Beschreibung von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	**Stand:**
Plattform für sichere Kommunikation in Bayern	09.07.2018

Ist die Verarbeitungstätigkeit nach Art. 26 BayDSG datenschutzrechtlich freigegeben oder wurde bereits eine Errichtungsanordnung nach Art. 47 PAG erteilt?

☐ Nein ☒ Ja, am 25.07.2014, AZ: IA7-1084

Angaben zum Verantwortlichen (Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer der Behörde)

Datenschutzbeauftragter Schulstr. 5 84186 Vilsheim datenschutz@vilsheim.de 08706 / 9485 - 0

Falls zutreffend: Angaben zu gemeinsam für die Verarbeitung Verantwortlichen (Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)

Name und Kontaktdaten des behördlichen Datenschutzbeauftragten (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)

Datenschutzbeauftragter Schulstr. 5 84186 Vilsheim datenschutz@vilsheim.de 08706 / 9485 - 0

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke

Die Umsetzung der EG-Dienstleistungsrichtlinie (Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt - DLR) und der EG-Berufsanerkennungsrichtlinie (Richtlinie 2013/55/EG des Europäischen Parlaments und des Rates vom 28.12.2013 über die Anerkennung von Berufsqualifikationen - BQRL) verlangt die Sicherstellung der elektronischen Verfahrensabwicklung für alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen bzw. die zur Anerkennung ausländischer Berufsqualifikationen erforderlich sind. Nach Art. 8 Abs. 1 DLR und Art. 58 BQRL haben die Mitgliedstaaten sicherzustellen, dass alle Verfahren und Formalitäten problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abgewickelt werden können.

Diesen Vorgaben trägt die in Ergänzung zum bestehenden Informationsportal „Dienstleistungsportal Bayern“ (www.eap.bayern.de) entwickelte Plattform für sichere Kommunikation in Bayern (Erreichbarkeitsplattform – EPF) Rechnung. Sie ermöglicht Bürgern und Unternehmern aus dem In- und Ausland eine kostenlose verschlüsselte elektronische Kommunikation mit den angeschlossenen öffentlichen Stellen in Bayern (insbesondere Behörden und Kammern sowie Einheitliche Ansprechpartner).

Die Plattform ist an das Dienstleistungsportal Bayern angebunden. Für die sichere elektronische Kommunikation muss der Bürger / Unternehmer das Dienstleistungsportal Bayern aufrufen und dort sein Vorhaben oder die öffentliche Stelle, die er kontaktieren möchte, auswählen. Er wird anschließend automatisch zum Authentifizierungsdienst „authega“ weitergeleitet. Im Rahmen der Registrierung wird ein Brief mit einem Aktivierungs-Code und eine E-Mail mit einer Aktivierungs-PIN an den Bürger / Unternehmer gesendet. Nach Abschluss der Registrierung wird ein Benutzerkonto und je Vorhaben oder öffentliche Stelle ein sog. Fallpostfach angelegt.

Die Nutzung der Plattform ist kostenfrei und erfolgt auf freiwilliger Basis. Die Kommunikation kann nur vom Bürger / Unternehmer angestoßen werden (z. B. durch Versand eines Antrages oder formlosen Schreibens an die zuständige Stelle oder den Einheitlichen Ansprechpartner). Der Bürger / Unternehmer kann Dokumente https-verschlüsselt in die Plattform zum Versand hochladen. Vor der Speicherung der Dokumente in der Plattform erfolgt eine systemseitige Virenprüfung. Die Verschlüsselung der Nachrichten, die Bürger / Unternehmer an öffentliche Stellen versenden, erfolgt automatisch durch die Plattform. Nachrichten und Dokumente werden auf der Plattform verschlüsselt abgelegt. Antragsteller können über die Plattform verschlüsselte Nachrichten oder Anträge nur an öffentliche Stellen, die sich an die Plattform angeschlossen haben, senden. Dazu muss mindestens das zentrale E-Mail-Postfach der öffentlichen Stelle mit einem Verschlüsselungs- und Signaturzertifikat der Bayerischen Verwaltungs-PKI ausgestattet sein. Nach Erhalt einer Nachricht von der Plattform entscheidet die öffentliche Stelle, ob sie eine verschlüsselte E-Mail-Nachricht an das Fallpostfach des Antragstellers auf der Plattform zurücksendet oder einen anderen Kommunikationsweg (z. B. Papier, Fax) wählt. Wenn eine Nachricht an das Fallpostfach gesendet wird,

wird der Bürger / Unternehmern über den Eingang der Nachricht per E-Mail benachrichtigt. Er muss sich auf der Plattform über den Authentifizierungsdienst „authega“ anmelden, um die Nachricht zu lesen und ggf. lokal zu speichern.

An die Plattform können die folgenden Stellen angeschlossen werden:

- Behörden und sonstige öffentliche Stellen des Freistaates Bayern
- Gemeinden und Gemeindeverbände in Bayern
- sonstige der Aufsicht des Freistaats Bayern unterstehende juristische Personen des öffentlichen Rechts wie z. B. Kammern
- ggf. Bundesbehörden und sonstige Institutionen (z. B. Verbände)

Rechtsgrundlagen

- Art. 6 Abs. 1 lit e Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Art. 4 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG)
- Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt – DLR
- Richtlinie 2013/55/EG des Europäischen Parlaments und des Rates vom 28.12.2013 über die Anerkennung von Berufsqualifikationen - BQRL

3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten
1	Stammdaten von Bürgern und Unternehmern • E-Mail-Adresse • Titel (optional) • Anrede • Vorname • Nachname • Firma (optional) • Straße / Hausnummer • Postleitzahl • Ort • Adresszusatz 1 (optional) • Adresszusatz 2 (optional) • Land • Benutzername • Passwort
2	Falldaten von Bürgern und Unternehmern • Telefon (optional) • Telefax (optional) • hochgeladene Dokumente (können personenbezogene Daten enthalten) • versandte Nachrichten mit Anhängen (enthalten personenbezogene Daten) • empfangene Nachrichten mit Anhängen (können personenbezogene Daten enthalten)

4. Kategorien der betroffenen Personen

Lfd. Nr.	Betroffene Personen
1	Bürger
2	Unternehmer

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

Lfd. Nr.	Empfänger	Anlass der Offenlegung
1	Firma ReadSpeaker (Vorlesesoftware)	Umwandlung der personenbezogen Daten in Audio-Dateien

2	Öffentliche Stellen	Bürger / Unternehmer sendet seine personenbezogenen Daten zusammen mit seiner Nachricht an die öffentlichen Stellen
3	Staatlicher IT-Dienstleister über dessen Server die Registrierung / Authentifizierung erfolgt	Technische Administratoren haben Zugriff auf die gespeicherten Daten
4	Staatlicher IT-Dienstleister auf dessen Servern die Fallpostfächer vorgehalten werden	Technische Administratoren haben Zugriff auf die gespeicherten Daten

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

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

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr.	Löschungsfrist
1	Stammdaten von Bürgern und Unternehmern: Der Nutzer kann sein Benutzerkonto jederzeit löschen. Damit werden sämtliche Daten von ihm, einschließlich der Registrierungsinformationen, auf der Plattform gelöscht. Eine automatische Löschung des Benutzerkontos erfolgt nach Ablauf von drei Jahren nach letztmaliger Anmeldung des Nutzers. Über eine beabsichtigte Löschung wird der Nutzer im Vorfeld per E-Mail informiert (erste Erinnerungs-E-Mail zwei Monate vor dem Löschtermin, zweite Erinnerungs-E-Mail ein Monat vor dem Löschtermin). Damit das Benutzerkonto nicht automatisch gelöscht wird, reicht es aus, dass sich der Nutzer vor dem Löschtermin erneut auf der Plattform anmeldet.
2	Falldaten von Bürgern und Unternehmern: Der Nutzer kann jederzeit einzelne Dokumente, Nachrichten und Fallpostfächer aktiv löschen. Nach sechs Monaten der Inaktivität erfolgt eine automatische Löschung des Fallpostfachs. Der Nutzer wird im Vorfeld per E-Mail darauf aufmerksam gemacht (erste Erinnerungs-E-Mail vier Wochen vor dem Löschtermin, zweite Erinnerungs-E-Mail eine Woche vor dem Löschtermin). Werden Dokumente oder Nachrichten in der Plattform gelöscht, werden sie in den Papierkorb verschoben. Inhalte des Papierkorbs, die älter als 14 Tage sind, werden automatisch gelöscht.

8. Nur für Verarbeitungen nach Art. 28 Abs. 1 BayDSG 2018: Profiling

Erfolgt ein Profiling im Sinne von Art. 3 Nr. 4 der Datenschutzrichtlinie für die Strafverfolgung (Richtlinie (EU) 2016/680)?
☐ Ja ☒ Nein
Falls ja: Welche Art von Profiling wird durchgeführt?

9. 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 2018

Die Datenhaltung erfolgt in einem staatlichen Rechenzentrum (IT-Dienstleistungszentrum des Freistaats Bayern). Es gelten damit die allgemeinen technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung des IT-Dienstleistungszentrums des Freistaats Bayern.

Jeder Bürger und Unternehmer hat Zugriff auf die auf der Plattform über ihn gespeicherten personenbezogenen Daten. Die Anmeldung auf der Plattform erfolgt über Benutzername und Passwort. Die Seite ist https-geschützt. Für angeschlossene Stellen ist kein direkter Zugriff möglich.

Ein inhaltlicher Zugriff auf die Stammdaten und die Falldaten durch das IT-Dienstleistungszentrum des Freistaats Bayern ist nur bei technischen Störungen zulässig. Die erforderlichen Zugriffe werden vom IT-Dienstleistungszentrum des Freistaats Bayern protokolliert.

Die Stamm- und Falldaten sind in der Datenbank verschlüsselt gespeichert.

10. Datenschutz-Folgenabschätzung

Ist für das Verfahren eine Datenschutz-Folgenabschätzung durchzuführen? ☐ Ja ☒ Nein
Begründung

11. Stellungnahme des behördlichen Datenschutzbeauftragten

Das Verfahren ist datenschutzrechtlich zulässig ☐ Ja ☐ Nein
Ggf. nähere Erläuterung