

Beschreibung einer Verarbeitungstätigkeit

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	Aktenzeichen	Stand
WebApp TaskCards		05/2022
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	
Bestandteil des digitalen Bildungsangebotes.	
Bereitstellung eines Lehrmittels für den digitalen Unterricht.	
Die TaskCards Pinnwand ist ein digitales Werkzeug zum Gestalten und Abspeichern von interaktiven, online und offline verfügbaren Posts. Diese können autorisierten Nutzer, sowie Gästen mit Zugangstoken selbst gestalten, indem sie die TaskCards Pinnwand mit Hilfe von Stiftwerkzeugen, Texteingaben, Formwerkzeugen und dem Bereitstellen multimedialer Inhalte füllen. Jeder in TaskCards eingeloggte Nutzer kann die so erstellte Datei in seinem eigenen Bereich „Meine Pinnwände“ auch innerhalb TaskCards abspeichern.	
TaskCards ist universell einsetzbar für jede Art von Bildungseinrichtung (Schulen, Kindergärten, Universitäten, usw.).	
Rechtsgrundlagen	
Spezialgesetzliche Regelung außerhalb der DSGVO	GOBD, 10 Jahre Aufbewahrungsfrist für Zahlungsdokument
Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DSGVO:	<input checked="" type="checkbox"/>
Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§26 BDSG)	<input checked="" type="checkbox"/>
Vertrag oder Vertragsanbahnung mit dem Anbieter / Betroffenen (Art. 6 Abs. 1 b) DSGVO	<input checked="" type="checkbox"/>
Berechtigte Interessen (Art. 6 Abs. 1 f) DSGVO	<input checked="" type="checkbox"/> Strafverfolgung bei Missbrauch der Plattform

3. Kategorien der personenbezogenen Daten

Nr.	Bezeichnung der Daten
1	Name, Vorname
2	Benutzername
2	Kontaktdaten (Telefon, E-Mail)
3	Onlinedaten (IP-Adresse, Zeit, Browser)

4. Kategorien der betroffenen Personen

Nr.	Betroffene Personen
1	Beschäftigte
2	Lehrer*innen
3	Lizenznehmer
4	SuS

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
1	OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken	Hosting
2	billwerk GmbH, Mainzer Landstraße 51, 60329 Frankfurt/Main	Zahlungsabwicklung von Lizenzen

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

Es findet kein Drittlandtransfer statt. Die Datenverarbeitung erfolgt ausschließlich im EWR.

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.	Datensatz zu	Löschungsfrist
1	Accountlöschung	Zum Vertragsende
2	Pinnwandlöschung	7 Tage
3	Lizenz- rechnungsdaten	10 Jahre
4	Organisationsinstanzen	Zum Vertragsende
5	Lizenznehmer	3 Jahre

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

- Hinsichtlich der allgemeinen Sicherheit wird auf vorhandene TOM/Sicherheitskonzept des Anbieters dSign Systems GmbH verwiesen
- Zu **zusätzlichen** Maßnahmen wird auf das spezifizierte TOM / Sicherheitskonzept des Anbieters dSign Systems GmbH verwiesen

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 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 Verzeichnisse.

Das Verzeichnisse soll einerseits alle Verarbeitungstätigkeiten ausreichend konkret darstellen, andererseits nicht zu kleinteilig sein. Der Begriff der „Verarbeitungstätigkeit“ umfasst alle Verarbeitungsschritte, Vorgänge und Vorgangsserien, die einem gemeinsamen Zweck dienen. Es ist daher nicht zu jedem einzelnen Verarbeitungsschritt bzw. Vorgang oder zu einer Vorgangsserie 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. (Nur für Verarbeitungen durch Polizei- und Strafjustizbehörden)

(Art. 31 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 Abs. 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. 47 PAG bzw. zukünftig nach Art. 64 Abs. 1 PAG-E 2018 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 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. Für Polizeibehörden richtet sich die Datenschutz-Folgenabschätzung nach Art. 64 Abs. 2 PAG-E 2018.

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. 12 (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.