Datenschutz-Geschäftsordnung der Bayerischen Akademie der Wissenschaften

Inhaltsverzeichnis:

[1] Zur besseren Lesbarkeit der Geschäftsordnung wurde vom Gebrauch von Paarformen Abstand genommen. Funktionsbezeichnungen beziehen sich im Folgenden auf alle Geschlechter.

Erster Teil: Allgemeine Regelungen

§ 1 Geltungsbereich

Die Geschäftsordnung gilt für alle Organisationseinheiten (Referate, Projekte, Institute) der Bayerischen Akademie der Wissenschaften.

Zweiter Teil: Datenschutzrechtliche Zuständigkeiten

§ 2 Akademieleitung / Institutsleitung

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

(2) [1]Die Akademieleitung benennt standortübergreifend oder bei Bedarf auch für ein Institut gesondert jeweils einen behördlichen Datenschutzbeauftragten und dessen Vertretung, soweit gesetzlich oder in dieser Geschäftsordnung nichts anderes bestimmt ist. [2]Für die Benennung ist die als Anlage 1 beigefügte Urkunde zu verwenden. Sofern für verschiedene Standorte / Institute jeweils verschiedene Datenschutzbeauftragte bestellt werden, sind diese für ihren jeweiligen Zuständigkeitsbereich ausschließlich verantwortlich.

(3) Die Akademieleitung / Institutsleitung benennt die für den jeweiligen Standort für die Umsetzung der Meldung bzw. Benachrichtigung gem. Art. 33, 34 DSGVO zuständige Organisationseinheit.

§ 3 Ansprechpartner an den Standorten

(1) Jeder Standort der Bayerischen Akademie der Wissenschaften benennt einen oder mehrere Ansprechpartner für den zuständigen Datenschutzbeauftragten.

(2) [1]Die Ansprechpartner erarbeiten zusammen mit dem zuständigen Datenschutzbeauftragten und dem jeweils für die IT-Sicherheit zuständigen Sachgebiet geeignete Datenschutzvorkehrungen nach Art. 24 Abs. 2 DSGVO. [2]Hierzu gehören insbesondere Datenschutz-Richtlinien und fachverfahrensspezifische Anweisungen an die Beschäftigten.

§ 4 IT-Sicherheit

Die am jeweiligen Standort für den Bereich IT-Sicherheit zuständigen Referate bzw. Abteilungen legen in Abstimmung mit dem zuständigen Datenschutzbeauftragten

a. geeignete technische 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,

fest.

Der zuständige Datenschutzbeauftragte wird über die Umsetzung der jeweiligen Maßnahmen informiert.

§ 5 Fachsachgebiete

(1) Die Fachsachgebiete (Referate, Abteilungen, Projekte, Institute) tragen für ihren Zuständigkeitsbereich die Verantwortung für die Beachtung der jeweils maßgeblichen datenschutzrechtlichen Vorschriften.

(2) Im Benehmen mit dem zuständigen 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 in diesem Zusammenhang ebenfalls als Fachsachgebiet. [2]Der besonderen Stellung der Personalvertretung ist Rechnung zu tragen.

§ 6 Behördlicher Datenschutzbeauftragter

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:

☐ 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

☐ Hinwirkung auf geeignete Schulungen der Beschäftigten

Dritter Teil: Zusammenarbeit

§ 7 Zusammenarbeit und gegenseitige Information

(1) [1]Die Ansprechpartner, die für die IT-Sicherheit zuständigen Sachgebiete und der zuständige 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 Akademieleitung / Institutsleitung über alle wesentlichen Vorgänge. [4]Sie arbeiten konstruktiv mit den Verantwortlichen zusammen und unterstützen diese aktiv bei der Findung von datenschutzkonformen Lösungen.

(2) [1]Jeder Beschäftigte meldet seinem jeweiligen Vorgesetzten unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen. [2]Die Fachsachgebiete informieren den zuständigen 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, regelmäßige Schulungen und auf sonstige Art und Weise für den Umgang mit personenbezogenen Daten zu sensibilisieren.

§ 9 Beteiligung des behördlichen Datenschutzbeauftragten

(1) Der zuständige Datenschutzbeauftragte wird frühzeitig in alle wesentlichen Datenschutzfragen eingebunden und von den für die IT-Sicherheit zuständigen Sachgebieten, den Fachsachgebieten und den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

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

(3) [1]Vor dem Einsatz einer Videoüberwachung sind dem zuständigen Datenschutzbeauftragten der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, der betroffene Personenkreis, die Maßnahmen

---

[2] Eine wesentliche Änderung umfasst jede Änderung der in Art 30 Abs. 1 DSGVO benannten erforderlichen Angaben sowie der Rechtsgrundlage, also unter anderem Anzahl, Art und Umfang der personenbezogenen Daten, Lösch- bzw. Speicherfristen, eine Übermittlung an Dritte und vor allem eine Zweckänderung.

nach Art. 24 Abs. 2 BayDSG und die vorgesehenen Auswertungen mitzuteilen. [2]Ihm ist Gelegenheit zur Stellungnahme zu geben.

(4) Der zuständige Datenschutzbeauftragte ist im Vorfeld von Vergabeverfahren und neuer Fachverfahren sowie vor der Beschaffung von IT-Hard- und Software zu beteiligen, Anschaffungen mit möglicher datenschutzrechtlicher Relevanz geplant werden.

§ 10 Datenschutzbericht[3]

[1]Jeder Datenschutzbeauftragte erstellt für seinen Zuständigkeitsbereich regelmäßig, mindestens alle zwei Jahre, einen Bericht zum Datenschutz. [2]In diesem sind die in der Akademie 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 Akademieleitung 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 dem zuständigen Datenschutzbeauftragten unaufgefordert die neu aufgenommenen Verarbeitungstätigkeiten sowie wesentliche Änderungen[4] bereits gemeldeter Verarbeitungstätigkeiten.

---

[3] 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.

[4] s.o., Fußnote 2

(2) [1]Für diese Meldung ist das als Anlage 3 beigefügte Formblatt zu verwenden. Alternativ darf nach vorheriger Rücksprache mit dem zuständigen Datenschutzbeauftragten ein anderes Format sowie ein anderes Mitteilungsverfahren zur Anwendung kommen.[2]Jeder Datenschutzbeauftragte übersendet den Fachsachgebieten in seinem Zuständigkeitsbereich jährlich eine Liste der von diesen gemeldeten Verarbeitungstätigkeiten. [2]Die Fachsachgebiete prüfen die Liste auf Richtigkeit und Vollständigkeit, aktualisieren sie und leiten sie dem zuständigen Datenschutzbeauftragten wieder zurück.

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 zuständigen Datenschutzbeauftragten hierüber.

(2) [1]Soweit der Akademieleitung / Institutsleitung und dem für die IT-Sicherheit zuständigen Sachgebiet der Verstoß noch nicht bekannt ist, unterrichtet der zuständige Datenschutzbeauftragte diese. [2]Er teilt ihnen dabei seine Einschätzung mit, ob eine Meldepflicht nach Art. 33 DSGVO oder eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. [3]Die Einschätzung ist schriftlich zu dokumentieren.

(3) [1]Die für die Umsetzung der Meldung zuständige Organisationseinheit[16] meldet im Einvernehmen mit der Akademieleitung / Institutsleitung und dem jeweils für die IT-Sicherheit zuständigen 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 die Akademieleitung / Institutsleitung und das jeweils für die IT-Sicherheit zuständige Sachgebiet unter Berücksichtigung der Einschätzung des zuständigen Datenschutzbeauftragten nach Abs. 2 der Auffassung sind, dass die Voraussetzungen des Art. 33 DSGVO nicht vorliegen. [4]Die Gründe hierfür sind zu dokumentieren. [5]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) [1]Die Akademieleitung / Institutsleitung und das jeweils für die IT-Sicherheit zuständige Sachgebiet entscheiden auf der Grundlage der Einschätzung des zuständigen 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 die Akademieleitung / Institutsleitung und das jeweils für die IT-Sicherheit zuständige Sachgebiet in Abstimmung mit dem zuständigen Datenschutzbeauftragten unverzüglich Abhilfemaßnahmen ein.

§ 13 Auftragsverarbeitung

[1]Vor Abschluss eines Vertrages über die Auftragsverarbeitung wird geprüft, ob der Auftragsverarbeiter hinreichende 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 die Akademie entsprechende Nachweise/Zertifikate vorlegen und holt die Stellungnahme des zuständigen Datenschutzbeauftragten, der für die IT-Sicherheit zuständigen Sachgebiete sowie des Justitiars ein.

§ 14 Inkrafttreten

Diese Geschäftsordnung tritt mit ihrer Unterzeichnung in Kraft.

München, den 25.7.2019

Prof. Dr. Thomas O. Höllmann
Präsident der Bayerischen Akademie der Wissenschaften

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)

Anlage 2 (zu § 6)

Aufgaben des 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. • bei der Erstellung der Verarbeitungsbeschreibungen • bei der Einführung neuer automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden sollen oder wesentlichen Änderungen • bei Planungen und Entwürfen von Verträgen zur Auftragsverarbeitung • hinsichtlich der Pflichten, insbesondere Informations- und Auskunftspflicht, in Bezug auf die Rechte betroffener Personen nach Art 13 ff. DSGVO • 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.2.6. Beratung bei der Erstellung eines IT-Sicherheitskonzeptes der Behörde zu Anforderungen, die sich aus den Bestimmungen zum Schutz personenbezogener Daten ergeben I.2.7. konstruktive Zusammenarbeit und aktive Unterstützung der Verantwortlichen bei der Findung von datenschutzkonformen Lösungen	
	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) 1.2.2. Überwachung und Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei der Ausführung der in den Verarbeitungsbeschreibungen dokumentierten Verarbeitungstätigkeiten 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 I.2.4. Prüfung und Stellungnahme zur Einhaltung der gesetzlichen Bestimmungen zum Schutz personenbezogener Daten in Verträgen zur Auftragsverarbeitung • bei der Umstellung von bestehenden Verträgen auf die neuen gesetzlichen Grundlagen • 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 1.2.6 Fertigung von Stellungnahmen zu Datenschutzproblemen von Verwaltungsbereichen auf Anfrage oder in Eigeninitiative 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	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	Art. 38 Abs. 4 DSGVO
	I.6.1. Beratung betroffener Personen - auf Anfrage I.6.2. Weiterleitung von Anfragen, Auskunftsersuchen und Beschwerden an den Verantwortlichen und Überwachung der Erledigung/Beantwortung durch ihn	
	I.7. Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden.	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 I.9.2. Erstellung von regelmäßigen Berichten zur Datenschutz-Situation der Behörde an die Behördenleitung, zu den in der Dienstanweisung Datenschutz festgelegten Terminen	Art. 38 Abs. 3 Satz 3 DSGVO

	I.10. Regelmäßige eigene Fortbildung zum Datenschutz	

Anlage 3 (zu § 11)

Beschreibung einer Verarbeitungstätigkeit

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)		
Behördlicher Datenschutzbeauftragter (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)		

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke
Rechtsgrundlagen

3. Kategorien der personenbezogenen Daten

Nr.	**Bezeichnung der Daten**

4. Kategorien der betroffenen Personen

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

Nr.	**Empfänger**	**Anlass der Offenlegung**

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

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

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

9. Verantwortliche Organisationseinheit

Dienststelle / Sachgebiet / Abteilung

10. 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

11. Stellungnahme des behördlichen Datenschutzbeauftragten

Liegt eine Stellungnahme des behördlichen Datenschutzbeauftragten vor?

☐ Ja ☐ Nein

Ggf. nähere Erläuterung

Erläuterungen

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 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:

- Führung des Melderegisters
- Führung des Gewerberegisters
- Personalaktenverwaltung
- Beihilfebearbeitung
- Wohngeldbearbeitung
- Bearbeitung von Bauanträgen
- 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 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 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 (Richtlinie (EU) 2016/680, vgl. Art. 28 Abs. 1 BayDSG) ist die Angabe der Rechtsgrundlagen demgegenüber verpflichtend (Art. 31 BayDSG). Soweit keine bereichsspezifische gesetzliche Regelung (wie etwa auch Art. 4 Abs. 1 BayDSG) besteht, kommen als Rechtsgrundlagen die Tatbestände nach Art. 6 – bei besonderen Kategorien personenbezogener Daten in Verbindung mit Art. 9 DSGVO und Art. 8 BayDSG - in Betracht.

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, denen die Daten weitergegeben werden oder die 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. 49 Abs. 1 Unterabsatz 2 DSGVO sind die geeigneten Garantien in Bezug auf den Schutz personenbezogener Daten in Spalte 3 festzuhalten. Soweit erforderlich kann dazu auf ergänzende Dokumente verwiesen werden.

Zu Nr. 7 (Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien)

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 erforderlich sein.

Anzugeben ist auch der Beginn der Löschungsfrist. Vor einer Löschung von Daten sind die archivrechtlichen Anbietungspflichten zu beachten.

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. Art. 11 Abs. 1 Satz 2 Bayerisches E-Government-Gesetz).

Zu Nr. 9 (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. 10 (Datenschutz-Folgenabschätzung)

Die Angabe, ob eine Datenschutz-Folgenabschätzung für die Verarbeitungstätigkeit durchzuführen ist, geht über die 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 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. Die Datenschutz-Folgenabschätzung ist „vorab", d.h. vor dem Einsatz einer Verarbeitung

durchzuführen. Für bereits laufende Verarbeitungen, die ohne wesentliche Änderungen fortgeführt werden und die eine Datenschutz-Folgenabschätzung erfordern, ist diese in einer Übergangsfrist spätestens bis zum 25. Mai 2021 nachzuholen.

Nr. 8 dieser Arbeitshilfe enthält weitere Hinweise zu den Voraussetzungen und der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.

Zu Nr. 11 (Stellungnahme des behördlichen Datenschutzbeauftragten)

Dem 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 behördlichen Datenschutzbeauftragten ist nach Art. 24 Abs. 5 BayDSG auch vor dem Einsatz einer Videoüberwachung einzuholen.