

## 4. Datenschutz-Geschäftsordnung

Die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften trägt nach der DSGVO nicht der behördliche Datenschutzbeauftragte, sondern der „Verantwortliche“ (vgl. hierzu Einführung unter 2.4.1). Die DSGVO weist dem Verantwortlichen eine Reihe neuer datenschutzrechtlicher Pflichten und Aufgaben zu, die im bisherigen Datenschutzrecht noch nicht vorgesehen waren (z.B. Meldung von Datenschutzverletzungen nach Art. 33 DSGVO). 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). 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 öffentlichen Stelle zugewiesen und notwendige Verfahrensabläufe festgelegt werden.

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

Die Dokumentation des Datenschutzkonzepts dient auch der Erfüllung der Rechenschaftspflicht.

Die Mindestaufgaben des behördlichen Datenschutzbeauftragten sind in Art. 39 Abs. 1 DSGVO, Art. 12 und Art. 24 Abs. 5 BayDSG gesetzlich festgelegt. Darüber hinaus können auf den behördlichen Datenschutzbeauftragten einzelne Aufgaben und Pflichten des

Verantwortlichen übertragen werden, sofern dies nicht zu einem Interessenkonflikt bei der Wahrnehmung seiner übrigen Kernaufgaben führt (Art. 38 Abs. 6 DSGVO).

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). Die im nachfolgenden Muster dargestellten Zuständigkeits- und Verfahrensregelungen, die Pflichten des Verantwortlichen nach der DSGVO betreffen, können deshalb auch bei Datenverarbeitungen zum Zwecke der Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten herangezogen werden (Art. 28 Abs. 1 Satz 1, 2 BayDSG). Aus dem 8. Kapitel 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. 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.

## 4.1 Muster einer Datenschutz-Geschäftsordnung

# Datenschutz-Geschäftsordnung<sup>1</sup> der ... (*Behörde*) .... vom....<sup>2</sup>

### Inhaltsverzeichnis:

#### **Erster Teil: Allgemeine Regelungen**

§ 1 Geltungsbereich

#### **Zweiter Teil: Datenschutzrechtliche Zuständigkeiten**

§ 2 Behördenleitung

§ 3 Organisationsfachgebiet

§ 4 IT-Fachgebiet

§ 5 Fachfachgebiete

§ 6 Behördlicher Datenschutzbeauftragter

#### **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 behördlichen Datenschutzbeauftragten

§ 10 Datenschutzbericht

§ 11 Gewährleistung der Richtigkeit und Vollständigkeit des Verzeichnisses

##### **Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen**

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

§ 13 Auftragsverarbeitung

§ 14 Vertrauliche Meldung von Datenschutzverstößen nach Art. 36 BayDSG

---

<sup>1</sup> Im kommunalen Bereich kann sich die Bezeichnung als „Dienstanweisung“ anbieten.

<sup>2</sup> Zur besseren Lesbarkeit der Geschäftsordnung wurde vom Gebrauch von Paarformen (vgl. Nr. 2.4.4.1 Organisationsrichtlinien) Abstand genommen.

## **Fünfter Teil: Schlussvorschriften**

§ 15 Inkrafttreten

3 Anlagen

## **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<sup>3</sup>**

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

(2)<sup>1</sup>Die Behördenleitung benennt einen behördlichen Datenschutzbeauftragten und dessen Vertretung, soweit gesetzlich oder in dieser Geschäftsordnung nichts anderes bestimmt ist. <sup>2</sup>Für die Benennung ist die als Anlage 1 beigefügte Urkunde zu verwenden.

### **§ 3 Organisationssachgebiet<sup>4</sup>**

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

(2) Soweit nichts anderes bestimmt<sup>5</sup> ist, führt das Organisationssachgebiet das Verarbeitungsverzeichnis nach Art. 30 DSGVO.

### **§ 4 IT-Sachgebiet<sup>6</sup>**

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

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

---

<sup>3</sup> Im gemeindlichen Bereich z.B. der erste Bürgermeister / Oberbürgermeister.

<sup>4</sup> Ggf. konkretisieren.

<sup>5</sup> Vgl. § 6 dieser Geschäftsordnung.

<sup>6</sup> Ggf. konkretisieren. Mit „IT-Sachgebiet“ wird die für IT verantwortliche Organisationseinheit bezeichnet.

- b. angemessene und spezifische Maßnahmen zum Schutz besonderer Kategorien personenbezogener Daten nach Art. 8 Abs. 2 BayDSG,
  - c. ggf. geeignete Maßnahmen nach Art. 32 Abs. 2 BayDSG<sup>7</sup>
- fest.

## § 5 Fachsachgebiete<sup>8</sup>

- (1) Die Fachsachgebiete tragen für ihren Zuständigkeitsbereich die Verantwortung für die Beachtung der jeweils maßgeblichen datenschutzrechtlichen Vorschriften.
- (2) Im Benehmen mit dem 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) <sup>1</sup>Die Personalvertretung gilt als Fachsachgebiet. <sup>2</sup>Der besonderen Stellung der Personalvertretung ist Rechnung zu tragen.

## § 6 Behördlicher Datenschutzbeauftragter<sup>9,10</sup>

Ergänzend zu den durch Art. 39 Abs. 1 DSGVO sowie Art. 12 und 24 Abs. 5 BayDSG zugewiesenen Aufgaben nach Anlage 2 werden dem behördlichen Datenschutzbeauftragten die nachfolgenden Aufgaben übertragen<sup>11</sup>:

- 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
- \_\_\_\_\_

<sup>7</sup> Entfällt, soweit die öffentliche Stelle nicht dem Anwendungsbereich des Art. 28 BayDSG 2018 unterliegt.

<sup>8</sup> Ggf. anpassen z.B. „Fachreferat“.

<sup>9</sup> Zur eingeschränkten Zuständigkeit des behördlichen Datenschutzbeauftragten in Gerichten vgl. Art. 37 Abs. 1 Buchstabe a DSGVO.

<sup>10</sup> Zur Gewährleistung der Erreichbarkeit des behördlichen Datenschutzbeauftragten wird empfohlen, ihm ein Funktionspostfach einzurichten z.B. [datenschutzbeauftragter@behoerde.de](mailto:datenschutzbeauftragter@behoerde.de)

<sup>11</sup> Die Übertragung zusätzlicher Aufgaben muss mit der in der DSGVO enthaltenen Rollenbeschreibung des 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) <sup>1</sup>Das Organisationssachgebiet, das IT-Sachgebiet und der behördliche Datenschutzbeauftragte arbeiten zur Gewährleistung des Datenschutzes vertrauensvoll zusammen und informieren sich gegenseitig. <sup>2</sup>Hierzu schaffen sie geeignete Verfahren der kontinuierlichen Zusammenarbeit. <sup>3</sup>Sie unterrichten die Behördenleitung über alle wesentlichen Vorgänge.
- (2) <sup>1</sup>Jeder Beschäftigte meldet seinem jeweiligen Vorgesetzten unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen. <sup>2</sup>Die Fachsachgebiete informieren den behördlichen Datenschutzbeauftragten 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 behördlichen Datenschutzbeauftragten**

- (1) Der behördliche Datenschutzbeauftragte wird frühzeitig in alle wesentlichen Datenschutzfragen eingebunden und vom Organisationssachgebiet, dem IT-Sachgebiet, den Fachsachgebieten und den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.
- (2) Ihm ist vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben.
- (3) <sup>1</sup>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. <sup>2</sup>Ihm ist Gelegenheit zur Stellungnahme zu geben.
- (4) Der behördliche Datenschutzbeauftragte ist im Vorfeld von Vergabeverfahren und neuer Fachverfahren sowie vor der Beschaffung von IT-Hard- und Software zu beteiligen, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden.

## **§ 10 Datenschutzbericht<sup>12</sup>**

<sup>1</sup>Der behördliche Datenschutzbeauftragte erstellt regelmäßig, mindestens alle zwei Jahre, einen Bericht zum Datenschutz. <sup>2</sup>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. <sup>3</sup>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. <sup>4</sup>Die Ergebnisse des Berichts werden mit der Behördenleitung und den zuständigen Organisationseinheiten erörtert und Verbesserungsmöglichkeiten geprüft. <sup>5</sup>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<sup>13</sup> 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) <sup>1</sup>Die für die Führung des Verarbeitungsverzeichnisses zuständige Organisationseinheit<sup>14</sup> übersendet den Fachsachgebieten jährlich eine Liste der von diesen gemeldeten Verarbeitungstätigkeiten. <sup>2</sup>Die Fachsachgebiete prüfen die Liste auf Richtigkeit und Vollständigkeit, aktualisieren sie und leiten sie der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit<sup>15</sup> zu.

## **Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen**

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

- (1) <sup>1</sup>Im Fall einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO informiert die jeweilige Organisationseinheit, der die

---

<sup>12</sup> 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 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.

<sup>13</sup> Ggf. konkretisieren: hierbei kann es sich z.B. um das Organisationssachgebiet (vgl. § 4 Abs. 2) oder bei einer Aufgabenübertragung nach § 6 um den behördlichen Datenschutzbeauftragten handeln.

<sup>14</sup> Siehe Fußnote 13.

<sup>15</sup> Siehe Fußnote 13.

Datenschutzverletzung bekannt geworden ist, unverzüglich den behördlichen Datenschutzbeauftragten hierüber.

- (2) <sup>1</sup>Soweit dem Organisationssachgebiet und dem IT-Sachgebiet der Verstoß noch nicht bekannt ist, unterrichtet der behördliche Datenschutzbeauftragte diese. <sup>2</sup>Er teilt ihnen dabei seine Einschätzung mit, ob eine Meldepflicht nach Art. 33 DSGVO oder eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. <sup>3</sup>Die Einschätzung ist schriftlich zu begründen.
- (3) <sup>1</sup>Die für die Umsetzung der Meldung zuständige Organisationseinheit<sup>16</sup> 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. <sup>2</sup>Ist eine Meldung innerhalb von 72 Stunden nicht möglich, sind die Gründe hierfür zu dokumentieren und die Meldung unverzüglich nachzuholen. <sup>3</sup>Die Meldung unterbleibt, wenn das Organisationssachgebiet und das IT-Sachgebiet unter Berücksichtigung der Einschätzung des behördlichen Datenschutzbeauftragten nach Abs. 2 der Auffassung sind, dass die Voraussetzungen des Art. 33 DSGVO nicht vorliegen. <sup>4</sup>Die Gründe hierfür sind zu dokumentieren. <sup>5</sup>Wenn Daten von oder an den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, sind im Anwendungsbereich der Art. 28 bis 37 BayDSG die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diesen zu melden.
- (4) <sup>1</sup>Das Organisationssachgebiet und das IT-Sachgebiet entscheiden auf der Grundlage der Einschätzung des 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. <sup>2</sup>Die Benachrichtigung der betroffenen Person erfolgt unverzüglich durch die für die Umsetzung der Benachrichtigung zuständige Organisationseinheit<sup>17</sup>. <sup>3</sup>Unterbleibt eine Benachrichtigung nach Art. 34 DSGVO, sind die Gründe hierfür zu dokumentieren.

---

<sup>16</sup> Ggf. konkretisieren: Die Meldung erfolgt z.B. durch den behördlichen Datenschutzbeauftragten, wenn ihm 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.

<sup>17</sup> Ggf. konkretisieren: Die Benachrichtigung erfolgt z.B. durch den behördlichen Datenschutzbeauftragten, wenn ihm 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.

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

### **§ 13 Auftragsverarbeitung**

<sup>1</sup>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. <sup>2</sup>Hierzu lässt sich das Organisationssachgebiet entsprechende Nachweise/Zertifikate vorlegen und holt die Stellungnahme des behördlichen Datenschutzbeauftragten sowie des IT-Sachgebiets ein.

### **§ 14 Vertrauliche Meldung von Datenschutzverstößen nach Art. 36 BayDSG<sup>18</sup>**

<sup>1</sup>Erlangt ein Mitarbeiter von einem Datenschutzverstoß Kenntnis, kann er sich jederzeit unmittelbar an den behördlichen Datenschutzbeauftragten wenden. <sup>2</sup>Der behördliche Datenschutzbeauftragte behandelt die Meldung vertraulich. <sup>3</sup>Er darf Tatsachen, die ihm in Ausübung seiner Funktion anvertraut wurden, und die Identität der mitteilenden Person nicht ohne dessen Einverständnis offenbaren.

### **§ 15 Inkrafttreten**

Diese Geschäftsordnung tritt am 25. Mai 2018 in Kraft.

---

<sup>18</sup> Entfällt, soweit die öffentliche Stelle nicht dem Anwendungsbereich der Art. 28 bis 37 BayDSG 2018 unterliegt.

## **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 mit der EU-Datenschutzreform einhergehenden neuen 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

behördlichen Datenschutzbeauftragten angewiesen, zu dessen Aufgaben u.a. die Unterrichtung und Beratung des Verantwortlichen im Hinblick auf datenschutzrechtliche Regelungen gehört (vgl. Art. 39 Abs. 1 Buchst. a DSGVO). Dem 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 Datenschutzbeauftragten vereinbar ist und auch nicht zu einem Interessenkonflikt bei der Wahrnehmung seiner 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 behördlichen Datenschutzbeauftragten gehört in der Regel zu den Aufgaben der Behördenleitung. Ein Muster für die Bestellungsurkunde 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 organisatorischen Maßnahmen im Benehmen mit dem 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 DSGVO. Bei Datenverarbeitungen im

Anwendungsbereich des Art. 28 BayDSG sind nach Art. 31 BayDSG ergänzende Angaben im Verarbeitungsverzeichnis anzugeben. 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 behördlichen Datenschutzbeauftragten § 6).

#### **Zu § 4 (IT-Sachgebiet)**

Aufgaben des Verantwortlichen im Zusammenhang mit der Gewährleistung der Sicherheit einschließlich der Vertraulichkeit, Verfügbarkeit und Integrität der Daten 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 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 2018. Beabsichtigte Maßnahmen müssen vor ihrem Erlass mit dem Organisationssachgebiet und den jeweils betroffenen Fachsachgebieten bzw. der Behördenleitung abgestimmt werden.

Das nach dem Bayerischen E-Government-Gesetz 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 im 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 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.

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.

### **Zu § 6 (Behördlicher Datenschutzbeauftragter)**

Dem 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 behördlichen Datenschutzbeauftragten nicht auf Verarbeitungen im Rahmen ihrer justiziellen Tätigkeit (Art. 37 Abs. 1 Buchstabe a DSGVO).

Neben den gesetzlich zugewiesenen Aufgaben können auf den behördlichen Datenschutzbeauftragten weitere Aufgaben übertragen werden. Von einer Übertragung ist abzusehen, wenn diese nicht mit der in der DSGVO enthaltenen Rollenbeschreibung des 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 behördlichen Datenschutzbeauftragten 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 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 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 zum Datenschutz etc.

### **Zu § 9 (Beteiligung des behördlichen Datenschutzbeauftragten)**

§ 9 gewährleistet die frühzeitige Einbindung des 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 behördliche Datenschutzbeauftragte hierüber zu informieren und es ist ihm Gelegenheit zur Stellungnahme einzuräumen sowie ggf. die Teilnahme an Besprechungen zu ermöglichen. Vorlagen, die grundsätzliche oder schwierige datenschutzrechtliche Fragestellungen behandeln, sind ihm gleichfalls mit der Gelegenheit zur Stellungnahme zuzuleiten.

In jedem Fall ist dem 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 BayDSG).

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

### **Zu § 10 (Datenschutzbericht)**

Zu den Aufgaben des behördlichen Datenschutzbeauftragten gehört auch die Überwachung der Einhaltung der Vorgaben der DSGVO nach Art. 39 Abs. 1 Buchst. b DSGVO. Der Datenschutzbeauftragte hat zudem 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 technisch-organisatorischen Maßnahmen

erforderlichenfalls zu überprüfen und zu aktualisieren. Durch den in § 10 vorgesehenen Bericht wird den beiden miteinander verschränkten Verpflichtungen des 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 behördlichen Datenschutzbeauftragten nach § 6 übertragen werden. Ein Online-Formular zur Meldung von Datenschutzverletzungen an den Landesbeauftragten für den Datenschutz, das auch eine Übersicht typischer vorkommender Datenschutzverletzungen beinhaltet, findet sich auf der

Homepage des Landesbeauftragten für den Datenschutz unter [https://www.datenschutz-bayern.de/service/data\\_breach.html](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 nach Art. 36 BayDSG)**

§ 14 enthält eine verfahrensrechtliche Bestimmung zur vertraulichen Meldung von Datenschutzverstößen nach Art. 32 BayDSG. Sie ist nur relevant bei Datenverarbeitungen im Anwendungsbereich der Art. 28 bis 37 BayDSG.

## **Fünfter Teil: Schlussvorschriften**

### **Zu § 15 (Inkrafttreten)**

Die Vorschrift legt das Inkrafttreten der Geschäftsordnung auf den Zeitpunkt der unmittelbaren Geltung der DSGVO fest.

#### 4.3 Anlage 1 (zu § 2)

### **Benennung als behördliche Datenschutzbeauftragte/behördlicher Datenschutzbeauftragter**

*(Bezeichnung der öffentlichen Stelle)*

## **Urkunde**

Hiermit benenne ich

Frau/Herrn

*(Amtsbezeichnung)*

*(Vorname)*

*(Name)*

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

alternativ: für die Dauer vom *(Datum)* bis zum *(Datum)*

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 des Unterzeichners)*

#### 4.4 Anlage 2 (zu § 6)

##### Aufgaben des behördlichen Datenschutzbeauftragten

	<b>Die Aufgaben des/der Datenschutzbeauftragten umfassen:</b> <i>(siehe Kennzeichnung)</i>	
	<b>I. Gesetzliche Aufgaben</b>	<b>Rechts- grundlage</b>
	<b>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.</b> 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. <ul style="list-style-type: none"><li>• bei der Erstellung der Verarbeitungsbeschreibungen</li><li>• bei der Einführung neuer automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden sollen oder wesentlichen Änderungen</li><li>• bei Planungen und Entwürfen von Verträgen zur Auftragsverarbeitung</li><li>• hinsichtlich der Pflichten, insbesondere Informations- und Auskunftspflicht, in Bezug auf die Rechte betroffener Personen nach Art 13 ff. DSGVO</li><li>• hinsichtlich Meldungen bei Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) und Benachrichtigungen (Art. 34 DSGVO)</li></ul> 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

	<p>I.2.6. Beratung bei der Erstellung eines IT-Sicherheitskonzeptes der Behörde zu Anforderungen, die sich aus den Bestimmungen zum Schutz personenbezogener Daten ergeben</p>	
	<p><b>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</b></p> <p>Dies umfasst insbesondere:</p> <p>I.2.1. Überwachung der Einhaltung der Datenschutzvorschriften sowie der behördeninternen Vorgaben zum Schutz personenbezogener Daten (Datenschutz-Dienstanweisung)</p> <p>1.2.2. Überwachung und Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei der Ausführung der in den Verarbeitungsbeschreibungen dokumentierten Verarbeitungstätigkeiten</p> <p>I.2.3. Überwachung und Kontrolle der Einhaltung der in den Verarbeitungsbeschreibungen dokumentierten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten und zur Datensicherheit in Zusammenarbeit mit dem Verantwortlichen, der IT-Abteilung und dem IT-Sicherheitsbeauftragten</p> <p>I.2.4. Prüfung und Stellungnahme zur Einhaltung der gesetzlichen Bestimmungen zum Schutz personenbezogener Daten in Verträgen zur Auftragsverarbeitung</p> <ul style="list-style-type: none"> <li>• bei der Umstellung von bestehenden Verträgen auf die neuen gesetzlichen Grundlagen</li> <li>• bei vom Verantwortlichen geplanten Abschluss neuer Verträge zur Auftragsverarbeitung</li> </ul> <p>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</p> <p>1.2.6 Fertigung von Stellungnahmen zu Datenschutzproblemen von Verwaltungsbereichen auf Anfrage oder in Eigeninitiative</p> <p>1.2.7 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</p>	<p>Art. 39 Abs. 1 Buchst. b DSGVO</p>

	<p><b>I.3. Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO</b></p> <p>I.3.1. Beratung auf Anfrage des Verantwortlichen hinsichtlich der Grundlagen und Erfordernisse von Datenschutz-Folgenabschätzungen</p> <p>I.3.2. Überwachung der ordnungsgemäßen Durchführung von Datenschutz-Folgenabschätzungen</p>	<p>Art. 39 Abs. 1 Buchst. c DSGVO</p>
	<p><b>I.4. Zusammenarbeit mit der Aufsichtsbehörde</b></p>	<p>Art. 39 Abs. 1 Buchst. d DSGVO</p>
	<p><b>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</b></p>	<p>Art. 39 Abs. 1 Buchst. e DSGVO</p>
	<p><b>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</b></p>	<p>Art. 38 Abs. 4 DSGVO</p>
	<p>I.6.1. Beratung betroffener Personen - auf Anfrage</p> <p>I.6.2. Weiterleitung von Anfragen, Auskunftersuchen und Beschwerden an den Verantwortlichen und Überwachung der Erledigung/Beantwortung durch ihn</p>	
	<p><b>I.7. Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden.</b></p>	<p>Art. 12 BayDSG</p>
	<p><b>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</b></p>	<p>Art. 24 Abs. 5 BayDSG</p>
	<p><b>I.9. Erstellung von Berichten und Meldungen an die Behördenleitung</b></p> <p>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</p> <p>I.9.2. Erstellung von regelmäßigen Berichten zur Datenschutz-Situation der Behörde an die Behördenleitung, zu den in der Dienstanweisung Datenschutz festgelegten Terminen</p>	<p>Art. 38 Abs. 3 Satz 3 DSGVO</p>

	<b>I.10. Regelmäßige eigene Fortbildung zum Datenschutz</b>	
--	---	--

*Ort, Datum*

*Unterschrift*

*Behördenleiter/in*

#### **4.5 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).