Landesamt für Digitalisierung,
Breitband und Vermessung

Landesamt für Digitalisierung, Breitband und Vermessung

per E-Mail
Herrn Präsident
Wolfgang Bauer o.V.i.A.
Landesamt für Digitalisierung, Breitband und Vermessung
Alexandrastraße 4
80538 München

nachrichtlich an:
Herrn Martin Stegmeier
Direktor des IT-Dienstleistungszentrum des Freistaats Bayern im Landesamt für Digitalisierung, Breitband und Vermessung

Name
Christine Schmid

Telefon
089 / 2119 - 2449

Telefax
089 / 2119 - 12449

E-Mail
it-dlz.Datenschutz@ldbv.bayern.de

Ihr Zeichen, Ihre Nachricht vom	Bitte bei Antwort angeben Unser Zeichen, Unsere Nachricht vom	Datum
	IT 1 – 0 1990 –1/2019	21.02.2019

Stellungnahme zum Betrieb der Datenaustauschplattform „BayernBox“ für kommunale öffentliche Stellen gemäß Art. 12 Absatz 1 Nr. 2 Bayerisches Datenschutzgesetz (BayDSG) i.V.m. Art. 39 Abs. 2 Buchstabe b) Datenschutzgrundverordnung (DSGVO)

Anlage
Beschreibung der Verarbeitungstätigkeit für Bereitstellung und Betrieb der Datenaustauschplattform BayernBox

Sehr geehrter Herr Präsident,

der für den Betrieb der Datenaustauschplattform BayernBox zuständige Referatsleiter hat mir den Vorgang zur Stellungnahme nach Art. 12 Abs.1 Nr.2 BayDSG übersandt.

Hierzu liegen mir folgende Unterlagen vor:

a) Benutzerhandbuch BayernBox
b) Nutzungsbedingungen BayernBox
c) Muster für Datenschutzerklärung und Impressum zur Bereitstellung für kommunale öffentliche Stellen

d) Beschreibung der Verarbeitungstätigkeit nach Art. 30 Abs. 1 DSGVO

Darüber hinaus begleitete ich das Projekt „BayernBox“ beratend zu den unterschiedlichsten datenschutzrechtlichen Fragestellungen. Hierzu sichtete ich unter anderem Dokumentationen des Softwareherstellers, der Firma ownCloud, und nahm an einer Produktbesprechung mit dem Hersteller teil.

Bereits im Vorgängerprojekt Datenaustauschplattforn „ownCloud“ für staatliche öffentliche Stellen war ich eng eingebunden und wirkte koordinierend an den Dokumentationen für die damalige landesweite datenschutzrechtliche Freigabe durch das Staatsministerium der Finanzen, für Landesentwicklung und Heimat vom 10.02.2017 (Rechtsstand bis 24.05.2018) mit.

Im Zuge des Aufbaus der Austauschplattform BayernBox mit dem Produkt „ownCloud“ wurden die Anforderungen der Aufsichtsbehörde (Bayerischer Landesbeauftragter für den Datenschutz) aus der datenschutzrechtlichen Freigabe für ownCloud vom 10.02.2017 hinsichtlich einer technischen Implementierung der Passwortrichtlinie und einer Funktion zur datenschutzrechtlichen Kontrollmöglichkeit (sog. Eingabekontrolle) für die jeweilige öffentliche Stelle umgesetzt.

Die Datenaustauschpattform „BayernBox“ wird vom IT-DLZ für kommunale öffentliche Stellen im Rahmen des Masterplans BAYERN DIGITAL II der Bayerischen Staatsregierung bereitgestellt. Hierbei wurde der Funktionsumfang der Plattform zwischen den kommunalen Spitzenverbänden und dem Bayerischen Staatsministerium der Finanzen und für Heimat abgestimmt.

Als behördliche Beauftragte für den Datenschutz des IT-Dienstleistungszentrum des Freistaats Bayern im Landesamt für Digitalisierung, Breitband und Vermessung nehme ich zur beabsichtigten Verarbeitungstätigkeit gemäß Art. 12 Abs. 1 Nr. 2 BayDSG wie folgt zusammenfassend Stellung:

1. Aktuell bestehen keine datenschutzrechtlichen Einwände für die Bereitstellung und den Betrieb der Datenaustauschplattform BayernBox für Datenkategorien mit Klassifizierung „normaler Schutzbedarf“.

2. Sollten kommunale Stellen nach Durchführung einer eigenen datenschutzrechtlichen Risikoanalyse (dem Risiko angemessener Schutzbedarf) und/oder beim Austausch insbesondere von Datenkategorien gemäß Art. 9 DSGVO, Art. 8 Abs. 1 BayDSG, Kommentar Wilde, Ehmann, Niese, Knoblauch zu Art. 8 BayDSG erhöhten Schutzbedarf verifizieren, wird empfohlen, selbst für den Schutz dieser Daten durch geeignete technisch-organisatorische Maßnahmen (wie etwa eine verschlüsselte Upload- bzw. Ablagemöglichkeit) Sorge zu tragen.
3. Für weiterführende Informationen bzw. Empfehlungen zum Gebrauch der BayernBox möchte ich auf die Beschreibung der Verarbeitungstätigkeit des IT-DLZ Bayern nach Art. 30. Abs. 1 DSGVO, das Benutzerhandbuch der BayernBox und die Nutzungsbedingungen der BayernBox aufmerksam machen.

Hinweis:
Sollten sich für Bereitstellung und Betrieb der Datenaustauschplattform BayernBox wesentliche Änderungen in technischer und/oder organisatorischer Hinsicht ergeben, ist mir der Vorgang mit der angepassten Beschreibung der Verarbeitungstätigkeit vor Produktivsetzung vom zuständigen Fachreferat erneut zur Stellungnahme vorzulegen, Art. 12 Abs. 1 Nr. 2 BayDSG i.V.m. Art. 39 Abs. 2 Buchstabe b) DSGVO.

Mit freundlichen Grüßen

gez. Christine Schmid
Beauftragte für den Datenschutz des IT-Dienstleistungszentrum des Freistaats Bayern im Landesamt für Digitalisierung, Breitband und Vermessung

Beschreibung einer Verarbeitungstätigkeit nach Art. 30 Abs. 1 Datenschutz-Grundverordnung (DSGVO)

1. a) Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	**Aktenzeichen**	**Stand**
Bereitstellung und Betrieb der Datenaustauschplattform „BayernBox“	IT1-01990-1/2019	02.01.2019

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

Landesamt für Digitalisierung. Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern, St.-Martin-Straße 47, 81541 München, poststelle@ldbv.bayern.de, 089 / 2119-0

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

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

Behördliche Beauftragte für den Datenschutz des IT-Dienstleistungszentrums des Freistaats Bayern,
Landesamt für Digitalisierung. Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern, St.-Martin-Straße 47, 81541 München, it-dlz.datenschutz@ldbv.bayern.de, 089 / 2119 -0

1 b) Verantwortliche Organisationseinheit

Dienststelle / Abteilung / Referat

Landesamt für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern, Abteilung IT2 , Referat IT 24

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke

1. Zentrale Bereitstellung und Betrieb einer Datenaustauschplattform für kommunale öffentliche Stellen

2. Datenaustausch mit öffentlichen bzw. nichtöffentlichen Stellen

Rechtsgrundlagen IT-DLZ Bayern als staatliches Rechenzentrum

- Auftragserteilung durch kommunale Gebietskörperschaften bzw. Verwaltungsmeinschaften des Freistaats Bayern i.V. mit Art. 28 DSGVO
- Art. 4 Abs. 1 BayDSG i.V. mit Art. 6 Abs. 1 UAbs. 1 Buchstabe e) i.V.m. Abs. 2, 3 DSGVO
- Art. 8 Abs. 2 BayEGovG (Basisdienst)
- Art. 12 Abs. 3 Satz 2 VermKatG
- Ministerratsbeschluss vom 30.05.2017 (Masterplan BAYERN DIGITAL II)

Erläuterung

Die nachfolgende „Beschreibung der Verarbeitungstätigkeit“ dient dem Landesamt für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern zur Dokumentation seiner Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO.

Die „BayernBox“ bietet die Plattform für einen sicheren Datenaustausch.

Dementsprechend befasst sich diese Beschreibung der Verarbeitungstätigkeit primär mit der Bereitstellung und dem Betrieb der *Datenaustauschplattform.*

Eine Aussage oder Freigabe hinsichtlich der im Einzelfall über die oder in der BayernBox verarbeiteten personenbezogenen Daten bzw. der dahinterstehenden Verarbeitungstätigkeit/Verfahren erfolgt hiermit explizit nicht.

Für die Einhaltung der Vorschriften der Datenschutzgrundverordnung (DSGVO) bzw. des Bayerischen Datenschutz-

gesetzes (BayDSG) oder anderer Vorschriften über den Datenschutz bei der Nutzung der Plattform sind die einsetzenden Stellen als Verantwortliche selbst zuständig. Dies gilt ebenso für eine ggf. durchzuführende Risikoanalyse, der Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO sowie der Prüfung, ob eine Datenschutzfolgenabschätzung durchzuführen ist.

Kommunale Gebietskörperschaften, die einen Datenaustausch mit der BayernBox durchführen, können sich diese Beschreibung jedoch, ggf. angepasst, zu Eigen machen und sie für ihre Zwecke in ihr „Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO übernehmen.

Zusätzliche Erläuterungen:

Zur Erfüllung ihrer Aufgaben ist für öffentliche Stellen häufig auch ein Datenaustausch mit anderen öffentlichen (ggf. auch nichtöffentlichen) Stellen erforderlich. Insbesondere bei großen Datenmengen ist dieser Austausch für öffentliche Stellen oft nicht oder nicht angemessen möglich. Mit Hilfe der BayernBox, basierend auf dem Softwareprodukt „ownCloud“, soll der automatisierte Austausch von Daten (Hochladen/Herunterladen) zwischen beteiligten Stellen vereinfacht und vor allem ausreichend sicher ermöglicht werden.

Basisdienst:

Das Bayerische Staatsministerium der Finanzen und für Heimat hat das IT-Dienstleistungszentrum des Freistaats Bayern im Landesamt für Digitalisierung. Breitband und Vermessung mit dem zentralen Betrieb der Plattform „BayernBox“ für kommunale Gebietskörperschaften beauftragt.

Die BayernBox stellt insoweit eine elektronische Verwaltungsinfrastruktur zur behörden- bzw. betriebsübergreifenden Nutzung im Sinne eines Basisdienst nach Art. 8 Abs. 2 des Gesetzes über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG) dar.

Weitere Hinweise:

Siehe Nutzungsbedingungen des IT-Dienstleistungszentrum des Freistaats Bayern

3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten
1. 1.1 1.2 1.3	Zugangsdaten zur BayernBox Instanz Benutzerkennung Passwort (verschlüsselt als Hashwert) Gültige E-Mail-Adresse
2. 2.1 2.2	Benachrichtigung über BayernBox Instanz Dateifreigaben via E-Mail Link Passwortschutz (verschlüsselt als Hashwert) Ablaufdatum der Freigabe
3. 3.1	*Inhaltsdaten der BayernBox Instanz Abhängig von der BayernBox Instanz der verantwortlichen Stelle: Die verantwortlichen (speichernden) Stellen haben vor der Nutzung der BayernBox Instanz festzulegen, ob die Daten verschlüsselt in die BayernBox Instanz eingestellt werden müssen; siehe auch Abschnitt 8 I. Nr. 3.3.4. *abstrakt
4. 4.1 4.2 4.3 4.4 4.5 4.6	Logdateien – BayernBox Instanz Datum und Uhrzeit der Verbindung Quelle IP-Adresse 1. aus dem Behördennetz kommend (IP-Adresse der Web-Proxies IT-DLZ) 2. von extern kommend (IP-Adresse des Providers des Benutzers) Benutzername Anmeldeinformation (Login failed/fehlgeschlagen)
5. 5.1 5.2	Logdateien – Apache Webserver Datum und Uhrzeit der Verbindung Quelle IP-Adresse 1. aus dem Behördennetz kommend (IP-Adresse der Web-Proxies IT-DLZ)

Lfd. Nr.	Bezeichnung der Daten
	2. von extern kommend (IP-Adresse des Providers des Benutzers)
5.3	Ziel IP-Adresse (BayernBox Server)
5.4	Name der BayernBox Instanz
5.5	Benutzername
5.6	Datenumfang der Verbindung (Bytes to Client)
5.7	Zugriffsmethode auf BayernBox Instanz (GET, PUT, POST)
5.8	Dateiname
5.9	Typ des verwendeten Browsers (User Agent)
6.	Eingabekontrolle (Audit.log)
6.1	Datum und Uhrzeit des Ereignisses
6.2	Quelle IP-Adresse 1. aus dem Behördennetz kommend (IP-Adresse der Web-Proxies IT-DLZ) 2. von extern kommend (IP-Adresse des Providers des Benutzers)
6.3	Ziel IP-Adresse (BayernBox Server)
6.4	Name der BayernBox Instanz
6.5	Benutzername
6.6	Zugriffsmethode auf BayernBox Instanz (GET, PUT, POST)
6.7	Durchgeführte Operationen (Authentifizierung / Dateioperationen / Sharing-Operationen / Zugriffe / Nutzermanagement-Operationen / Änderungen von Einstellungen / Tagging-/Kommentar-Operationen)
6.8	Dateiname bzw. Pfad (bei Dateioperationen)
6.9	Typ des verwendeten Browsers (User Agent)
6.10	Eigentümer der Datei (bei Dateioperationen)
7.	Cookies
7.1	☒ Cookie_ID

7.2	7.3	7.4	7.5	7.6	7.7
Cookie Variante.	Name des Cookie	Anbieter	Zweck (was macht der Cookie?)	Ablauf	Typ (z.B. gif, http etc.)
Persistent Cookie	oc_Session_passphrase	ownCloud	Enthält den Schlüssel um den eigentlichen Auth cookie zu entschlüsseln.	Wird beim Login angelegt um die UserSession zu persistieren. Bleibt bestehen.	http
Persistent Cookie	Prefix oc_: Danach cryptografiert	ownCloud	Das ist der Authentifizierungscookie	Wird beim Login angelegt um die UserSession zu persistieren. Bleibt bestehen.	http

4. Kategorien der betroffenen Personen

Lfd. Nr.	Bezeichnung der Daten *abstrakt
1.	Nutzer der Bayernbox
1.1	☐ *Beschäftigte von Einrichtungen kommunaler Gebietskörperschaften
1.2	☐ *Beschäftigte der Kommunikationspartner
1.3	☐ *Sonstige Personen, die BayernBox zum Datenaustausch nutzen.
2.	☐ *Alle Personen über die Informationen in den getauschten Daten enthalten sind. Die datenschutzrechtliche Zulässigkeit hinsichtlich der Übermittlung dieser Daten liegt im Verantwortungsbereich der BayernBox einsetzenden Stellen.

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** *Angabe abstrakt	**Rechtsgrundlage** *****abhängig von der Aufgabe	**Anlass der Offenlegung** Kategorien von Verarbeitungen *Angabe abstrakt
I. Abschnitt 3 Nr. 1.1, 1.3, 2, 3	*Nutzer der BayernBox Instanz im Rahmen der erteilten Rechte	• *Art. 4 Abs. 1 BayDSG • *Art. 5 Abs. 1 BayDSG • *ggf. i.V. mit anderen Vorschriften zum Datenschutz bzw. spezialgesetzlichen Vorschriften	• *Abhängig von der Aufgabe
II. Abschnitt 3 Nr. 1.1, 1.3, 2, 3	*Linknutzer der BayernBox Instanz im Rahmen der erteilten Rechte	• *Art. 4 Abs. 1 BayDSG • *Art. 5 Abs. 1 BayDSG • *ggf. i.V. mit anderen Vorschriften zum Datenschutz bzw. spezialgesetzlichen Vorschriften	• *Abhängig von der Aufgabe
III. Abschnitt 3 Nr. 1.1, 1.3, 6	*gesondert berechtigte BayernBox Instanz Benutzer (nur lesend), wie z.B. zuständige behördliche Datenschutzbeauftragte, Personalratsmitglieder etc.	• Art. 32 Abs. 1 DSGVO • Art. 32 Abs. 2 Nr. 4c) BayDSG • Art. 39 Abs. 1 b DSGVO • Art. 6 Abs. 4 BayDSG	• Durchführung von datenschutzrechtlichen Stichprobenkontrollen / Eingabekontrolle • siehe Benutzerhandbuch, Rollen- und Rechtekonzept
IV. Abschnitt 3 Nr. 1.1, 1.3, 2, 3	*BayernBox Instanz Administratoren, wie z.B. Administratoren des IuK Benutzerservices , der Fachämter, der Fachreferate der Kommune etc.	• Art. 4 Abs. 1 BayDSG	• Verwaltung der Benutzerrechte, zur Verfügung stehende Apps • siehe Benutzerhandbuch, Rollen- und Rechtekonzept
V. Abschnitt 3 Nr. 1.1,1.3, 3, 4, 5	IT-DLZ BayernBox Infrastruktur Administratoren	• Art. 4 Abs. 1 BayDSG • Auftragserteilung i.V.m. Art. 28 DSGVO	• Bereitstellung und Administration der zentralen BayernBox IT-Infrastruktur inkl. Wartung und Pflege • Betriebsführung der bereitgestellten Server inkl. Wartung und Pflege • Anlegen des initialen BayernBox Instanz Administrators • Zuteilung der Rechte an den initialen BayernBox InstanzAdministrator • Vornahme von globalen BayernBox Einstellungen (wie z.B. keine DropBoxFunktion, Passwortrichtlinie, nur ausgewählte Apps) • Fehlerverifizierung und Behebung bei technischen Störungen • siehe Benutzerhandbuch, Rollen- und Rechtekonzept

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
I. Abschnitt 5 Nr.	abhängig von der jeweiligen „BayernBox Instanz“ der verantwortlichen Stelle	Verantwortlich für die Rechtmäßigkeit der Datenübermittlung und der Feststellung, ob geeignete Garantien vorliegen, sind die einsetzenden verantwortlichen Stellen

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr.	Löschungsfrist
von Abschnitt 3	
Nr. 1	Die Zugangskennungen für BayernBox Instanzbenutzer werden gelöscht, wenn die Nutzung nicht mehr erforderlich ist. Für die Verwaltung der Benutzerkennungen innerhalb der BayernBox Instanz ist die jeweilige öffentliche Stelle selbst verantwortlich. Sie hat eigenverantwortlich dafür Sorge zu tragen, dass Benutzer, die zur Aufgabenbewältigung die Nutzung der BayernBox Instanz nicht mehr benötigen, aus der Instanz entfernt werden.
Nr.1	Die Zugangskennungen für gesondert Berechtigte (Empfänger nach Abschnitt 5 III.) werden gelöscht, wenn die Nutzung nicht mehr erforderlich ist. Für die Verwaltung der Benutzerkennungen für gesondert Berechtigte innerhalb der BayernBox Instanz ist die jeweilige öffentliche Stelle selbst verantwortlich. Sie hat eigenverantwortlich dafür Sorge zu tragen, dass gesondert Berechtigte, die zur Aufgabenbewältigung die Nutzung der BayernBox Instanz nicht mehr benötigen, aus der Instanz entfernt werden.
Nr. 1	Die Zugangskennungen für BayernBox Instanz Administratoren werden gelöscht, wenn die Aufgabe nicht mehr wahrgenommen wird. Für die Verwaltung der BayernBox Instanz Administratoren ist die öffentliche Stelle selbst verantwortlich. Sie hat eigenverantwortlich dafür Sorge zu tragen, dass BayernBox Instanz Administratoren, die zur Aufgabenbewältigung die Nutzung der BayernBox Instanz nicht mehr benötigen, aus der Instanz entfernt werden.
Nr. 1	Die Zugangskennungen für BayernBox Infrastrukturadministratoren werden gelöscht, wenn die Aufgabe nicht mehr wahrgenommen wird. Nimmt ein BayernBox Infrastruktur Administrator des IT-DLZ Bayern seine Aufgabe nicht mehr war, werden seine Kennung und BayernBox Infrastrukturberechtigungen durch den nun zuständigen BayernBox Infrastrukturadministrator entfernt. Zuständig hierfür ist das IT-DLZ Bayern.
Nr. 3	Jede BayernBox Instanz dient zum „Austausch“ von Daten. Eine dauerhafte Vorhaltung von Dateien im Sinne einer „erweiterten Dateiablage“ ist nicht Zweck der Verarbeitungstätigkeit mit der BayernBox. Jede verantwortliche Stelle hat daher nach einer Regelfrist von jeweils 90 Tagen zu prüfen, ob die abgelegten Inhalte noch zur Aufgabenerfüllung erforderlich sind und sie ggf. aus der BayernBox Instanz zu löschen.
Nr. 4, 5	Die Daten werden nach 7 Tagen gelöscht.
Nr. 6	Die Daten werden nach 1 Jahr gelöscht.
Nr. 1 -6.	Wird die BayernBox Instanz von einer kommunalen Stelle nicht mehr benötigt, wird sie im Rahmen der nach den Nutzungsbedingungen vereinbarten Kündigungsfrist vom hierzu Berechtigten des Verantwortlichen beim Kundenservice des IT-DLZ Bayern gekündigt.

Lfd. Nr.	Löschungsfrist
	Verantwortlicher und Auftragsverarbeiter vereinbaren ggf. Aufbewahrungsfristen für Inhaltsdaten und bestimmen einen verbindlichen Einstellungstermin, zu dem die Löschung der Instanz erfolgt. Zum Einstellungstermin löscht ein Systemadministrator der BayernBox Plattform die BayernBox Instanz. Damit werden auch alle personenbezogenen Benutzerdaten, Berechtigungen und Inhaltsdaten unwiederbringlich entfernt.
Nr. 7	Die Cookies werden solange gespeichert, solange eine Zugangskennung zur BayernBox Instanz besteht.

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

I.

Zur Erreichung der in Art. 32 Abs.1 DSGVO genannten Schutzziele und der Umsetzung der in Art. 25 DSGVO genannten Grundsätze sind für die BayernBox IT-Infrastruktur bzw. BayernBox Instanz im IT-DLZ Bayern folgende spezifischen Maßnahmen getroffen:

1. BayernBox IT-Infrastruktur

1.1. Standort:

„BayernBox“, realisiert mit dem Softwareprodukt „ownCloud“ ist zentral am Standort des IT-Dienstleistungszentrum des Freistaats Bayern, St.-Martin-Straße 47, 81541 München installiert und wird von dort aus betrieben.

1.2. Internet / Bayerisches Behördennetz

Die Austauschplattform ist sowohl aus dem Internet wie auch aus dem Bayerischen Behördennetz erreichbar

1.3. Transportverschlüsselung:

Die Verbindung zur Plattform BayernBox findet über eine mit HTTPS gesicherte Verbindung und dem Verschlüsselungsprotokoll TLS 1.2 statt.

Zur Serverauthentifizierung dient ein Zertifikat der Bayerischen SSL- / Infrastruktur PKI auf Basis von RSA mit einer Schlüssellänge von 2048 Bit.

1.4. Managementnetz:

Für administrative Tätigkeiten der BayernBox Infrastruktur Administratoren wird die Verbindung zu den BayernBox Infrastrukturkomponenten über ein gesondertes Managementnetz hergestellt.

1.5. Sicherheitsüberprüftes Personal / sicherheitsempfindliche Stelle:

Die für die BayernBox IT-Infrastruktur zuständigen Administratoren des IT-DLZ Bayern sind einer Sicherheitsüberprüfung der Stufe 1 (Ü1) nach dem Bayerischen Sicherheitsüberprüfungsgesetz unterzogen.

2. BayernBox Plattform

2.1. Rollen- und Rechtekonzept:

Es existiert ein Rollen- und Rechtekonzept (Bayern Box Plattform / BayernBox Instanz), in dem die jeweiligen Zuständigkeiten beschrieben sind.

2.2. Folgende zentrale Voreinstellungen, gültig für alle BayernBox Instanzen, sind getroffen:

2.2.1 Verschlüsselung

standardmäßige https Verbindungsverschlüsselung während des Transports; siehe auch 1.3

2.2.2 „DropBox“ Funktion:

Das Einbinden externer Datenquellen (z.B. fremde Datenhoster bzw. sonstige Storagesysteme, ServerzuServer-Freigaben) für die Dateiablage ist seitens der Konfiguration für die gesamte BayernBox Plattform unterbunden.

2.2.3 Passwörter:

Benutzerpasswörter und die Passwörter bei Linkfreigaben werden als Hashwert mit einer Stärke

I.

Zur Erreichung der in Art. 32 Abs.1 DSGVO genannten Schutzziele und der Umsetzung der in Art. 25 DSGVO genannten Grundsätze sind für die BayernBox IT-Infrastruktur bzw. BayernBox Instanz im IT-DLZ Bayern folgende spezifischen Maßnahmen getroffen:

AES 256 in der jeweiligen Instanzdatenbank abgelegt.

2.2.4 Passwortrichtlinie:

Bei der Erstanmeldung wird die Neuvergabe eines Passwortes (mit Prüfung Passworthistorie, Passwortstärke mind. 8 Zeichen bei zwei Sonderzeichen, Groß- und Kleinschreibung) systemseitig erzwungen. Ein Passwortwechsel ist vierteljährlich vorzunehmen. Ebenso erzwungen wird die Eingabe eines Passwortes bei jeder Anmeldung und bei Linkfreigaben.

2.2.5 Linkfreigaben:

Bei Linkfreigaben wird systemseitig die Eingabe eines Ablaufdatums erzwungen.

2.2.6 Virenschutz:

Beim Hochladen von Dateien werden diese auf Schadsoftware überprüft. Dies erfolgt über den auf dem jeweiligen Server installierten ClamAV-Dienst.

Zusätzlich ist auf den Servern "Sophos Anti-Virus" installiert und es wird wöchentlich ein On-Demand-Scan des gesamten Dateisystems durchgeführt.

2.2.7 Brute-Force Protection:

Nach 3-maliger fehlgeschlagener Anmeldung an der BayernBox wird die Anmeldung über den jeweiligen Benutzernamen für 5 Minuten gesperrt.

2.2.8 File Firewall:

Das Hochladen von Dateien mit dem MIME-Typ „x-ms-dos-executable“ wird systemseitig unterbunden.

3. BayernBox Instanz

3.1. Mandantentrennung:

Möchte eine kommunale Gebietskörperschaft des Freistaates Bayern die BayernBox nutzen, wird ihr eine dedizierte BayernBox Instanz bereitgestellt. Diese beinhaltet eine, von den Daten anderer Stellen getrennte, eigene Datenbank und einen ebenfalls separierten Storagebereich für die Dateiablage. Der BayernBox Instanzname wird aufgabenspezifisch (https://instanzname.bayernbox.de) festgelegt und ist nur den BayernBox Instanz Administratoren und dem IT-DLZ bekannt.

3.2. Benutzerverwaltung innerhalb Bayernbox Instanz:

Die Benutzerverwaltung innerhalb der BayernBox Instanz obliegt vollständig den BayernBox Instanz Administratoren. Das IT-DLZ Bayern hat keine Möglichkeit auf die BayernBox Instanz zuzugreifen oder die Berechtigung Kennungen zu ändern.

3.3. Authentifizierung an der Bayernbox Instanz:

Der von der verantwortlichen Stelle benannte Ansprechpartner (Datenerhebung über den Verantwortlichen gemäß Art. 4 Abs. 2 S.1 BayDSG) erhält vom IT-DLZ Bayern die erstmaligen persönlichen Zugangsdaten (Benutzerkennung, Passwort) für die Administration der eigenen BayernBox Instanz. Im Anschluss daran wird für den benannten Ansprechpartner an die angegebene E-Mail-Adresse ein gesonderter Initialisierungslink versandt und so die Gültigkeit der E-Mail-Adresse geprüft (= Nutzung einer gültigen E-Mail-Adresse). Mit Aufruf des Links (https://instanzname.bayernbox.de) gelangt der BayernBox Instanz Administrator auf die webbasierte Benutzeroberfläche der BayernBox Instanz, über die er sich am System anmelden kann. Eine Passwortänderung wird hierbei beim ersten Anmeldevorgang systemseitig erzwungen (siehe 2.2.4).

Für alle weiteren vom BayernBox Instanz Administrator angelegten Benutzer einer BayernBox gelten die gleichen Authentifizierungsmechanismen.

3.4. Dateien freigeben / Link teilen

I.
Zur Erreichung der in Art. 32 Abs.1 DSGVO genannten Schutzziele und der Umsetzung der in Art. 25 DSGVO genannten Grundsätze sind für die BayernBox IT-Infrastruktur bzw. BayernBox Instanz im IT-DLZ Bayern folgende spezifischen Maßnahmen getroffen:

BayernBox Instanz-Administratoren oder berechtigte Benutzer einer BayernBox können Dateien für andere BayernBox Benutzer oder Benutzergruppen zum Lesen oder Bearbeiten freigeben. Es besteht für berechtigte BayernBox Benutzer aber auch die Möglichkeit, Inhalte durch Versand entsprechender Links per E-Mail für beliebig andere Personen (ohne Benutzerkonto) freizugeben. Hierbei wird die Passworteingabe systemseitig für den Link erzwungen (siehe 2.2.4).

Das Passwort ist den berechtigten Benutzern aus Sicherheitsgründen außerhalb der E-Mail, mit der der Link zur freigegebenen Datei übermittelt wird, gesondert mitzuteilen.

3.5. Verschlüsselte Ablage:
Sollen Daten wegen eines erhöhten Schutzbedarfs an Vertraulichkeit (z.B. besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO, Art. 8 Abs. 2 BayDSG) inhaltsverschlüsselt in BayernBox abgelegt werden müssen, hat die verantwortliche Stelle eigenverantwortlich durch geeignete Maßnahmen selbst für die Verschlüsselung Sorge zu tragen.

3.6. Eingabekontrolle / datenschutzrechtliche Stichprobenkontrolle:
Zur Durchführung anlassloser bzw. anlassbezogener Stichprobenkontrollen durch gesondert Berechtigte (Empfänger nach Abschnitt 5 Nr. III.) wurde für jede BayernBox Instanz eine eigene Benutzerrolle eingerichtet (siehe 2.1). Ausschließlich gesondert Berechtigten ist es möglich auf entsprechende Protokolldaten zuzugreifen; siehe Rechte- und Rollenkonzept. Die Daten werden automatisch nach einem Jahr gelöscht.

II.
Zur Erreichung der in Art. 32 Abs. 2 DSGVO genannten Schutzziele sind folgende **allgemeinen Maßnahmen im IT-DLZ Bayern** getroffen:

Einzelheiten siehe im **Datenschutzkonzept des Landesamts für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern**

Das Datenschutzkonzept wird beim Bestellvorgang sowie bei der Bereitstellungsinformation der jeweiligen BayernBox zur Verfügung gestellt bzw. mitgeliefert.

9. Datenschutz-Folgenabschätzung

Ist für die Form der Verarbeitung eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO erforderlich?
☐ Ja, ☒ Nein Falls ja, bis wann durchzuführen oder zu überprüfen
Begründung Die Prüfung, ob eine Datenschutzfolgenabschätzung für die Verarbeitungstätigkeit (Bereitstellung und Betrieb der Plattform) erforderlich ist, wurde nach dem in 9 I. bis 9 III. aufgeführten Prüfschema vorgenommen; zum Prüfschema siehe auch Ausführungen des Bayerischen Landesbeauftragten für den Datenschutz in seiner Orientierungshilfe zur Durchführung von Datenschutzfolgenabschätzungen; Leitlinien nach EU -Working Paper 248 Rev. 01, S. 9 ff. https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

I.

Prüfungsschema Erforderlichkeit einer Datenschutzfolgenabschätzung (DSFA)	
Frage / Ergebnis	**Antwort**
1) Unterfällt der Verarbeitungsvorgang einem Tatbestand des Art. 14 Abs. 1 BayDSG? **Ergebnis:** Prüfung der Erforderlichkeit der DSFA fortsetzen	1. Nein; vom zuständigen Bayerischen Staatsministerium der Finanzen und für Heimat als Fachaufsichtsbehörde wurde für diese Verarbeitungstätigkeit keine DSFA vorgenommen. 2. Nein, der konkrete Verarbeitungsvorgang ist auch nicht in einer Rechtsvorschrift geregelt.
(2) Liegt eine „Whitelist“ des Bayerischen Landesbeauftragten für den Datenschutz (Art. 35 Abs. 5 DSGVO) vor und wird der Verarbeitungsvorgang von ihr erfasst? **Ergebnis:** Prüfung der Erforderlichkeit der DSFA fortsetzen	Nein, es liegt keine Whitelist des Bayerischen Landesbeauftragten für den Datenschutz vor.
(3) Ist für einen ähnlichen Verarbeitungsvorgang bereits eine DSFA vorhanden? **Ergebnis:** Prüfung der Erforderlichkeit der DSFA fortsetzen	Nein, es ist für einen ähnlichen Verarbeitungsvorgang (Datenaustausch mit Externen; ebenfalls mit dem Produkt ownCloud für staatliche Stellen) keine DSFA vorhanden.
(4) Wird der Verarbeitungsvorgang von der „Blacklist“ (eine DSFA ist zwingend vorzunehmen) des Bayerischen Landesbeauftragten für den Datenschutz (Art. 35 Abs. 4 DSGVO) erfasst? **Ergebnis:** Prüfung der Erforderlichkeit der DSFA fortsetzen	Nein, es liegt aktuell keine „Blacklist“ des Bayerischen Landesbeauftragten für den Datenschutz vor.

II.

5) Unterfällt der Verarbeitungsvorgang einem Tatbestand des Art. 35 Abs. 3DSGVO?	**Erläuterung der Tatbestände**

Art. 35 Abs. 3 Buchst. a DSGVO	systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
Art. 35 Abs. 3 Buchst. b DSGVO	umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO.
Art. 35 Abs. 3 Buchst. c DSGVO	bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.
Analyse: Die Bereitstellung und der Betrieb der Plattform durch das IT-DLZ fällt in keinen Tatbestand des Art. 35 Abs. 3 Buchstabe a bis c DSGVO. **Ergebnis:** Prüfung der Erforderlichkeit der DSFA fortsetzen	

III.

6) Hat der Verarbeitungsvorgang (Bereitstellung und Betrieb der Austauschplattform) auf Grundlage einer eigenen Risikoabschätzung des Verantwortlichen „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge? **Durchführung einer eigenen Schwellwertanalyse** nach den Leitlinien des EU -Working Papers248 Rev. 01.	**Erläuterung der Kriterien (siehe Ausführungen in der Orientierungshilfe des BayLFD).**
(1) Bewerten und Einstufen	Hierunter fällt auch das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von „Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person“ (vgl. Erwägungsgründe 71 und 91 DSGVO). Beispiel: Eine Behörde erstellt anhand der Nutzung ihrer Website personenbezogene Verhaltensprofile.

(2) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung	Dies umfasst Verarbeitungen, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „die Rechtswirkung gegenüber natürlichen Personen entfalten“ oder diese „in ähnlich erheblicher Weise beeinträchtigen“ (vgl. Art. 35 Abs. 3Buchst. a DSGVO). So kann die Verarbeitung beispielsweise zum Ausschluss oder zur Benachteiligung von Personen führen. Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium.
(3) Systematische Überwachung	Dies betrifft Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von betroffenen Personen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „eine systematische [...] Überwachung öffentlich zugänglicher Bereiche“ (vgl. Art. 35 Abs. 3 Buchst. c DSGVO) zurückgreifen.
(4) Vertrauliche oder höchst persönliche Daten	Hierzu zählen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Art. 10 DSGVO. Beispiel: Ein Krankenhaus archiviert die Krankenakten seiner Patienten. Auch weitere Datenkategorien, die zwar nicht in den Art. 9 und 10 DSGVO aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten natürlicher Personen erhöhen können, sind – je nach Fallgestaltung – diesem Kriterium zuzuordnen. Dies kann etwa auch Standort- oder Finanzdaten betreffen. Zu berücksichtigen ist in diesem Zusammenhang unter anderem, ob Daten durch die betroffene Person bereits öffentlich zugänglich gemacht worden sind.
(5) Datenverarbeitung in großem Umfang	Bei Beurteilung der Frage, ob eine Datenverarbeitung „in großem Umfang“ erfolgt, sind insbesondere die folgenden Faktoren zu berücksichtigen: (a) Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil an der entsprechenden Bevölkerungsgruppe (b) verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente (c) Dauer oder Dauerhaftigkeit der Datenverarbeitung (d) geografisches Ausmaß der Datenverarbeitung

6) Abgleichen oder Zusammenführen von Datensätzen	Dies betrifft beispielsweise Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht.
(7) Daten von schutzbedürftigen betroffenen Personen (vgl. Erwägungsgrund 75 DSGVO)	Als schutzbedürftige betroffene Personen gelten beispielsweise folgende Bevölkerungsgruppen: Kinder und Personen mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Patienten usw.).
(8) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen	Hierunter fällt beispielsweise die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle. Aus Art. 35 Abs. 1 DSGVO und Erwägungsgründen 89 und 91 DSGVO wird deutlich, dass der Einsatz einer neuen Technologie, die „entsprechend dem jeweils aktuellen Stand der Technik“ (Erwägungsgrund 91 DSGVO) als solche einzuordnen ist, der Grund für die Notwendigkeit einer DSFA sein kann.
(9) Betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	(Vgl. Art. 22 DSGVO und Erwägungsgrund 91 DSGVO). Hierzu zählen beispielsweise Verarbeitungsvorgänge, mit deren Hilfe betroffenen Personen der Zugriff auf eine Dienstleistung gestattet oder verwehrt werden soll.
Analyse Für Bereitstellung und Betrieb der Plattform durch das IT-DLZ werden keine Verarbeitungen im Sinne der aufgeführten Kriterien vorgenommen. **Gesamtergebnis:** **Es ist keine DSFA durchzuführen.**	

10. Stellungnahme des behördlichen Datenschutzbeauftragten

Liegt eine Stellungnahme des behördlichen Datenschutzbeauftragten vor? ☒ Ja, siehe Anlage ☐ Nein
Ggf. nähere Erläuterung Die Stellungnahme der behördlichen Datenschutzbeauftragten wird beim Bestellvorgang, sowie bei der Bereitstellungsinformation der jeweiligen BayernBox zur Verfügung gestellt bzw. mitgeliefert.

München_____ 21.02.2019_____ gez.: Rudolf Zenkert__

Ort, Datum, Unterschrift (RefL IT24)