet. Gegenstand der Verarbeitung ist …. Die Verarbeitung ist auf die Dauer von … bis … angelegt.[51]

1.4 Die Parteien legen die Prozessabschnitte gemäß **Anlage 1** fest, in denen personenbezogene Daten in gemeinsamer Verantwortlichkeit verarbeitet werden (Art. 26 DSGVO). Für die übrigen Prozessabschnitte, bei denen keine gemeinsame Festlegung der Zwecke und Mittel einzelner Phasen der Datenverarbeitung besteht, ist jede Partei eigenständiger Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

2. Wirkbereiche

2.1 Im Rahmen der gemeinsamen Verantwortlichkeit ist Partei 1 für die Verarbeitung personenbezogener Daten wie folgt zuständig (Wirkbereich A):

Prozessabschnitt (vgl. **Anlage 1**)

_____

Art, Zweck und Gegenstand der Verarbeitung

_____

Im Rahmen der gemeinsamen Verantwortlichkeit ist Partei 2 für die Verarbeitung personenbezogener Daten wie folgt zuständig (Wirkbereich B):
Prozessabschnitt (vgl. **Anlage 1**)

_____

Art, Zweck und Gegenstand der Verarbeitung

_____

Die Parteien erklären einvernehmlich, dass diese Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegelt.

[51] Angabe zur Dauer ist nicht zwingend, jedoch, wenn möglich, aufzunehmen.

2.2 Die Kategorien der verarbeiteten Daten, die Kategorien der betroffenen Personen sowie die Rechtsgrundlagen der Verarbeitung, für die eine gemeinsame Verantwortlichkeit besteht, sind in der **Anlage 1** dieser Vereinbarung festgelegt.

3. Zuweisung der datenschutzrechtlichen Verpflichtungen

3.1 Jede Partei ist für die Umsetzung der Verpflichtungen gemäß der DSGVO, insbesondere der Informationspflichten sowie der Rechte der betroffenen Personen, in ihrem Wirkbereich zuständig. Diesbezügliche Informationen und Mitteilungen gegenüber betroffenen Personen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu gestalten.

Alternativ können hier auch andere Gestaltungen hinsichtlich der Erfüllung der Informationspflichten gewählt werden. Beispielsweise kann vereinbart werden, dass eine der beiden Parteien alleine für die Zurverfügungstellung der Informationen nach Art. 13 und 14 DSGVO zuständig ist.

3.2 Ungeachtet dieser Festlegung können betroffene Personen ihre Betroffenenrechte bei und gegenüber jeder Partei geltend machen. Die Parteien verpflichten sich, einander sämtliche für die Beantwortung von Auskunftsersuchen notwendigen Informationen zur Verfügung zu stellen.

3.3 Soweit sich eine betroffene Person an eine der Parteien in Wahrnehmung ihrer Betroffenenrechte wendet, insbesondere wegen Auskunft oder Berichtigung und Löschung ihrer personenbezogenen Daten, verpflichten sich die Parteien, dieses Ersuchen unverzüglich unabhängig von der Pflicht zur Gewährleistung des Betroffenenrechtes an die andere Partei weiterzuleiten. Diese ist verpflichtet, der anfragenden Partei die zur Bearbeitung des Ersuchens notwendigen Informationen aus ihrem Wirkbereich unverzüglich zur Verfügung zu stellen.

3.4 Sollen personenbezogene Daten gelöscht werden, informieren sich die Parteien zuvor gegenseitig. Die jeweils andere Partei kann der Löschung aus berechtigtem Grund widersprechen, etwa sofern sie eine gesetzliche Aufbewahrungspflicht trifft.

3.5 Die zuständigen Ansprechpartner der Parteien sind:

Ansprechpartner der Partei 1:
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

_____

Ansprechpartner der Partei 2:
(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

_____

3.6 Die Parteien teilen sich gegenseitig den Namen und die Kontaktdaten des / der Datenschutzbeauftragten mit, sofern ein solcher / eine solche von der jeweiligen Partei benannt werden muss.

Datenschutzbeauftragte(r) der Partei 1:
(Name, Vorname, Telefon, E-Mail)

_____

Datenschutzbeauftragte(r) der Partei 2:
(Name, Vorname, Telefon, E-Mail)

_____

3.7 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner oder des / der Datenschutzbeauftragten ist dies der jeweils anderen Partei unverzüglich anzuzeigen.

4. Grundsätze der gemeinsamen Verarbeitung

4.1 Jede Partei gewährleistet die Einhaltung der gesetzlichen Bestimmungen, insbesondere die Rechtmäßigkeit der durch sie im Rahmen der gemeinsamen Verantwortlichkeit durchgeführten Datenverarbeitungen. Die Verarbeitung kann nur bei Vorliegen einer entsprechenden Rechtsgrundlage erfolgen.

4.2 Die Parteien speichern die personenbezogenen Daten in einem strukturierten gängigen und maschinenlesbaren Format.

4.3 Die Parteien tragen dafür Sorge, dass nur personenbezogene Daten erhoben werden, die für die rechtmäßige Prozessabwicklung zwingend erforderlich sind. Im Übrigen beachten

die Parteien den Grundsatz der Datenminimierung im Sinne von Art. 5 Abs. 1 Buchst. c DSGVO.

5. Technisch-organisatorische Maßnahmen

5.1 Die Parteien stellen innerhalb ihres Wirkbereichs sicher, dass die nach Art. 24, 25, 32 DSGVO jeweils erforderlichen technischen und organisatorischen Maßnahmen implementiert und eingehalten werden.

5.2 Die Parteien stellen innerhalb ihres Wirkbereiches sicher, dass alle mit der Datenverarbeitung befassten Mitarbeitenden die Vertraulichkeit der Daten gemäß Art. 28 Abs. 3, 29 und 32 DSGVO für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses wahren sowie in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen werden.

5.3 Die Parteien haben eigenständig dafür Sorge zu tragen, dass sie sämtliche in Bezug auf die Daten bestehenden gesetzlichen Aufbewahrungspflichten einhalten. Sie haben hierzu angemessene Datensicherheitsvorkehrungen (Art. 32 ff. DSGVO) zu treffen. Dies gilt insbesondere im Falle der Beendigung der Zusammenarbeit.

5.4 Die Parteien ergreifen alle erforderlichen technischen und organisatorischen Maßnahmen, damit die Rechte der betroffenen Personen, insbesondere nach den Art. 12 bis 22 DSGVO, innerhalb der gesetzlichen Fristen jederzeit gewährleistet werden können bzw. sind.

6. Auftragsverarbeitung

6.1 Die Parteien verpflichten sich, beim Einsatz von Auftragsverarbeitern im Anwendungsbereich dieser Vereinbarung einen Vertrag nach Art. 28 DSGVO abzuschließen und die schriftliche Zustimmung der anderen Vertragspartei vor Abschluss des Vertrages einzuholen. Sollte ein Auftragsverarbeiter von mehreren Vertragspartnern gleichzeitig in Anspruch genommen werden, so verpflichten sich diese, im Rahmen des Auftragsverarbeitungsverhältnisses klarzustellen, in wessen Wirkbereich die jeweilige Datenverarbeitung im Auftrag erfolgt.

6.2 Die Parteien informieren sich gegenseitig rechtzeitig über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von als Subunternehmer eingesetzten Auftragsverarbeitern und beauftragen nur solche Subunternehmer, die die Anforderungen des Datenschutzrechts und die Festlegungen dieser Vereinbarung erfüllen.

7. Melde- und Benachrichtigungspflichten

7.1 Den Parteien obliegen die aus Art. 33, 34 DSGVO resultierenden Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen für ihren jeweiligen Wirkbereich. Die Parteien verpflichten sich gegenseitig, auch im Interesse der jeweils anderen Vertragsparteien, den Pflichten nach Art. 33, 34 DSGVO unverzüglich nachzukommen.

7.2 Die Parteien informieren sich unverzüglich gegenseitig über die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde nach Art. 33 DSGVO und leiten sich die zur Durchführung der Meldung erforderlichen Informationen jeweils unverzüglich zu.

7.3 Ist eine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person nach Art. 34 DSGVO erforderlich, so informieren und unterstützen sich die Parteien gegenseitig und führen die Benachrichtigung gegebenenfalls gemeinsam durch.

8. Dokumentation

Dokumentationen im Sinne von Art. 5 Abs. 2 DSGVO, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, werden durch jede Partei entsprechend den rechtlichen Befugnissen und Verpflichtungen über das Ende der Vereinbarung hinaus aufbewahrt.

9. Verarbeitungsverzeichnis

Die Parteien nehmen die Verarbeitungstätigkeiten in das Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO auf, auch und insbesondere mit einem Vermerk zur Natur der Verarbeitungstätigkeiten in gemeinsamer oder alleiniger Verantwortlichkeit.

10. Bekanntgabe an betroffene Personen

Die Parteien verpflichten sich, den wesentlichen Inhalt der Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit gemäß Art. 26 Abs. 2 Satz 2 DSGVO den betroffenen Personen zur Verfügung zu stellen. (**Anlage 2**)

Alternativ können hier auch andere Gestaltungen gewählt werden. Beispielsweise kann vereinbart werden, dass eine der beiden Parteien alleine für die Zurverfügungstellung des wesentlichen Inhalts zuständig ist und wie die Informationen zur Verfügung gestellt werden. Die betroffene Person kann ihre Rechte allerdings gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).

11. Datenschutz-Folgenabschätzung

Ist eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO erforderlich, unterstützen sich die Parteien gegenseitig.

12. Schadensersatz

12.1 Unbeschadet der Regelungen dieser Vereinbarung haften die Parteien für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, im Außenverhältnis gemäß Art. 82 Abs. 4 DSGVO gemeinsam gegenüber den betroffenen Personen.

12.2 Im Innenverhältnis haften die Parteien, unbeschadet der Regelungen dieser Vereinbarung, nur für Schäden, die innerhalb ihres jeweiligen Prozessabschnittes entstanden sind.

12.3 Für den Fall einer Inanspruchnahme hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig bei der Abwehr der Ansprüche im Rahmen ihrer Möglichkeiten zu unterstützen.

13. Schlussbestimmungen

13.1 Die Parteien informieren sich gegenseitig unverzüglich und vollständig, wenn sie bei der Prüfung der Verarbeitungstätigkeiten Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellen.

13.2 Die Parteien informieren sich unverzüglich gegenseitig, wenn eine Datenschutzaufsichtsbehörde sich an sie wendet und dies eine Verarbeitung betrifft, die von dieser Vereinbarung umfasst ist.

13.3 Nebenabreden zu dieser Vereinbarung sind nicht getroffen. Änderungen oder Ergänzungen bedürfen zu ihrer Rechtswirksamkeit der Textform und enthalten den ausdrücklichen Hinweis darauf, dass es sich um Änderungen bzw. Ergänzungen dieser Vereinbarung handelt. Das gilt auch für den Verzicht auf das Erfordernis der Textform.

13.4 Falls eine Bestimmung dieser Vereinbarung unwirksam sein sollte, so berührt dies die Wirksamkeit der übrigen Regelungen dieser Vereinbarung nicht. Dies gilt auch, soweit die Vereinbarung eine Regelungslücke enthält. An die Stelle der unwirksamen Regelung oder Lücke sollen die Parteien eine angemessene Ersatzregelung treffen, die dem am nächsten kommt, was die Parteien gewollt hätten, wenn sie diesen Aspekt bedacht hätten.

_____, den _____	_____, den _____
Ort *Datum*	*Ort* *Datum*
_____	_____
- Partei 1 -	- Partei 2 -

Anlage 1

Festlegung der verantworteten Prozessabschnitte

Prozessabschnitt	Datenkategorien	Betroffene Personen	Rechtsgrundlage	Zuständiger Verantwortlicher

Anlage 2

Informationen zur gemeinsamen Verantwortlichkeit der Partei 1 und der Partei 2 nach Art. 26 Abs. 2 S. 2 der Datenschutz-Grundverordnung (DSGVO)

Was ist der Grund für die gemeinsame Verantwortlichkeit?

Bei *„dem Projekt“* arbeiten *Partei 1* und *Partei 2* eng zusammen. Dies betrifft auch die Verarbeitung Ihrer persönlichen Daten. Die Parteien haben gemeinsam die Reihenfolge der Verarbeitung dieser Daten in den einzelnen Prozessabschnitten festgelegt. Sie sind daher innerhalb der nachfolgend beschriebenen Prozessabschnitte gemeinsam für den Schutz Ihrer personenbezogenen Daten verantwortlich (Art. 26 DSGVO).

Was haben die Parteien vereinbart?

Im Rahmen ihrer gemeinsamen datenschutzrechtlichen Verantwortlichkeit haben *Partei 1* und *Partei 2* vereinbart, wer von ihnen welche Pflichten nach der DSGVO erfüllt. Dies betrifft insbesondere die Wahrnehmung der Rechte der betroffenen Personen und die Erfüllung der Informationspflichten gemäß den Artikeln 13 und 14 DSGVO.

Diese Vereinbarung ist notwendig, da bei *[Anwendung/System konkret benennen]* personenbezogene Daten in unterschiedlichen Prozessabschnitten und Systemen verarbeitet werden, die entweder von *Partei 1* oder *Partei 2* betrieben werden.

Was bedeutet das für Sie als betroffene Person?

Auch wenn eine gemeinsame Verantwortlichkeit besteht, erfüllen die Parteien die datenschutzrechtlichen Pflichten entsprechend ihrer jeweiligen Zuständigkeiten für die einzelnen Prozessabschnitte wie folgt:

Prozessabschnitt	Datenkategorien	Betroffene Personen	Rechtsgrundlage	Zuständiger Verantwortlicher

- Jede Partei macht Ihnen im Rahmen ihrer Zuständigkeit die gemäß Art. 13 und 14 DSGVO erforderlichen Informationen unentgeltlich zugänglich.
- Ihre Datenschutzrechte können sowohl bei *Partei 1* als auch bei *Partei 2* geltend gemacht werden. Sie erhalten die Rückmeldung grundsätzlich von der Stelle, bei der Sie Ihre Rechte geltend gemacht haben. Hierfür lässt jede Partei der anderen sämtliche dafür notwendigen Informationen aus ihrem Prozessabschnitt zukommen.

12. Datenschutz-Folgenabschätzung und Risikoanalyse nach der DSGVO

12.1 Wozu dient die Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung nach Art. 35 und 36 DSGVO (DSFA) soll sicherstellen, dass bei Verarbeitungen, die voraussichtlich ein hohes datenschutzrechtliches Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine besondere Prüfung der Rechtmäßigkeit und Sicherheit der geplanten Verarbeitungen durchgeführt wird. Ziel ist, geeignete technische und organisatorische Maßnahmen zu ermitteln und umzusetzen, mit denen diese datenschutzrechtlichen Risiken für die betroffenen Personen vermieden oder zumindest auf ein angemessenes Niveau minimiert werden können (vgl. Erwägungsgrund 90, Satz 2).

Voraussetzungen und Durchführung dieser DSFA unterscheiden sich erheblich von der vor Inkrafttreten der DSGVO datenschutzrechtlichen Freigabe nach Art. 26 BayDSG-alt. Insbesondere ist nicht für jedes bisher freigabepflichtige Verfahren eine DSFA durchzuführen.

Im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz gelten in Umsetzung von Art. 27 Richtlinie zum Datenschutz bei Polizei und Justiz spezialgesetzliche Sonderregelungen.

Für die **Verfolgung von Straftaten und Ordnungswidrigkeiten** (und somit insoweit für Polizeibehörden ebenso wie für kommunale Stellen relevant) wurden die Vorgaben des Art. 27 Richtlinie zum Datenschutz bei Polizei und Justiz zur DSFA in **§ 67 BDSG** (i.V.m. § 500 Abs. 1 StPO, § 46 Abs. 1 OWiG) umgesetzt.[52]

[52] Sonderregelungen im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz ergeben sich außerdem aus Art. 200 Abs. 1 Bayerisches Strafvollzugsgesetz (BayStVollzG), Art. 34 Bayerisches Maßregelvollzugsgesetz (BayMRVG), Art. 96 Bayerisches Sicherungsverwahrungsvollzugsgesetz (BaySvVollzG), Art. 34 Bayerisches Jugendarrestvollzugsgesetz (BayJAVollzG), Art. 36 Bayerisches Untersuchungshaftvollzugsgesetz (BayUVollzG).

12.2 Für welche Verarbeitungen ist eine DSFA durchzuführen?

Eine DSFA ist vom Verantwortlichen durchzuführen, wenn eine Form der Verarbeitung „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein *hohes* Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat („Hochrisikoverarbeitungen“). Eine DSFA ist jedenfalls vor dem Einsatz einer solchen Verarbeitung durchzuführen. Eine Pflicht zur Durchführung einer DSFA gilt ferner auch für bereits im Einsatz befindliche Verarbeitungsvorgänge und die sie unterstützenden Verfahren (siehe auch 12.2.5), wenn die o.g. Punkte zutreffen und noch keine DSFA erfolgt ist. Ist bereits eine DSFA erfolgt und ändert sich der Verarbeitungsvorgang wesentlich, ist erneut eine DSFA durchzuführen.

Dazu ist vor dem Einsatz eines Verarbeitungsvorgangs oder bei wesentlicher Änderung eines im Einsatz befindlichen Verarbeitungsvorgangs zunächst eine Vorabprüfung vorzunehmen, ob dieser möglicherweise ein solch hohes datenschutzrechtliches Risiko für die Betroffenen darstellen könnte (sog. DSFA-Erforderlichkeitsprüfung mit der **„Schwellwertanalyse“**). Eine gute Grundlage für die Vorabprüfung bietet dabei das jeweilige Informationssicherheitskonzept.

Kommt die Vorabprüfung zu dem Ergebnis, dass mangels hohem datenschutzrechtlichen Risiko keine DSFA-Pflicht besteht, hat der Verantwortliche unabhängig davon die gemäß Art. 24 und 32 DSGVO stets erforderliche **Risikoanalyse** durchzuführen und die geeigneten **technischen und organisatorischen Maßnahmen** zu treffen (Risikoanalyse, vgl. dazu Erwägungsgrund 83; im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz auch Art. 32 BayDSG).

12.2.1 Ausnahmen

Eine DSFA durch den Verantwortlichen kann unterbleiben, soweit

- eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird (Art. 35 Abs. 1 Satz 2 DSGVO i.V.m. Art. 14 Abs. 1 Nr. 1 BayDSG) oder
- eine öffentliche Stelle ein automatisiertes Verfahren entwickelt hat, das zum Einsatz durch öffentliche Stellen bestimmt ist, für dieses Verfahren die DSFA bereits durchgeführt hat

und das Verfahren von der einsetzenden öffentlichen Stelle im Wesentlichen unverändert übernommen wird (Art. 35 Abs. 1 Satz 2 DSGVO i.V.m. Art. 14 Abs. 2 BayDSG).

Ob ein Verarbeitungsvorgang bzw. -Verfahren „im Wesentlichen unverändert übernommen wird“, ist vom Verantwortlichen zu prüfen. Regelmäßig sollte bei zentralen Verfahren eine sog. „Zentral-DSFA“ vom Betreiber bzw. Hersteller durchgeführt werden und den einsetzenden Stellen diese zur Verfügung gestellt werden. Die Verantwortlichen der einsetzenden Stellen haben dann lediglich die am Einsatzort spezifischen Punkte noch zu prüfen und ggf. in der DSFA zu ergänzen.

- Hinweis: Eine sog. Whitelist im Sinne von Art. 35 Abs. 5 DSGVO, welche die Arten von Verarbeitungsvorgängen umfasst, für die keine DSFA erforderlich ist, hat der Bayerische Landesbeauftragte für den Datenschutz bisher nicht erstellt.

- Eine DSFA durch den Verantwortlichen kann auch unterbleiben, soweit der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine DSFA erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist (Art. 35 Abs. 10 DSGVO i.V.m. Art. 14 Abs. 1 Nr. 2 BayDSG). Ob eine DSFA bereits im Rechtssetzungsverfahren erfolgt ist, muss sich in diesem Fall aus den entsprechenden Unterlagen, z. B. den Landtags-Drucksachen, ergeben. Art. 14 Abs. 1 Nr. 2 BayDSG findet auch im Bereich der Richtlinie zum Datenschutz bei Polizei und Justiz gem. Art. 28 Abs. 3 Nr. 3 BayDSG Anwendung.

- In Art. 35 Abs. 1 Satz 2 DSGVO und für die Straf- und Bußgeldverfolgung in § 67 Abs. 2 BDSG ist außerdem eine gemeinsame DSFA für mehrere ähnliche Verarbeitungsvorgänge vorgesehen.

Auch wenn die Überprüfung ergeben hat, dass keine DSFA durchgeführt werden muss, so ist gemäß Art. 24 und 32 DSGVO stets eine **Risikoanalyse** durchzuführen und es müssen Maßnahmen zum Schutz der personenbezogenen Daten ergriffen werden, die gemäß Art. 5 Abs. 2 DSGVO auch zu dokumentieren sind (vgl. dazu auch Erwägungsgrund 83). Ein Informationssicherheitskonzept (Art. 11 Abs. 1 Satz 2 BayEGovG bzw. künftig Art. 43 Abs. 1 Satz 2 BayDiG-E) kann teilweise Basis dafür sein.

Die Risikoanalyse und die darauf basierenden Maßnahmen sind im Richtlinienbereich für die Bayerische Polizei hinsichtlich der Sicherheit der Verarbeitung ausführlich in Art. 32 BayDSG geregelt. Für die Datenverarbeitung zur Verfolgung von **Straftaten oder Ordnungswidrigkeiten** enthält § 64 Abs. 3 BDSG eine ähnliche Regelung.

12.2.2 Schwellwertanalyse[53]

Ein *Risiko* im Sinne der DSGVO ist das Bestehen einer Möglichkeit des Eintritts eines Ereignisses, das einen Schaden darstellt. Im Mittelpunkt steht der mögliche datenschutzrechtliche Schaden für die betroffenen Personen. Der Rufschaden für die öffentliche Stelle, der durch Bekanntwerden eines Schadens für betroffene Personen entsteht, stellt zwar selbst keine datenschutzrechtliche Schadensposition dar, kann allerdings erfahrungsgemäß die Motivation für entsprechende Abhilfemaßnahmen erhöhen.

Mögliche datenschutzrechtliche Schäden können physischer, materieller oder immaterieller Art sein, wie z. B. eine Diskriminierung, ein Identitätsdiebstahl, ein finanzieller Verlust, eine Rufschädigung bei den betroffenen Personen, eine Hinderung der Kontrolle über eigene Daten, ein Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, eine unbefugten Aufhebung der Pseudonymisierung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile (vgl. Erwägungsgrund 75 DSGVO). Insbesondere Ursache, Art, Besonderheit und Schwere von Risiken eines Verarbeitungsvorgangs sind zu evaluieren (vgl. Erwägungsgrund 84 DSGVO). Einzubeziehen ist auch die Eintrittswahrscheinlichkeit eines Schadens. Je höher der mögliche Schaden eines Vorfalls ist und je höher dessen Eintrittswahrscheinlichkeit ist, desto höher ist das Risiko.

Voraussetzung für eine Pflicht zur DSFA nach Art. 35 DSGVO ist ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen. Nicht jeder möglicherweise eintretende Schaden führt automatisch zu einem hohen Risiko. Ein hohes Risiko liegt nur vor, wenn ein erheblicher datenschutzrechtlicher Schaden bei einer Verletzung des Schutzes der Daten droht und die Wahrscheinlichkeit für den Eintritt eines solchen Schadens nicht unerheblich ist.

---

[53] Vgl. zur Methodik der Schwellwertanalyse umfassend die Orientierungshilfe des BayLfD zur Datenschutz-Folgenabschätzung, S. 9 ff, abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf.

12.2.3 Regelbeispiele in Art. 35 Abs. 3 DSGVO

In Art. 35 Abs. 3 DSGVO werden Verarbeitungsvorgänge beispielhaft aufgeführt, die einer DSFA unterliegen. Im öffentlichen Bereich wird insbesondere die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO, von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO und die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche als Voraussetzung für eine DSFA in Frage kommen.

Bei der Prüfung der Frage, was eine „umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten" ist, ist insbesondere die Zahl voraussichtlich betroffener Personen zu berücksichtigen (Erwägungsgrund 91, Satz 1 DSGVO). Andererseits kann auch eine besondere Sensibilität der verarbeiteten besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO ein Kriterium für die Verpflichtung zur DSFA sein.
Eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche" liegt z. B. bei einer umfangreichen Videoüberwachung von öffentlichen Verkehrsmitteln, Fußgängerzonen oder öffentlichen Plätzen vor. Die Videoüberwachung eines Dienstgebäudes im Rahmen des Hausrechts erfüllt dagegen diese Voraussetzung regelmäßig nicht, wenn sich diese Überwachung auf das Gebäude selbst und den unmittelbar angrenzenden Eingangsbereich beschränkt.

Für den Bereich der Richtlinie zum Datenschutz bei Polizei und Justiz können die Regelbeispiele des Art. 35 Abs. 3 DSGVO, welche Anhaltspunkte dafür liefern, wann im Anwendungsbereich der DSGVO eine DSFA durchzuführen ist, nicht uneingeschränkt übernommen werden. Insbesondere die dort genannte Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten wäre stets gegeben. Erwägungsgrund 52 zur Richtlinie zum Datenschutz bei Polizei und Justiz stellt dementsprechend für die Notwendigkeit einer DSFA auf ein „besonderes Risiko" der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen ab.

12.2.4 „Blacklist" im Sinne von Art. 35 Abs. 4 DSGVO

Der Bayerische Landesbeauftragte für den Datenschutz hat auf seiner Internetseite eine „Bayerische Blacklist"[54] im Sinne von Art. 35 Abs. 4 DSGVO veröffentlicht, die anhand von neun Kriterien Leitlinien für die Prüfung der Frage enthält, für welche Verarbeitungen eine

[54] Die Liste ist abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf.

DSFA nach Art. 35 DSGVO in jedem Fall durchzuführen ist. Anhand von 21 Fallgruppen wird darin die Anwendung dieser Kriterien an Beispielen verdeutlicht.

Für die Entscheidung, ob eine Form der Verarbeitung eine DSFA erfordert, ist die Liste des Bayerischen Landesbeauftragten für den Datenschutz hilfreich, aber nicht abschließend. Für alle Verarbeitungsvorgänge, die nicht in der „Blacklist" enthalten sind, ist vom Verantwortlichen im Rahmen einer Schwellwertanalyse zu prüfen und zu dokumentieren, ob die Voraussetzungen von Art. 35 Abs. 1 DSGVO vorliegen und eine DSFA durchgeführt werden muss.

Im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz gibt es keine derartige „Blacklist". Allerdings sieht Art. 64 Abs. 1 Satz 2 PAG die generelle Mitteilung aller Errichtungsanordnungen an den Bayerischen Landesbeauftragte für den Datenschutz vor. Art. 64 Abs. 2 Satz 3 PAG erlaubt dem Bayerischen Landesbeauftragten für den Datenschutz außerdem festzulegen, welche Verarbeitungsvorgänge vor ihrer erstmaligen Anwendung einer DSFA bedürfen.

12.2.5 Alt- bzw. Bestandsverfahren

Der Bayerische Landesbeauftragte für den Datenschutz sah für Verarbeitungen, die bei Geltungsbeginn der DSGVO bereits im Einsatz waren, eine Übergangsfrist bis spätestens Mai 2021 vor.[55] Im Falle eines DSFA-pflichtigen Bestandsverfahrens kann auch nach Mai 2021 einstweilen auf die Durchführung einer DSFA verzichtet werden, wenn

- für das Bestandsverfahren eine ordnungsgemäße, noch tragfähige Freigabe im Sinne des Art. 26 BayDSG-Alt (Datenschutzrechtliche Freigabe automatisierter Verfahren) besteht,
- ein noch tragfähiges IT-Sicherheitskonzept vorliegt und
- das Bestandsverfahren ohne wesentliche Änderung fortgeführt wird.

Die Prüfung und das Ergebnis, ob einstweilen auf eine DSFA verzichtet werden kann, muss dokumentiert werden. Wichtig ist in diesem Zusammenhang, dass sich im Hinblick auf die IT-Sicherheit technische Standards sehr häufig ändern und sich neue Bedrohungsszenarien ergeben können. Zudem können sich wesentliche Änderungen an einem Verfahren auch durch äußere Umstände ergeben, ohne dass aktiv eine Änderung herbeigeführt wurde.

---

[55] Dazu Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz, https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf, S. 13.

Unabhängig davon müssen auch bei Bestandsverfahren vom Verantwortlichen die Vorgaben von Art. 24 und Art. 32 DSGVO in Hinblick auf die stets erforderliche **Risikoanalyse** und die geeigneten technisch-organisatorische Maßnahmen eingehalten werden (vgl. Erwägungsgrund 83 DSGVO).

12.3 Durchführung der DSFA

Die DSFA umfasst:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung (Art. 35 Abs. 7 Buchst. a DSGVO).
  Geeigneter Ausgangspunkt dafür ist die entsprechende Beschreibung im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck (Art. 35 Abs. 7 Buchst. b DSGVO).
- Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (Art. 35 Abs. 7 Buchst. c DSGVO) Die bereits bei der Entscheidung, ob eine DSFA durchzuführen ist, kursorisch durchgeführte Schwellwertanalyse ist hier zu konkretisieren.
- Die geplanten Abhilfemaßnahmen zur Bewältigung dieser Risiken (Art. 35 Abs. 7 Buchst. d DSGVO). Das von einer Form der Verarbeitung ausgehende Risiko muss durch geeignete technische, organisatorische und ggf. rechtliche Schutzmaßnahmen „bewältigt", d.h. beseitigt oder auf ein angemessenes Niveau minimiert werden. Technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung sind nach Art. 32 DSGVO ohnehin durchzuführen. Im Rahmen der DSFA ist zu prüfen, ob zusätzliche Maßnahmen zur Bewältigung des festgestellten hohen datenschutzrechtlichen Risikos erforderlich und angezeigt sind. Zu berücksichtigen ist auch das Risiko fahrlässigen und unrechtmäßigen Handelns interner und externer Risikoquellen. Als technisch-organisatorische Maßnahmen zur Bewältigung möglicher Risiken kommen z. B. die Begrenzung von Zugriffsberechtigungen oder die Protokollierung von Abrufen mit Stichprobenüberprüfungen in Frage.

Die Durchführung der DSFA und die dabei vorgenommenen Beschreibungen und Bewertungen sind zu dokumentieren (vgl. Art. 5 Abs. 2 DSGVO).

Ergänzende und vertiefende Ausführungen finden sich in

- der Orientierungshilfe Datenschutz-Folgenabschätzung des Bayerischen Landesbeauftragten für den Datenschutz, Stand: 1. Februar 2021, Ziff. 4 (S. 13 ff)[56]
- dem Working Paper 248 der Datenschutzgruppe nach Artikel 29, Abschn. D (S. 17 ff.)[57] und
- dem Arbeitspapier Datenschutz-Folgenabschätzung – Methodik und Fallstudie des Bayerischen Landesbeauftragten für den Datenschutz, Stand: 1. Oktober 2019, nebst Leerformularen und Ausfüllbeispielen.[58]

Inwiefern davon die nach Art. 64 Abs. 2 Satz 4 PAG vorgesehene Bewertung der Risiken betroffen wird, ist noch in der Abstimmung.

12.4 Personelle Rahmenbedingungen hinsichtlich der Durchführung

Aufgrund der umfassenden Betrachtung und Analyse bei einer DSFA sollte diese von einem Team durchgeführt werden.

Bei dessen Zusammenstellung ist es wichtig, eine Balance zwischen Unabhängigkeit und Verantwortlichkeit herzustellen. Für die Objektivität und Glaubwürdigkeit der Ergebnisse ist es entscheidend, dass das Team in der Lage ist, eine wirkungsvolle Prüfung vorzunehmen. Dafür ist sicherzustellen, dass ausreichend Ressourcen (Zeit, Personal, Kompetenzen) zur Verfügung stehen.

Das Team sollte über eine möglichst große Bandbreite von Qualifikationen und Erfahrungen verfügen, da die Identifikation von Risiken für die Rechte und Freiheiten natürlicher Personen und die Erarbeitung passender Lösungen i. d. R. eine Mischung aus technischer, juristischer betriebswirtschaftlicher und praktischer, anwenderbezogener Expertise erfordert. Aus diesem Grund empfiehlt sich die Einbeziehung des IT-Bereichs, des/der Informationssicherheitsbeauftragten sowie des / der Datenschutzbeauftragten.

---

[56] Abrufbar unter https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf.
[57] Abrufbar unter https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
[58] Abrufbar unter https://www.datenschutz-bayern.de/technik/orient/oh_dsfa_beispiel.pdf.

Damit die Prüfung die gewünschten Ziele erreichen kann, insbesondere die Änderung von als kritisch bewerteten Elementen, ist gleichzeitig zu gewährleisten, dass die für die Entwicklung oder Einführung verantwortlichen Personen in den Bewertungsprozess eingebunden sind.

Zudem sind Dritte, etwa Auftragsverarbeiter oder Hersteller von IT-Systemen, einzubeziehen, wenn dies notwendig ist, um eine vollständige Beschreibung eines Systems sowie der Entwicklung etwaiger Abhilfemaßnahmen zu gewährleisten.

Im Rahmen der Beschaffung entsprechender IT-Systeme bietet es sich an, die geeignete Unterstützung bei der Erstellung einer DSFA bzw. einer Risikoanalyse nach Art. 24 und 32 DSGVO durch den Hersteller oder Betreiber mitauszuschreiben.

12.5 Beteiligung der betroffenen Personen oder ihrer Vertreter

Nach Art. 35 Abs. 9 DSGVO holt der Verantwortliche gegebenenfalls den Standpunkt der betroffenen Personen oder deren Vertreter ein. Die Feststellung, welche konkreten Personen von einer Verarbeitung betroffen sind, wird oft schwierig oder gar nicht möglich sein. Nicht umfassend möglich ist dies z. B. bei online-Angeboten von Verwaltungsverfahren. Beteiligt werden können in solchen Fallgestaltungen allenfalls die potentiell betroffenen Personen. Denkbar wäre dazu z. B. in geeigneten Fällen die Veröffentlichung entsprechender Pläne für Verarbeitungen mit dem Hinweis, dass eine Stellungnahme dazu abgegeben werden kann.

Vertreter der betroffenen Personen können z. B. bei der Verarbeitung von Personaldaten die zuständigen Personalvertretungen sein, die nach den Vorschriften des Personalvertretungsrechts ohnehin bei der Einrichtung entsprechender automatisierter Verfahren zu beteiligen sind.

Eine Beteiligung der betroffenen Personen oder deren Vertreter erfolgt nicht, soweit dies zum Schutz gewerblicher oder öffentlicher Interessen notwendig ist oder die Sicherheit der Verarbeitungsvorgänge gefährdet ist.

Im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz ist keine Beteiligung der betroffenen Personen vorgesehen.

12.6 Beteiligung des / der behördlichen Datenschutzbeauftragten

Der Verantwortliche hat bei der Durchführung einer DSFA den Rat des / der Datenschutzbeauftragten einzuholen (Art. 35 Abs. 2 DSGVO), d.h. er hat diesem/dieser Gelegenheit zur Stellungnahme zu geben. Die Verantwortung für die Rechtmäßigkeit der Verarbeitung sowie für die ordnungsgemäße Durchführung der DSFA verbleibt allerdings bei dem Verantwortlichen, der an die Stellungnahme des / der behördlichen Datenschutzbeauftragten nicht gebunden ist.

Im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz ist die Beteiligung des / der behördlichen Datenschutzbeauftragten nach § 67 Abs. 3 BDSG, nicht aber nach Art. 64 Abs. 2 PAG, verpflichtend. Allerdings sollte der / die behördliche Datenschutzbeauftragte bei komplexen Fragen zum Datenschutz stets um seine / ihre Unterstützung gebeten werden.

12.7 Vorherige Konsultation der Aufsichtsbehörde

Die Konsultation der Aufsichtsbehörde ist gemäß Art. 36 Abs. 1 DSGVO nur dann erforderlich, wenn eine DSFA gemäß Art. 35 DSGVO zu dem Ergebnis führt, dass die beabsichtigte Verarbeitung ein hohes datenschutzrechtliches Risiko zur Folge hätte und der Verantwortliche keine Maßnahmen zur Eindämmung dieses Risikos trifft (vgl. hierzu auch Erwägungsgrund 94, Satz 1 DSGVO).

Im Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz erhält der Bayerische Landesbeauftragte für den Datenschutz gemäß Art. 64 Abs. 2 Satz 6 bis 8 PAG stets Gelegenheit zur Stellungahme zu einer durchgeführten DSFA. Das BDSG (i.V.m. § 500 StPO, § 47 OWiG) sieht im Rahmen der Straf- oder Ordnungswidrigkeitenverfolgung in § 69 Abs. 1 Satz 1 Nr. 1 BDSG lediglich die Konsultation des Bayerischen Landesbeauftragten für den Datenschutz ähnlich den Vorgaben des Art. 36 DSGVO vor. In § 69 Abs. 1 Satz 2 BDSG ist darüber hinaus lediglich die Befugnis des Bayerischen Landesbeauftragten für den Datenschutz vorgesehen, eine Liste der Verarbeitungsvorgänge zu erstellen, die der Pflicht zur Anhörung des Bayerischen Landesbeauftragten für den Datenschutz unterliegen.

12.8 Regelmäßige Überprüfung

Nach Art. 35 Abs. 11 DSGVO führt der Verantwortliche erforderlichenfalls eine Überprüfung durch, ob der Verarbeitung gemäß der DSFA durchgeführt wird. Zumindest dann, wenn neue Risiken aufgetreten sind, ist die DSFA durch den Verantwortlichen auch auf ihre Aktualität zu überprüfen und ggf. entsprechend anzupassen.
Der / die behördliche Datenschutzbeauftragte überwacht dies nach Maßgabe von Art. 39 Abs. 1 Buchst. c DSGVO.

13. Muster[59] einer Zweckvereinbarung für die Zusammenarbeit im Datenschutz

Zweckvereinbarung

Zusammenarbeit im Datenschutz

Der Landkreis _____,

vertreten durch den Landrat,

folgende Städte, Märkte und Gemeinden:

_____,

jeweils vertreten durch den Oberbürgermeister/ersten Bürgermeister,

folgende Verwaltungsgemeinschaften[60]:

_____,

jeweils vertreten durch den Gemeinschaftsvorsitzenden,

und

folgende Zweckverbände:

_____,

jeweils vertreten durch den Verbandsvorsitzenden,

(im Folgenden als „Beteiligte“ bezeichnet) schließen nach Art. 7 ff. des Gesetzes über die kommunale Zusammenarbeit (KommZG), folgende

Z W E C K V E R E I N B A R U N G:

§ 1

Zweck der Vereinbarung

Jeder Beteiligte der Zweckvereinbarung hat nach Art. 37 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) eine(n) behördliche(n) Datenschutzbeauftragte(n) zu benennen.

---

[59] Bei dem Muster handelt es sich um eine Gemeinschaftsvereinbarung gemäß Art. 7 Abs. 3 KommZG.

[60] Die Mitgliedsgemeinden der beteiligten Verwaltungsgemeinschaften sind aufgrund von Art. 4 Abs. 2 Satz 1 Verwaltungsgemeinschaftsordnung zudem selbst an der Zweckvereinbarung beteiligt. Ergänzende Informationen zum Thema der Datenschutzverantwortlichkeit bei Verwaltungsgemeinschaften finden sich in der Aktuellen Kurz-Information 2: Datenschutzverantwortlichkeit bei bayerischen Verwaltungsgemeinschaften des Bayerischen Landesbeauftragten, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki02.html.

Die Beteiligten wollen im Wege der interkommunalen Zusammenarbeit den Datenschutz durch eine(n) gemeinsame(n) behördliche(n) Datenschutzbeauftragte(n) effizienter und effektiver gestalten, sowie eine fachlich kompetente und wirtschaftliche Erfüllung von beim Vollzug des Datenschutzes anfallenden Aufgaben gewährleisten.

§ 2
Gemeinsame Aufgabenerfüllung

1. Die Beteiligten beabsichtigen, eine(n) gemeinsame(n) behördliche(n) Datenschutzbeauftragte(n) (Datenschutzbeauftragte(r)) zu benennen.
2. Der Landkreis / die Stadt / der Markt / die Gemeinde / die Verwaltungsgemeinschaft / der Zweckverband _____ (Bestellungsbehörde) stellt zu diesem Zweck im Einvernehmen mit den übrigen Beteiligten eine geeignete Fachkraft bereit, die im Umfang von ___ Wochenstunden als Datenschutzbeauftragte(r) tätig wird sowie eine Vertretung. Die Beteiligten benennen diese Personen jeweils zu ihrem / ihrer behördlichen Datenschutzbeauftragten sowie zu dessen / deren Vertretung. Die Bestellungsbehörde stellt die zur Erfüllung dieser Aufgabe erforderlichen Einrichtungen sowie einen ausgestatteten Arbeitsplatz zur Verfügung.
3. Die Beteiligten unterstützen den / die Datenschutzbeauftragten bei der Arbeit. Sie gewährleisten, dass der / die Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird und im Rahmen seiner / ihrer Aufgaben ungehinderten Zugang zu allen Akten, Dokumenten und sonstigen schriftlichen und elektronischen Unterlagen in der betreffenden Behörde erhält. Ferner stellen sie dem / der Datenschutzbeauftragten innerhalb ihrer Behörde die erforderlichen Arbeitsmittel sowie einen örtlichen Ansprechpartner zur Verfügung, der den / der Datenschutzbeauftragten bei der Erfüllung seiner / ihrer Aufgaben vor Ort unterstützt. Der / die Datenschutzbeauftragte und die örtlichen Ansprechpartner informieren sich gegenseitig umfassend und rechtzeitig über datenschutzrechtlich relevante Angelegenheiten. Hierzu schaffen sie geeignete Verfahren der Zusammenarbeit. Dazu zählen regelmäßige Vor-Ort-Termine bei den Beteiligten sowie der Austausch über Telefon und Internet. Informationen, Muster und Checklisten für die Beteiligten werden bereitgestellt.

§ 3
Aufgabenbereich des Datenschutzbeauftragten

1. Der / die Datenschutzbeauftragte erfüllt die ihm / ihr gesetzlich zugewiesenen Aufgaben bei allen Beteiligten. Dazu zählen die Aufgaben nach Art. 39 Abs. 1 und 38 Abs. 4 DSGVO, Art. 12 Abs. 1 Satz 1 Nr. 2 und Art. 24 Abs. 5 BayDSG, insbesondere auch
   - die Beratung der Beteiligten bei Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Abs. 1 DSGVO und bei Benachrichtigungen der betroffenen Personen nach Art. 34 Abs. 1 DSGVO
   - die Beratung der Beteiligten, ob eine Datenschutz-Folgenabschätzung vor einer Verarbeitung erforderlich ist und ggf. Hilfestellung bei deren Durchführung
   - die Zusammenarbeit mit der Aufsichtsbehörde und die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung personenbezogener Daten durch die Beteiligten zusammenhängende Fragen.
2. Der / die Datenschutzbeauftragte erstattet jedem Beteiligten regelmäßig, mindestens alle zwei Jahre, Bericht zum Datenschutz. In dem Bericht sind die bei dem jeweiligen Beteiligten eingesetzten technischen und organisatorischen Maßnahmen darzustellen sowie ggf. festgestellte Datenschutzverstöße und Schutzlücken aufzuführen. Die Berichte enthalten eine Bewertung, ob die eingesetzten technischen und organisatorischen Maßnahmen ausreichend sind, dem Stand der Technik entsprechen und ob datenschutzrechtliche Risiken bestehen. Die Ergebnisse der Berichte werden mit den Beteiligten erörtert. Die Berichte werden nicht veröffentlicht.
3. Der / die Datenschutzbeauftragte erfüllt ferner folgende Aufgaben bei allen Beteiligten:
   - ☐ die Führen des Verzeichnisses der Verarbeitungstätigkeiten
   - ☐ die Überprüfung und Anpassung von Formularen im Hinblick auf Art. 13 DSGVO
   - ☐ die Überprüfung und Anpassung bestehender Vereinbarungen zur Auftragsverarbeitung
   - ☐ die Meldung der Kontaktdaten nach Art. 37 Abs. 7 DSGVO an die Aufsichtsbehörde.
4. Die Verantwortung für die Einhaltung und Beachtung datenschutzrechtlicher Vorschriften tragen weiterhin die Beteiligten in ihrer datenschutzrechtlichen Funktion als Verantwortliche selbst.

§ 4
Kosten- und Umlageregelung

1. Die durch die Aufgabenerfüllung des / der Datenschutzbeauftragten bei der Bestellungsbehörde anfallenden Betriebs-, Personal- und Sachkosten werden von den Beteiligten gemeinsam getragen:
   Der Landkreis trägt _____ % der Kosten.
   Die Stadt _____ trägt _____ % der Kosten.
   Der Markt _____ trägt _____ % der Kosten.
   Die Gemeinde _____ trägt _____ % der Kosten.
   Die Verwaltungsgemeinschaft _____ trägt _____ % der Kosten.
   Der Zweckverband _____ trägt _____ % der Kosten.
2. Die Bestellungsbehörde legt die Kosten nach Ablauf des jeweiligen Kalenderjahres auf die Beteiligten um und erstellt jährlich bis spätestens _____ eine Abrechnung, mit welcher die Kosten des Vorjahres abgerechnet werden. Die Abrechnung enthält eine Kostenübersicht und ist an alle übrigen Beteiligten zuzusenden. Diese entrichten den Betrag innerhalb _____ nach dem Zugang der Abrechnung an die Bestellungsbehörde.

§ 5
Kündigung

1. Die auf unbestimmte Zeit abgeschlossene Zweckvereinbarung kann unter Einhaltung einer Kündigungsfrist von einem Jahr jeweils zum Ende eines Kalenderjahres von jedem Beteiligten gekündigt werden. Die Kündigung ist schriftlich gegenüber den übrigen Beteiligten zu erklären.
2. Das Recht jedes Beteiligten zur Kündigung aus wichtigem Grund (außerordentliche Kündigung) bleibt unberührt.
3. Sollte ein Beteiligter die Zweckvereinbarung kündigen, so bleibt die Zweckvereinbarung in dieser Fassung für die verbleibenden Beteiligten weiterhin gültig.
4. Bei einer Kündigung dieser Vereinbarung durch einen oder mehrere Beteiligte erhöht sich der Kostenanteil der verbleibenden Beteiligten entsprechend.

§ 6
Schriftformerfordernis

Änderungen dieser Zweckvereinbarung bedürfen der Schriftform.

§ 7
Schlichtung

Bei Streitigkeiten über Rechte und Pflichten unter den Beteiligten aufgrund dieser Zweckvereinbarung soll vor Beschreitung des Klagewegs die Regierung _____ als übergeordnete Aufsichtsbehörde zur Schlichtung aufgerufen werden.

§ 8
Wirksamwerden

Diese Zweckvereinbarung wird am ..... wirksam.

Ort, Datum Unterschriften

14. Muster für ein Impressum und eine Datenschutzerklärung im Internetauftritt einer Behörde

14.1 Impressum

Herausgeber

- *Bezeichnung, Hausanschrift und Postanschrift der Behörde:*
  (vollständige ladungsfähige Anschrift, die ausschließliche Angabe einer Postfachadresse genügt nicht)
- *Telefon:*
- *evtl. Telefax:*
- *E-Mail:*
  (in der Regel: poststelle@behördenkürzel.de)
- *Vor- und Nachname des / der Vertretungsberechtigte(n):*
  (in der Regel der Dienststellenleiter / Dienstellenleiterin oder Bürgermeister / Bürgermeisterin)
- *USt-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz*

Verantwortlich für den Inhalt

Vor- und Nachname der für den Inhalt verantwortlichen Person oder Personen (Anschrift siehe oben).
Namentlich gekennzeichnete Internetseiten geben die Auffassungen und Erkenntnisse der genannten Personen wieder.

Nutzungsbedingungen

Texte, Bilder, Grafiken sowie die Gestaltung dieser Internetseiten können dem Urheberrecht unterliegen.
Nicht urheberrechtlich geschützt sind nach § 5 des Urheberrechtsgesetzes (UrhG)

- Gesetze, Verordnungen, amtliche Erlasse und Bekanntmachungen sowie Entscheidungen und amtlich verfasste Leitsätze zu Entscheidungen und

- andere amtliche Werke, die im amtlichen Interesse zur allgemeinen Kenntnisnahme veröffentlicht worden sind, mit der Einschränkung, dass die Bestimmungen über Änderungsverbot und Quellenangabe in § 62 Abs. 1 bis 3 und § 63 Abs. 1 und 2 UrhG entsprechend anzuwenden sind.

Als Privatperson dürfen Sie urheberrechtlich geschütztes Material zum privaten und sonstigen eigenen Gebrauch im Rahmen des § 53 UrhG verwenden. Eine Vervielfältigung oder Verwendung urheberrechtlich geschützten Materials dieser Seiten oder Teilen davon in anderen elektronischen oder gedruckten Publikationen und deren Veröffentlichung ist nur mit unserer Einwilligung gestattet. Diese Einwilligung erteilen auf Anfrage die für den Inhalt Verantwortlichen. Der Nachdruck und die Auswertung von Pressemitteilungen und Reden sind mit Quellenangabe allgemein gestattet.

Weiterhin können Texte, Bilder, Grafiken und sonstige Dateien ganz oder teilweise dem Urheberrecht Dritter unterliegen. Auch über das Bestehen möglicher Rechte Dritter geben Ihnen die für den Inhalt Verantwortlichen nähere Auskünfte.

Haftungsausschluss

Alle auf dieser Internetseite bereitgestellten Informationen haben wir nach bestem Wissen und Gewissen erarbeitet und geprüft. Eine Gewähr für die jederzeitige Aktualität, Richtigkeit, Vollständigkeit und Verfügbarkeit der bereit gestellten Informationen können wir allerdings nicht übernehmen. Ein Vertragsverhältnis mit den Nutzern / der Nutzerin des Internetangebots kommt nicht zustande.

Wir haften nicht für Schäden, die durch die Nutzung dieses Internetangebots entstehen. Dieser Haftungsausschluss gilt nicht, soweit die Vorschriften des § 839 BGB (Haftung bei Amtspflichtverletzung) einschlägig sind. Für etwaige Schäden, die beim Aufrufen oder Herunterladen von Daten durch Schadsoftware oder der Installation oder Nutzung von Software verursacht werden, übernehmen wir keine Haftung.

Falls im Einzelfall erforderlich: Der Haftungsausschluss gilt nicht für Informationen, die in den Anwendungsbereich der Europäischen Dienstleistungsrichtlinie (Richtlinie 2006/123/EG – DLRL) fallen. Für diese Informationen wird die Richtigkeit und Aktualität gewährleistet.

Links

Von unseren eigenen Inhalten sind Querverweise („Links“) auf die Webseiten anderer Anbieter zu unterscheiden. Durch diese Links ermöglichen wir lediglich den Zugang zur Nutzung fremder Inhalte nach § 8 Telemediengesetz. Bei der erstmaligen Verknüpfung mit diesen Internetangeboten haben wir diese fremden Inhalte daraufhin überprüft, ob durch sie eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Wir können diese fremden Inhalte aber nicht ständig auf Veränderungen überprüfen und daher auch keine Verantwortung dafür übernehmen. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung von Informationen Dritter entstehen, haftet allein der jeweilige Anbieter der Seite.

14.2 Datenschutzerklärung[61]

Dem/der [*Behörde*] ist Datenschutz ein wichtiges Anliegen. Wir legen deshalb auch bei der mit unserer Aufgabenerfüllung verbundenen Verarbeitung personenbezogener Daten Wert auf eine datensparsame und bürgerfreundliche Datenverarbeitung.
Diese Datenschutzerklärung bezieht sich auch auf die Verarbeitung personenbezogener Daten und Informationen im Sinnes des § 25 TTDSG im Rahmen dieses Internetauftritts, einschließlich der dort angebotenen Dienste.

Name und Kontaktdaten des Verantwortlichen

Bezeichnung der öffentlichen Stelle
Postanschrift:
Telefon:
Evtl. Telefax:
E-Mail:

[61] Über die Information des Betroffenen über die Datenverarbeitung im Rahmen des Internetauftritts hinausgehend kann die Datenschutzerklärung auch als Standort gewählt werden, um den Betroffenen über weitere Datenverarbeitungen der Behörde gemäß Art. 13 und 14 DSGVO zu informieren z. B. Information des Betroffenen über die Verarbeitung personenbezogener Daten bei Veranstaltungen oder bei bestimmten Fachverfahren. In diesem Fall gilt es, die Datenschutzerklärung abhängig vom Einzelfall um die jeweiligen Angaben zu ergänzen.

Kontaktdaten des / der Datenschutzbeauftragten

Sie erreichen unseren Datenschutzbeauftragten / unsere Datenschutzbeauftragte unter:
Behördliche/r Datenschutzbeauftragte/r der/des (Bezeichnung der öffentlichen Stelle)
- persönlich -
Postanschrift:
Telefon:
E-Mail: (z. B. datenschutz@behörde.de)

Zwecke und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

Zweck der Verarbeitung ist die Erfüllung der uns vom Gesetzgeber zugewiesenen öffentlichen Aufgaben.
Die Rechtsgrundlage für die Verarbeitung Ihrer Daten ergibt sich, soweit nichts anderes angegeben ist, aus Art. 4 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG) in Verbindung mit Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e der Datenschutzgrundverordnung (DSGVO). Demnach ist es uns erlaubt, die zur Erfüllung einer uns obliegenden Aufgabe erforderlichen Daten zu verarbeiten.
Soweit Sie in eine Verarbeitung eingewilligt haben, stützt sich die Datenverarbeitung auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DSGVO.

Empfänger von personenbezogenen Daten

Soweit Ihre Daten elektronisch verarbeitet werden, erfolgt der technische Betrieb unserer Datenverarbeitungssysteme durch [*Stelle xy, z. B. das*
Bayerische Landesamt für Digitalisierung, Breitband und Vermessung
Alexandrastr. 4
80538 München
E-Mail: poststelle@ldbv.bayern.de]

Gegebenenfalls werden Ihre Daten an die zuständigen Aufsichts- und Rechnungsprüfungsbehörden zur Wahrnehmung der jeweiligen Kontrollrechte übermittelt.
Zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik können Protokolldaten auf Grundlage von Art. 12 des Bayerischen E-Government-Gesetzes bzw. Art. 44 BayDiG-E an das Landesamt für Sicherheit in der Informationstechnik weitergeleitet werden (näheres siehe unter „Protokollierung“).

Dauer der Speicherung der personenbezogenen Daten

Wir speichern Ihre Daten solange dies für die Erfüllung der Aufgabe, zu Dokumentationspflichten bzw. aufgrund gesetzlicher Aufbewahrungsfristen erforderlich ist.

Rechte der betroffenen Person

Soweit wir von Ihnen personenbezogene Daten verarbeiten, stehen Ihnen als betroffene Person nachfolgende Rechte zu:

- Sie können Auskunft dazu verlangen, ob wir personenbezogene Daten von Ihnen verarbeiten. Ist dies der Fall, so haben Sie ein Recht auf Auskunft über diese Daten sowie auf weitere mit der Verarbeitung zusammenhängende Informationen (Art. 15 Datenschutz-Grundverordnung - DSGVO). Bitte beachten Sie, dass dieses Auskunftsrecht in bestimmten Fällen eingeschränkt oder ausgeschlossen sein kann (vgl. insbesondere Art. 10 des Bayerischen Datenschutzgesetzes - BayDSG). Für den Fall, dass personenbezogene Daten über Sie nicht (mehr) zutreffend oder unvollständig sind, können Sie eine Berichtigung und gegebenenfalls Vervollständigung dieser Daten verlangen (Art. 16 DSGVO).
- Bei Vorliegen der gesetzlichen Voraussetzungen können Sie die Löschung Ihrer personenbezogenen Daten (Art. 17 DSGVO) oder die Einschränkung der Verarbeitung dieser Daten (Art. 18 DSGVO) verlangen. Das Recht auf Löschung nach Art. 17 Abs. 1 und 2 DSGVO besteht jedoch unter anderem dann nicht, wenn die Verarbeitung personenbezogener Daten erforderlich ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 17 Abs. 3 Buchstabe b DSGVO).
- Falls Sie in die Verarbeitung eingewilligt haben und die Verarbeitung auf dieser Einwilligung beruht, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.
- Aus Gründen, die sich aus Ihrer besonderen Situation ergeben, können Sie der Verarbeitung Sie betreffender personenbezogener Daten durch uns zu dem jederzeit widersprechen (Art. 21 DSGVO). Sofern die gesetzlichen Voraussetzungen vorliegen, verarbeiten wir in der Folge Ihre personenbezogenen Daten nicht mehr.

Weitere Einschränkungen, Modifikationen und gegebenenfalls Ausschlüsse der vorgenannten Rechte können sich aus der Datenschutz-Grundverordnung oder nationalen Rechtsvorschriften ergeben.

Ausführlichere Informationen zu diesen Rechten erteilt Ihnen auch unser/e behördliche/r Datenschutzbeauftragte/r.

Beschwerderecht bei der Aufsichtsbehörde

Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz. Diesen können Sie unter folgenden Kontaktdaten erreichen:
Postanschrift: Postfach 22 12 19, 80502 München
Adresse: Wagmüllerstraße 18, 80538 München
Telefon: 089 212672-0
Telefax: 089 212672-50

Online-Meldung https://www.datenschutz-bayern.de/service/complaint.html

Technische Umsetzung

Unser Web-Server wird durch [*Stelle xy, z. B. das Bayerische Landesamt für Digitalisierung, Breitband und Vermessung*] betrieben. Die von Ihnen im Rahmen des Besuchs unseres Webauftritts übermittelten personenbezogenen Daten werden daher in unserem Auftrag durch [*Stelle xy, z. B. das Bayerische Landesamt für Digitalisierung, Breitband und Vermessung*] verarbeitet:
Bezeichnung und Kontaktdaten der Stelle:
z. B. Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung
Alexandrastr. 4
80538 München
E-Mail: poststelle@ldbv.bayern.de

Protokollierung

Wenn Sie diese oder andere Internetseiten aufrufen, übermitteln Sie über Ihren Internetbrowser Daten an unseren Webserver. Die folgenden Daten werden während einer laufenden Verbindung zur Kommunikation zwischen Ihrem Internetbrowser und unserem Webserver aufgezeichnet: (***ggf. anpassen***:)

- *Datum und Uhrzeit der Anforderung*
- *Name der angeforderten Datei*
- *Seite, von der aus die Datei angefordert wurde*
- *Zugriffsstatus (beispielsweise Datei übertragen, Datei nicht gefunden)*
- *verwendete Webbrowser und verwendetes Betriebssystem*

- *vollständige IP-Adresse des anfordernden Rechners*
- *übertragene Datenmenge*

Aus Gründen der technischen Sicherheit, insbesondere zur Abwehr von Angriffsversuchen auf unseren Webserver, werden diese Daten von uns gespeichert. *Nach spätestens sieben Tagen werden die Daten durch Verkürzung der IP-Adresse auf Domain-Ebene anonymisiert, so dass es nicht mehr möglich ist, einen Bezug zu einzelnen Nutzern herzustellen*.
Zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik werden diese Daten auf Grundlage von Art. 12 des Bayerischen E-Government-Gesetzes bzw. Art. 44 BayDiG-E an das Landesamt für Sicherheit in der Informationstechnik weitergeleitet.

Sichere Datenübertragung
Mit Aufruf dieses Informationsangebots bieten wir eine *mit HTTPS und Perfect Forward Secrecy verschlüsselte Verbindung mit dem Verschlüsselungsprotokoll TLS 1.2 an*, sodass Ihre Daten bei der Datenübertragung vor einer Kenntnisnahme durch Dritte geschützt sind. Wir empfehlen Ihnen, Ihren Internetbrowser zur Nutzung dieser Möglichkeit aktuell zu halten.

Cookies
Zur korrekten technischen und funktionellen Bereitstellung dieses Informationsangebots verwenden wir Cookies. Cookies sind kleine Textdateien, die auf dem von Ihnen verwendeten Gerät gespeichert werden.
Rechtsgrundlage für die Speicherung von Informationen sowie die Verarbeitung personenbezogener Daten mittels Cookies ist § 25 TTDSG.
Die Verwendung funktionaler Cookies ist freiwillig. Wenn diese Cookies blockiert werden, ist die Bereitstellung bestimmter Funktionen ggf. nicht in vollem Umfang möglich.
Technisch notwendige Cookies sind nur für die jeweils aktuelle Sitzung gültig und werden automatisch gelöscht, sobald Sie Ihren Browser schließen.

In den Cookies werden dabei folgende Daten gespeichert und verarbeitet ***(ggf. anpassen):***
- *Spracheinstellungen,*
- *Log-In-Informationen*
- *(…)*

Ggf. verwenden wir nach Erteilung der Einwilligung Cookies zur Analyse des Surfverhaltens der Nutzerinnen und Nutzer dieses Internetangebots, vgl. den Punkt „Webanalyse-Tool Matomo“

Webanalyse-Tool Matomo

Unter der Voraussetzung, dass Sie uns diesbezüglich Ihre Einwilligung erteilen (§ 25 TTDSG), werten wir das Nutzerverhalten aus, um unseren Internetauftritt für Sie und andere Benutzer möglichst bedarfsgerecht zu gestalten. Hierzu verwenden wir das Webanalyse-Tool Matomo Analytics. Dieses setzt Cookies, also kleine Textdateien, die auf dem von Ihnen verwendeten Endgerät mit einer Gültigkeitsdauer von maximal zwei Jahren gespeichert werden. Die durch die Cookies gewonnenen Daten, wie beispielsweise die Länge der Verweildauer auf der Homepage oder eingegebene Suchbegriffe, werden auf Basis Ihrer Einwilligung von uns verarbeitet. Diese Daten ermöglichen uns Rückschlüsse über technische Parameter (z. B. das von Ihnen verwendete Betriebssystem oder die Bildschirmauflösung auf dem von Ihnen verwendeten Endgerät) sowie über die Nutzung unseres Internetauftritts. Ihre IP-Adresse wird dabei vor der Speicherung und der weiteren Verarbeitung anonymisiert.
Sofern Sie eine von Ihnen zuvor erteilte Einwilligung widerrufen, wird ein Cookie mit einer Laufzeit von zwei Jahren gesetzt, um die Webanalyse künftig zu verhindern.
Die Cookies enthalten lediglich anonymisierte Daten; ein Personenbezug kann wegen der anonymisierten Speicherung der IP-Adresse nicht hergestellt werden.
[Schaltfläche zur Zulässigkeit der Webanalyse (Widerruf der Einwilligung)]

Aktive Komponenten

Im Informationsangebot werden aktive Komponenten wie Javascript, Java-Applets oder Active-X-Controls verwendet. Diese Funktion kann durch die Einstellung Ihres Internetbrowsers von Ihnen abgeschaltet werden.

Einbindung von YouTube-Videos und SocialPlugins[62]

Beim Besuch unserer Internetseite werden über eine sogenannte Zwei-Klick-Lösung Zusatzdienste von YouTube und SocialPlugins (z. B. Twitter und Facebook) angeboten. Beim ersten Aufruf der Website werden keine Daten an die Betreiber übermittelt. Erst nachdem Sie als Nutzer durch einen entsprechenden Klick in das Opt-In-Verfahren eingewilligt haben, werden ab sofort und bei jedem weiteren Besuch Daten (unter anderem die URL der aktuellen Seite sowie Ihre IP-Adresse) an den jeweiligen Betreiber übertragen. Als Nutzer können

[62] Bei der Einbindung von Zusatzdiensten sind insbesondere die bestehenden Informationspflichten sowie die Anforderungen der Art. 44 ff. DSGVO zu beachten – die öffentliche Stelle als Websitebetreiberin unterliegt auch insoweit der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Sie damit selbst entscheiden, ob Sie der Aktivierung dieser Angebote und der Datenübermittlung zustimmen. Sie können diese Einwilligung jederzeit widerrufen und durch den entsprechenden Klick auf der Homepage die weitere Datenübermittlung an die Betreiber unterbinden.[63]

Einbindung von YouTube-Videos

Auf unserer Webseite sind Videos der externen Videoplattform YouTube eingebunden. Standardmäßig werden dabei lediglich deaktivierte Bilder des YouTube-Kanals eingebettet, die keine automatisierte Verbindung mit den Servern von YouTube herstellen. Damit erhält der Betreiber beim Aufruf der Webseiten keine Daten vom Benutzer.
Sie können selbst entscheiden, ob die YouTube-Videos aktiviert werden sollen. Erst wenn Sie das Abspielen der Videos mit Klick auf „Dauerhafte Aktivierung" freigeben, erteilen Sie die Einwilligung, dass die dafür erforderlichen Daten (unter anderem die Internetadresse der aktuellen Seite sowie Ihre IP-Adresse) an den Betreiber übermittelt werden.
Um die von Ihnen gewünschte Einstellung zu speichern, wird von uns ein Cookie gesetzt, das die Parameter abspeichert. Beim Setzen dieser Cookies werden von uns allerdings keine personenbezogenen Daten gespeichert, sie enthalten lediglich anonymisierte Daten zur Anpassung des Browsers. Anschließend sind die Videos aktiv und können vom Nutzer abgespielt werden. Möchten Sie das automatische Laden der YouTube-Videos wieder deaktivieren, können Sie unter dem Datenschutz-Symbol das Häkchen für die Zustimmung wieder entfernen. Damit werden auch die Einstellungen des Cookies aktualisiert.
YouTube ist ein Angebot von YouTube LLC, 901 Cherry Ave., San Bruno, CA 94066, USA, einem Tochterunternehmen von Google LLC., 1600 Amphitheater Parkway, Mountainview, California 94043, USA. Weitere Informationen zu Zweck und Umfang der Datenverarbeitung (auch außerhalb der Europäischen Union und außerhalb der USA) sowie Informationen zu Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre erhalten Sie in der Datenschutzerklärung: https://policies.google.com/privacy?hl=de&gl=de. Google verarbeitet Ihre personenbezogenen Daten unter anderem in den USA.

Einbindung von Facebook-Like-Button

Standardmäßig werden lediglich deaktivierte Buttons eingeblendet, die noch keinen Kontakt mit den Servern von Facebook herstellen. Erst wenn Sie mit einem zweiten Klick Ihre Einwilligung erklären, wird die Verbindung hergestellt und Ihr „Like" an Facebook übertragen. Nur

[63] Eine entsprechende Schaltfläche ist leicht zugänglich zu machen und gut zu kennzeichnen.

wenn Sie bei Facebook bereits angemeldet sind, wird Ihr „Like“ ohne ein weiteres Fenster übermittelt.
Die Datenschutzhinweise von Facebook finden Sie unter https://www.facebook.com/help/568137493302217. Die Verarbeitung Ihrer Daten durch Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Irland bzw. die Verarbeitung Ihrer Daten auch außerhalb der Europäischen Union und der USA erläutert Facebook unter: https://www.facebook.com/privacy/explanation. Facebook Inc., 1601 Willow Road, Menlo Park, California 94025, verarbeitet Ihre personenbezogenen Daten auch in den USA.

Vorlesefunktion
Wir möchten möglichst vielen Nutzern einen breiten und auf die individuellen Bedürfnisse abgestimmten Zugang zu unserer Homepage ermöglichen. Im Sinne der Barrierefreiheit wird daher auf der Homepage eine Vorlesefunktion angeboten.
Bei Nutzung dieser Vorlesefunktion werden die dafür erforderlichen technischen Daten (wie z. B. Browsereinstellungen) übermittelt an den Auftragsverarbeiter, die Firma:
[…]

Erhebung weiterer Daten
Soweit Sie in unserem Internetauftritt persönliche oder geschäftliche Daten (E-Mail-Adressen, Namen, Anschriften, etc.) eingeben, werden diese ausschließlich für die Übersendung der gewünschten Informationen oder die im Formular genannten Zwecke verwendet. Ihre Daten werden dabei auf dem Transport unter Verwendung einer Software (SSL) verschlüsselt und sind vor einer Kenntnisnahme durch Dritte geschützt. Die Daten werden nicht an Dritte weitergegeben. Die Nutzung der dort angebotenen Serviceleistungen und Dienste erfolgt auf freiwilliger Basis.
Sie können sich regelmäßig unseren Newsletter zusenden lassen. Ihre E-Mail-Adresse wird für den Versand des Newsletters gespeichert und nur zum Zweck der Versendung verarbeitet.
Die Zusendung des Newsletters können Sie jederzeit selbst wie folgt beenden: Wenn Sie sich abmelden wollen, abonnieren Sie bitte den Newsletter erneut auf die bereits eingetragene E-Mail-Adresse. Sie erhalten dann eine E-Mail mit einem Abmelde-Link. Ihre E-Mail-Adresse wird nach Klick auf den Abmelde-Link automatisch gelöscht.
Bei einer Bestellung von Veröffentlichungen werden Ihre Kontaktdaten nur zum Zweck der Zusendung der bestellten Veröffentlichungen verarbeitet. Spätestens ein Jahr nach der Bestellung werden Ihre Daten bei uns gelöscht.

Ihre Adresse und Ihre Bestellung werden zur Abwicklung an die mit dem Versand beauftragte Firma weitergeleitet:
[…]

Elektronische Post (E-Mail)
Informationen, die Sie unverschlüsselt per Elektronische Post (E-Mail) an uns senden, können möglicherweise auf dem Übertragungsweg von Dritten gelesen werden. Wir können in der Regel auch Ihre Identität nicht überprüfen und wissen nicht, wer sich hinter einer E-Mail-Adresse verbirgt. Eine rechtssichere Kommunikation durch einfache E-Mail ist daher nicht gewährleistet. Wir setzen - wie viele E-Mail-Anbieter - Filter gegen unerwünschte Werbung („SPAM-Filter“) ein, die in seltenen Fällen auch normale E-Mails fälschlicherweise automatisch als unerwünschte Werbung einordnen und löschen. E-Mails, die schädigende Programme („Viren“) enthalten, werden von uns in jedem Fall automatisch gelöscht.
Wenn Sie schutzwürdige Nachrichten an uns senden wollen, empfehlen wir, unser sicheres Kontaktformular zu nutzen.

Bewerbungen[64]
Zum Zwecke der Abwicklung des Bewerbungsverfahrens werden die übersandten personenbezogenen Daten von Bewerbern verarbeitet. Die Verarbeitung kann auch auf elektronischem Wege erfolgen. Dies ist insbesondere dann der Fall, wenn ein Bewerber entsprechende Bewerbungsunterlagen auf elektronischem Weg, beispielsweise per sicherem Kontaktformular, übermittelt. Kommt es zu einem Beschäftigungsverhältnis mit einem Bewerber, werden die übermittelten Daten zum Zwecke der Abwicklung des Beschäftigungsverhältnisses unter Beachtung der gesetzlichen Vorschriften gespeichert. Zudem können Daten im Bewerbungs- und Einstellungsverfahren an weitere Behörden (*z. B.Behörde xy*) oder an Behörden, die für die Abwicklung des Beschäftigungsverhältnisses zuständig sind (*z. B. Behörde xy*) übermittelt werden. Kommt es zu keinem Beschäftigungsverhältnis, so werden die Bewerbungsunterlagen nach Bekanntgabe der Absageentscheidung nach den einschlägigen Vorschriften gelöscht, sofern einer Löschung keine sonstigen berechtigten Interessen [*der Stelle xy*] entgegenstehen. Sonstiges berechtigtes Interesse in diesem Sinne ist beispielsweise eine Beweispflicht in einem Verfahren nach dem Allgemeinen Gleichbehandlungsgesetz (AGG).

[64] Sofern gesonderte Datenschutzinformationen für die spezifische Verarbeitungstätigkeit existieren, sind die gegenständlichen Ausführungen dort anzubringen.

Veranstaltungen[65]

[*Behörde xy*] ist Organisator oder Mitorganisator von Veranstaltungen. Zu diesem Zweck verarbeiten wir auf Grundlage von Art. 4 Abs. 1 BayDSG i. V. m. Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DSGVO personenbezogene Daten (Name, Kontaktdaten etc.) der Teilnehmerinnen und Teilnehmer.

Woher stammen diese Daten?

Die Daten erheben wir aus allgemein zugänglichen Quellen (z. B. Zeitung oder Veröffentlichungen im Internet), direkt bei den Teilnehmern der Veranstaltungen (z. B. durch Bereitstellen eines Formulars, per E-Mail oder per Telefon) oder erhalten sie von anderen öffentlichen oder nichtöffentlichen Stellen.

Was geschieht mit den Daten?

Die Daten werden zur Vorbereitung und Durchführung der jeweiligen Veranstaltungen (z. B. Erstellung von Gästelisten und die Ermöglichung von Zugangskontrollen) verarbeitet.
Je nach Art der Veranstaltung tritt [*Behörde xy*] neben einem weiteren Kooperationspartner als Mitveranstalter auf. In diesen Fällen werden die erhobenen Daten an diesen Kooperationspartner oder ggf. an einen externen Dienstleister übermittelt, wobei diese die Daten ebenfalls nur zur ordnungsgemäßen Durchführung der Veranstaltung verwenden dürfen.
Die Daten werden gelöscht, wenn sie zur Erfüllung der Aufgaben [*der Behörde xy*] nicht mehr erforderlich sind, spätestens jedoch nach 30 Jahren.

Foto- und Videoaufnahmen, Teilnahme von Medienvertretern

Bei unseren Veranstaltungen werden Fotos und ggf. auch Videos aufgenommen, die für die Öffentlichkeitsarbeit [*der Behörde xy*] verwendet werden. Bei manchen Veranstaltungen sind auch Medienvertreter anwesend.

Ihre Rechte

Ihnen stehen die oben beschriebenen Rechte zu (siehe „Rechte der betroffenen Person").
Im Fall eines Widerspruchs gegen die Verarbeitung Ihrer Daten ist die Teilnahme an der Veranstaltung allerdings dann u.U. nicht möglich.

---

[65] Vgl. Fußnote 64.

Unabhängig davon haben Sie das Recht, der Veröffentlichung von Fotos oder Videos, auf denen Sie erkennbar sind, zu widersprechen. Für einen Widerspruch wenden Sie sich bitte an die einladende Stelle.

Vorbereitung und Durchführung von Auszeichnungen und Ehrungen[66]
Behörde xy ist Organisator oder Mitorganisator von Veranstaltungen, bei denen Personen Auszeichnungen oder Ehrungen für besondere Verdienste verliehen bzw. ausgehändigt werden. *Zudem sind wir an der Prüfung von Vorschlägen für Auszeichnungen und Ehrungen anderer staatlichen Stellen beteiligt.*
Zu diesem Zweck verarbeiten wir auf Grundlage von Art. 27 BayDSG personenbezogene Daten der zu ehrenden Personen (Name, Kontaktdaten, Grund der Auszeichnung etc.).

Woher stammen die Daten?
Die Daten erhalten wir von anderen öffentlichen oder nichtöffentlichen Stellen oder Personen oder erheben sie aus öffentlich zugänglichen Quellen (z. B. aus Zeitungen oder Veröffentlichungen im Internet). Einige Daten erheben wir auch direkt bei den zu ehrenden Personen (z. B. durch Bereitstellen eines Formulars, per E-Mail oder per Telefon).

Was geschieht mit den Daten?
Die Daten werden zur Prüfung von Auszeichnungsvorschlägen und zur Vorbereitung und Durchführung der jeweiligen Veranstaltungen verarbeitet.
Je nach Auszeichnung oder Ehrung kann auch eine Übermittlung an Mitglieder der Staatsregierung, Abgeordnete, kommunale Mandatsträger, Kooperationspartner und externe Dienstleister erfolgen.
Im Rahmen der Öffentlichkeitsarbeit können Daten der geehrten Personen und die jeweilige Auszeichnung oder Ehrung im Internetauftritt *von Behörde xy* veröffentlicht und an die Medien zur Veröffentlichung übermittelt werden.
Die Daten werden gelöscht, wenn sie zur Erfüllung der Aufgaben *von Behörde xy* nicht mehr erforderlich sind.

[66] Vgl. Fußnote 64.

Foto- und Videoaufnahmen, Teilnahme von Medienvertretern

Bei unseren Veranstaltungen werden Fotos und ggf. auch Videos aufgenommen, die für die Öffentlichkeitsarbeit *der Behörde xy* und ggf. von Mitveranstaltern verwendet werden. Bei den Veranstaltungen sind in der Regel auch Medienvertreter anwesend.

Ihre Rechte

Wenn Sie eine Verarbeitung Ihrer personenbezogenen Daten nicht wünschen, teilen Sie uns dies bitte mit. Die Teilnahme an der Veranstaltung ist in diesem Fall allerdings dann u.U. nicht möglich.

Unabhängig davon haben Sie das Recht,

- der Veröffentlichung Ihrer Auszeichnung oder Ehrung im Rahmen der Öffentlichkeitsarbeit *von Behörde xy*, und ggf. von Mitveranstaltern,
- der Veröffentlichung von Fotos oder Videos, auf denen Sie erkennbar sind, und
- [*ggf. der Mitteilung Ihrer Auszeichnung oder Ehrung an Mitglieder der Staatsregierung, Abgeordnete und kommunale Mandatsträger zu Gratulationszwecken*]

zu widersprechen. Für einen Widerspruch wenden Sie sich bitte an die einladende Stelle.

Weiterer Hinweis zur Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung gelegentlich anzupassen, damit sie stets den aktuellen rechtlichen Anforderungen entspricht.

15. Weiterführende Informationen

- Bayerischer Landesbeauftragter für den Datenschutz, https://www.datenschutz-bayern.de/, v.a. unter den Reitern „Datenschutzreform 2018“ und „Aktuelles“,

- Datenschutzkonferenz (DSK), https://www.datenschutzkonferenz-online.de, v.a. unter dem Reiter „Infothek“,

- Europäischer Datenschutzausschuss (EDSA), https://edpb.europa.eu/edpb_de, v.a. unter dem Reiter „Unsere Arbeit und Hilfsmittel“,

- Bayerisches Staatsministerium für Unterricht und Kultus – Handreichung für den Datenschutz an Schulen, www.schuldatenschutz.bayern.de.

16. Mitwirkende

Diese Arbeitshilfen wurden vom Staatsministerium des Innern, für Sport und Integration unter Beteiligung des Bayerischen Landesbeauftragten für den Datenschutz erstellt und aktualisiert. An der Erstellung und Aktualisierung der Arbeitshilfen waren im Rahmen einer Arbeitsgruppe auch Vertreterinnen und Vertreter des Staatsministeriums der Finanzen und für Heimat, der kommunalen Spitzenverbände und der kommunalen Praxis maßgeblich beteiligt, denen wir an dieser Stelle für ihre konstruktive Mitarbeit ausdrücklich danken:

Frau Gudrun Aschenbrenner, Anstalt für Kommunale Datenverarbeitung in Bayern;
Herr Bernd Bauer-Banzhaf, Stadt Bamberg;
Herr Dr. Stephan Bobe, Staatsministerium der Finanzen und für Heimat;
Herr Jochen Dann, Stadt Aschaffenburg;
Frau Anna Distler, Landeshauptstadt München;
Herr Joachim Fackler, Staatsministerium der Finanzen und für Heimat;
Frau Brigitte Frey, Landeshauptstadt München;
Herr Klaus Geiger, Bayerischer Landkreistag;
Frau Irmgard Gihl, Bayerischer Bezirketag;
Frau Anne-Maria Helber, Staatsministerium für Ernährung, Landwirtschaft und Forsten;
Frau Annette Holl, Staatsministerium der Finanzen und für Heimat;
Herr Christian Hummel, Bezirk Oberpfalz;
Frau Marie Jungnickl, Stadt Nürnberg;
Frau Gabriele Kamm, Staatsministerium für Unterricht und Kultus:
Frau Doris Kirmeyer, Anstalt für Kommunale Datenverarbeitung in Bayern;
Herr Anton Knoblauch, Staatsministerium des Innern, für Sport und Integration;
Herr Thomas Koeckerbauer, Stadt Regensburg;
Herr Thomas Kraft, Stadt Fürth;
Herr Alexander Lutz, Staatsministerium der Finanzen und für Heimat;
Herr Dr. Marc Maisch, Lehrbeauftragter an der Hochschule für den öffentlichen Dienst in Bayern;
Frau Annette Mattausch, Staatsministerium der Finanzen und für Heimat;
Frau Elisabeth Mayer, Landkreis Regensburg;
Herr Bernd Mikolai, Stadt Ansbach;
Frau Korinna Pöppl, Anstalt für Kommunale Datenverarbeitung in Bayern;
Herr Gabriel Rackl, Staatsministerium des Innern, für Sport und Integration;
Frau Helga Richter, Stadt Würzburg;

Frau Christina Rölz, Staatsministerium des Innern, für Sport und Integration;
Herr Robert Santl, Staatsministerium des Innern, für Sport und Integration;
Herr Jens Schmidt, Landratsamt Nürnberger Land;
Herr Winfried Schober, Bayerischer Gemeindetag;
Herr Roland Schulze, Stadt Kempten;
Herr Alexander Seidl, Hochschule für den öffentlichen Dienst in Bayern;
Herr Maximilian Lino Sindram, Staatsministerium des Innern, für Sport und Integration;
Herr Richard Stelzer, Bayerischer Städtetag;
Herr Dr. Matthias Stief, Landesbeauftragter für den Datenschutz;
Frau Daniela Will, Vorsitzende des ERFA-Kreis Bayern der GDD e.V.;
Herr Michael Will, Staatsministerium des Innern, für Sport und Integration;
Frau Karin Wölfl, Staatsministerium des Innern, für Sport und Integration.