Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder

Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG)

Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen

Version 1.1

Stand:
Dezember 2025

Inhalt

Am 24. Juli 2024 ist das OZG-Änderungsgesetz in Kraft getreten.[1] In der Version 1.0 dieser Orientierungshilfe[2] haben die Datenschutzaufsichtsbehörden die aus ihrer Sicht wesentlichen datenschutzrelevanten Änderungen gegenüber der alten Rechtslage zusammengestellt, um die von der Gesetzesänderung betroffenen Stellen bei der Rechtsanwendung zu unterstützen. Als Artikelgesetz umfasst das OZG-Änderungsgesetz in Art. 1 eine Änderung des Onlinezugangsgesetzes, in Art. 2 eine Änderung des E-Government-Gesetzes des Bundes und in den weiteren Artikeln Gesetzesänderungen, auf die in diesem Dokument nicht eingegangen wird.[3]

In der vorliegenden Version 1.1 befassen sich die Aufsichtsbehörden zusätzlich mit Fragestellungen, die an sie seit der Veröffentlichung der Version 1.0 im Rahmen ihrer Aufsichts- und Beratungspraxis herangetragen wurden.

1 Hintergrund der datenschutzrechtlichen Änderungen im OZG

Mit dem Inkrafttreten des Onlinezugangsgesetzes alte Fassung im August 2017 standen der Bund, die Länder und die Kommunen vor der Herausforderung, über 6.000 Verwaltungsleistungen, die zu 575 „Leistungsbündeln“ zusammengefasst wurden, bis Ende 2022 zu digitalisieren.[4] So sollte es beispielsweise möglich werden, den Anwohnerpark-ausweis, das Wohngeld oder auch Leistungen nach BAföG online zu beantragen.

Um mehrfachen Entwicklungs- und Umsetzungsaufwand in den einzelnen Ländern zu vermeiden, hat der nationale IT-Planungsrat das sogenannte EfA (Einer-für-Alle)-Prinzip etabliert. Nach diesem Prinzip soll eine Behörde einen Onlinedienst, z. B. das elektronische Antragsformular zur Beantragung einer Baugenehmigung, entwickeln und allen anderen Behörden – auch über die Landesgrenzen hinaus – zur Nachnutzung zur Verfügung stellen. Die auf diese Weise zu digitalisierenden Leistungen wurden in Themenfelder unterteilt und verschiedenen Themenfeldführern (dem Bund und den Ländern) zugeordnet. Die Idee ist demnach, dass jeder Themenfeldführer für die Entwicklung bestimmter Onlinedienste zuständig ist und diese länderübergreifend verwendet werden.

In der Regel liegt dabei das elektronische Antragsformular auf der IT-Infrastruktur des entwickelnden Landes; Nutzende aus dem eigenen Bundesland, aber auch aus anderen Bundesländern können in dieses Antragsformular ihre Daten eingeben. Die jeweilige den länderübergreifenden Onlinedienst betreibende Behörde übermittelt diese Daten sodann an diejenige

[1] Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 19.7.2024 (BGBl. 2024 I Nummer 245).

[2] Veröffentlicht im November 2024.

[3] Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nummer 245) geändert worden ist und E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert worden ist. Zum E-Government-Gesetz siehe auch Ziffer 8 „Once-Only-Prinzip und der neue § 5 EGovG“.

[4] BMI, OZG-Leistungen: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/ozg-grundlagen/info-leistungen/info-leistungen-node.html.

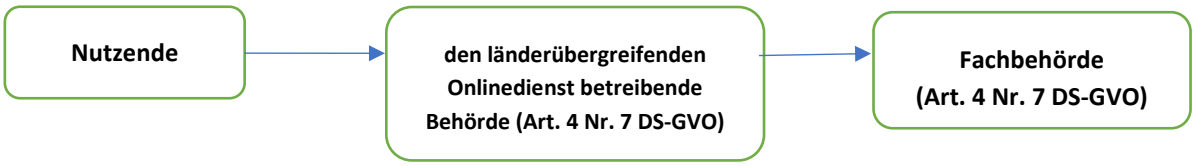
Fachbehörde, die für die jeweilige Antragsbearbeitung örtlich und fachlich zuständig ist und hierfür ein entsprechendes Fachverfahren einsetzt.

Abbildung 1:

Aus datenschutzrechtlicher Sicht stellte sich hierbei die Frage, wer für die personenbezogenen Daten im Antragsformular, das vom länderübergreifenden Onlinedienst bereitgestellt wird, datenschutzrechtlich Verantwortlicher ist und auf welcher Rechtsgrundlage diese personenbezogenen Daten verarbeitet werden. Hierzu existierten unterschiedliche Bewertungsansätze, was zu einer erheblichen Rechtsunsicherheit für die die länder-übergreifenden Onlinedienste betreibenden Behörden und die nachnutzenden Stellen führte.

Die Frage der datenschutzrechtlichen Verantwortlichkeit wurde mit Inkrafttreten des neuen § 8a Abs. 4 OZG geklärt, wonach die jeweilige den länderübergreifenden Onlinedienst betreibende Behörde für die Verarbeitung im Onlinedienst alleinige datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO ist. Hiervon unberührt bleibt die datenschutzrechtliche Verantwortlichkeit der Fachbehörden für die Verarbeitung im „Back-End“. Es stehen somit mehrere datenschutzrechtliche Verantwortliche in der Kette hintereinander.

Abbildung 2:



Wer konkret die den länderübergreifenden Onlinedienst betreibende Behörde für welche Verwaltungsleistung ist, richtet sich nach dem jeweiligen Landes-(organisations-)recht. Hierbei handelt es sich um eine Frage der verwaltungsorganisationsrechtlichen Zuständigkeit. Das heißt, die datenschutzrechtliche Regelung verweist hier auf die Behörde, die den länderübergreifenden Onlinedienst als örtlich und sachlich zuständige Behörde betreibt. Zuständige Behörde könnte je nach landesrechtlicher Zuständigkeitsregelung beispielsweise das für die Onlinedienste zuständige Ministerium sein.

2 Länderübergreifender Onlinedienst

Gemäß § 2 Abs. 8 OZG ist ein „**Onlinedienst**" eine IT-Komponente, die ein **eigenständiges** elektronisches Angebot an die Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund oder Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen von

Bund oder Ländern, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an die Nutzer, gegebenenfalls unter Einbindung von Nutzerkonten einschließlich deren Funktion zur Übermittlung von Daten aus einem Nutzerkonto an eine für die Verwaltungsleistung zuständige Behörde. Der Onlinedienst **kann** auch **verfahrensunabhängig** und **länderübergreifend**, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.

Mit dieser Begriffsbestimmung sollte ein technikneutraler Begriff eingeführt werden, um hinreichend genau bestimmen zu können, welche Datenverarbeitungsvorgänge in § 8a OZG geregelt werden. Gemeint ist in der Regel ein digitales Angebot, das Bürgerinnen und Bürgern sowie Unternehmen ein elektronisches Ausfüllen von Behördenformularen ermöglicht, die Daten also für einen kurzen Zeitraum sammelt und dann kanalisierend an die zuständige Fachbehörde weiterleitet. Der Begriff soll alle elektronischen Angebote erfassen, auch solche, die nicht in einem verfahrensrechtlichen Antrag münden, sondern beispielsweise der Abwicklung einer Informationspflicht dienen.[5] Damit hat sich der Gesetzgeber bewusst für eine weite Definition des Begriffs „Onlinedienst“ entschieden, die von der konkreten technischen Ausgestaltung unabhängig ist.

Durch die tatsächliche Ausgestaltung einer Anwendung (ihr „Design“) können die Regelungen der §§ 2 Abs. 8, 8a OZG nicht umgangen werden. Diese Regelungen gelten beispielsweise unabhängig davon, ob der Onlinedienst über den Browser zu erreichen ist oder als App zur Verfügung steht und ob für den Bürger der Eindruck einer direkten Kontaktaufnahme mit der Fachbehörde oder mit der den Onlinedienst betreibenden Behörde entsteht.[6]

Ferner kann auch allein das Vorhandensein etwaiger Zusatzfunktionen (z. B. zu der Erhöhung der Nutzerfreundlichkeit) nicht dazu führen, dass kein „Onlinedienst“ vorliegt. Vielmehr ist im Hinblick auf die Zusatzfunktionen zu prüfen, ob die durch diese (und nur durch diese) vorgenommenen Verarbeitungen unter ein anderes Regelungsregime fallen oder möglicherweise auf Grund des Sachzusammenhanges noch unter die Regelungen der §§ 2 Abs. 8, 8a OZG subsumiert werden können.

Im Falle einer zu engen Auslegung des „Onlinedienstes“ könnte die Regelung des § 8a OZG umgangen und den damit bezweckten rechtlichen Klarstellungen und Vereinfachungen entgegengewirkt werden (siehe Ziffer 1.). Damit wären auch die in § 8a OZG enthaltenen Rechtsgrundlagen sowie die Verantwortungszuweisung nach Absatz 4 nicht anwendbar (siehe Ziffern 3 und 5 unten). Infolgedessen würde erneut die mit der Schaffung des § 8a OZG geschlossene Regelungslücke auftreten.

[5] BT-Drs. 20/8093, S. 37 f. Aus diesem Grund wurde der ursprünglich vorgesehene Begriff „Antragsassistent“ im Laufe des Gesetzgebungsverfahrens zugunsten des Begriffs „Onlinedienst“ aufgegeben.

[6] Wird dem Bürger durch die Ausgestaltung der falsche Eindruck vermittelt, muss das Design der Anwendung entsprechend dem Transparenzgrundsatz des Art. 5 Abs. 1 Buchst. a DS-GVO angepasst werden.

Das Merkmal „**eigenständig**“ ist weder im Gesetz noch in der Gesetzesbegründung definiert. Gemeint ist, dass der Dienst den Nutzenden als solcher angeboten wird und für diese auffindbar ist (beispielsweise „die digitale Baugenehmigung“).

Das Merkmal „**verfahrensunabhängig**“ unterstreicht die technische Unabhängigkeit vom nachgelagerten Verwaltungsverfahren, in welchem inhaltlich über den Antrag entschieden wird. Hierzu führt die Gesetzesbegründung[7] aus: „Zur elektronischen Unterstützung bei der Inanspruchnahme einer Verwaltungsleistung, insbesondere bei der Antragsvorbereitung und Antragstellung, aber beispielsweise auch der Abwicklung einer Informationspflicht, können informationstechnische Systeme als Assistenzdienste für den Nutzer auch fachunabhängig und ebenenübergreifend eingerichtet und betrieben werden. „Verfahrensunabhängig“ ist ein „Kann“-Merkmal, d. h. ein Onlinedienst im Sinne des § 2 Abs. 8 OZG kann auch dann gegeben sein, wenn dieser nur mit dem nachgelagerten Fachverfahren funktioniert oder eine Mitwirkung der Fachbehörde erfordert.

Beispiel: Die Fachbehörde gestaltet das Frontend des Onlinedienstes mit, indem sie vor der Anbindung des Onlinedienstes den sie betreffenden Teil der Datenschutzerklärung ausfüllt.

Das Merkmal **„länderübergreifend**“ erfasst die Konstellation, dass der Onlinedienst von der Behörde eines Bundeslandes betrieben wird, die Nutzenden jedoch auch in anderen Bundesländern ansässig sein können.

3 Rechtsgrundlagen der Verarbeitung in einem länderübergreifenden Onlinedienst

In den Absätzen 1 bis 3 regelt § 8a OZG die Rechtsgrundlagen der Verarbeitung innerhalb eines länderübergreifenden Onlinedienstes.[8]

§ 8a Abs. 1 S. 1 OZG:

Die den länderübergreifenden Onlinedienst betreibende Behörde kann gemäß § 8a Abs. 1 OZG die erforderlichen personenbezogenen Daten der antragstellenden Personen für die folgenden Zwecke verarbeiten:

- Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung,
- Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde und
- Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an den Nutzer.

[7] BT-Drs. 20/8093, S. 45.

[8] Die vollständige Bezeichnung der Rechtsgrundlage lautet: Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO in Verbindung mit § 8a Abs. 1 OZG (je nach Verarbeitung ggf. in Verbindung mit Abs. 2 und 3).

Beispiele anhand des Falls, in dem eine Baugenehmigung online beantragt werden soll:

Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung (§ 8a Abs. 1 S. Alt. 1 OZG):

- Die antragstellende Person möchte eine Baugenehmigung beantragen und gibt ihre Daten in das elektronische Antragsformular ein – die den Onlinedienst betreibende Behörde erhebt somit die für den Antrag benötigten Daten.

Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde (§ 8a Abs. 1 S. 1 Alt. 2 OZG):

- Nachdem die antragstellende Person die Antragsdaten in das elektronische Antragsformular eingegeben hat, übermittelt die den Onlinedienst betreibende Behörde diese Daten an die Fachbehörde, die für die inhaltliche Bearbeitung des Antrags zuständig ist (z. B. die Stadt Göttingen für Bauanträge der dort ansässigen Antragstellenden); die Daten können dabei – je nach technischer Ausgestaltung – an die Fachbehörde versendet, aber auch zum Abruf durch die Fachbehörde vorgehalten werden.

Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an den Nutzer (§ 8a Abs. 1 S. 1 Alt. 3 OZG):

- Die Fachbehörde (im o. g. Fall des Bauantrags die Stadt Göttingen) gibt der antragstellenden Person den Bescheid über das Nutzerkonto bekannt (§ 9 OZG); hierzu leitet sie die Daten durch den länderübergreifenden Onlinedienst, da dieser über Schnittstellen zum Nutzerkonto verfügt; die Verarbeitung im Rahmen dieser technischen Durchleitungsfunktion wird auf § 8a Abs. 1 S. 1 Alt. 3 OZG gestützt.[9] Eine datenschutzfreundlichere Alternative stellen aus der Sicht der Datenschutzkonferenz jedoch Lösungen dar, die eine direkte Übermittlung des Bescheids in das Nutzerkonto des Bürgers ermöglichen, ohne den länderübergreifenden Onlinedienst passieren zu müssen.

Wichtig: Der Umfang der Verarbeitung und der verarbeiteten Daten ist in allen drei Alternativen auf das für die Abwicklung der elektronischen Verwaltungsleistung Erforderliche beschränkt.

§ 8a Abs. 2 und 3 OZG:

Die Absätze 2 und 3 regeln die Zwischenspeicherung der personenbezogenen Daten im länderübergreifenden Onlinedienst. In der Regel sind die zwischengespeicherten Daten nach Ablauf von 30 Tagen nach der letzten Bearbeitung des Online-Formulars durch den

[9] Vgl. BT-Drs. 20/8093, S. 46.

Nutzer vom Betreiber des Onlinedienstes zu löschen. Abs. 3 S. 3 enthält eine Ausnahmeregelung, wonach auch eine längerfristige – über die 30 Tage hinausgehende – Zwischenspeicherung zulässig sein soll, wenn zu erwarten ist, dass dies für die Unterstützung des Nutzers bei der Inanspruchnahme der elektronischen Verwaltungsleistung erforderlich ist. Hierbei ist insbesondere unklar, auf wessen Erwartungshaltung zu welchem Zeitpunkt abzustellen ist. Als Beispiel wird in der Gesetzesbegründung ein Fall angeführt, in dem eine Antragstellung in zeitlichen Etappen erfolgt und nicht zeitnah abgeschlossen ist.[10] Die praktische Relevanz dieser Konstellation und die tatsächliche Notwendigkeit einer längeren Zwischenspeicherung wird sich noch zeigen müssen. Nach derzeitiger Einschätzung dürfte es sich bei den einschlägigen Fällen um besonders zu begründende Ausnahmefälle handeln.

Besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO:

Für die Verarbeitung besonderer Kategorien personenbezogener Daten enthält § 8a Abs. 1 S. 2 und 3 sowie Abs. 2 S. 2 OZG Sonderregelungen. Durch den Verweis auf § 22 Abs. 2 BDSG ist sichergestellt, dass den vorzunehmenden technischen und organisatorischen Maßnahmen zum Datenschutz ein besonderes Gewicht zukommt. Diese sind auf Grundlage einer entsprechenden Risikoanalyse im Einzelfall zu bestimmen. Hinzuweisen ist dabei insbesondere auf die in der Regel vorzunehmende ausreichende Verschlüsselung gemäß § 22 Abs. 2 S. 2 Nr. 7 BDSG. Durch den Verweis auf § 22 Abs. 2 BDSG richten sich die technischen und organisatorischen Maßnahmen nicht nach den Regelungen der Landesdatenschutzgesetze[11]. Hiervon unberührt bleibt die Anwendbarkeit von spezifischen Regelungen der Landesdatenschutzgesetze auf die Verarbeitung durch die Fachbehörden.

4 Rechtsgrundlagen der Verarbeitung für nicht länderübergreifend angebotene Onlinedienste

Die Rechtsgrundlagen des neuen § 8a OZG (siehe Ziffer 3 oben) sind auf länderübergreifende Onlinedienste beschränkt.

Für die Dienste, die nicht länderübergreifend, sondern dezentral angeboten werden,[12] gelten die Rechtsgrundlagen des § 8a OZG nicht und es bleibt bei der Rechtsgrundlage für die Verarbeitung, die auch bisher angewandt wurde. Diese wird sich in der Regel aus dem Fachgesetz ergeben, nach welchem die Verwaltungsleistung erbracht wird. Soweit der Onlinedienst über einen IT-Dienstleister angeboten wird, wird dieser in der Regel als Auftragsverarbeiter im Auftrag der Fachbehörde tätig.

[10] BT-Drs. 20/8093, S. 47.

[11] Siehe beispielsweise § 17 Abs. 2 und 3 NDSG, § 14 Abs. 3 BlnDSG, § 20 Abs. 2 HDSIG.

[12] Und z. B. nur den Nutzerinnen und Nutzern des betreibenden Landes zur Verfügung stehen.

5 Konsequenzen der neuen datenschutzrechtlichen Regelungen

5.1 Datenschutzrechtliche Verantwortlichkeit kraft gesetzlicher Zuweisung

Die den länderübergreifenden Onlinedienst betreibende Behörde wird kraft Gesetzes zum datenschutzrechtlich Verantwortlichen im Sinne des Art. 4 Nr. 7 Hs. 2 DS-GVO, der die personenbezogenen Daten auf Basis einer eigenen Rechtsgrundlage verarbeitet.[13] Als Verantwortliche treffen diese Behörde insbesondere die Informationspflichten aus Art. 12 ff. DS-GVO, ferner können ihr gegenüber die Betroffenenrechte aus Art. 15 ff. DS-GVO ausgeübt werden. Auch etwaige „Datenpannen" sind gemäß Art. 33 DS-GVO vom Verantwortlichen an die zuständige Datenschutzaufsichtsbehörde zu melden; die Betroffenen sind gemäß Art. 34 DS-GVO vom Verantwortlichen zu unterrichten. Für die Erfüllung der gegebenenfalls neu hinzukommenden Pflichten sind beim Verantwortlichen entsprechende Prozesse vorzusehen. Auch eine etwaige Verpflichtung zur Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO obliegt dem Verantwortlichen.

Ferner muss die Datenschutzerklärung des länderübergreifenden Onlinedienstes angepasst werden. Während in der bisherigen Datenschutzerklärung im Beispielsfall die jeweilige Fachbehörde als Verantwortliche anzugeben war, ist nun zu prüfen, welche Behörde für den Betrieb des länderübergreifenden Onlinedienstes zuständig ist.[14] Diese Behörde ist gemäß § 8a Abs. 4 OZG nun für die Verarbeitung im länderübergreifenden Onlinedienst verantwortlich und ist in der Datenschutzerklärung als Verantwortliche anzugeben.

5.2 Aufhebung von entgegenstehenden datenschutzrechtlichen Vereinbarungen

Bereits vor dem Inkrafttreten des OZG-Änderungsgesetzes wurden länderübergreifende Onlinedienste in Betrieb genommen und durch andere Behörden nachgenutzt. Hierzu wurden in vielen Fällen datenschutzrechtliche Regelungen getroffen, beispielsweise Auftragsverarbeitungsverträge gemäß Art. 28 Abs. 3 DSGVO oder Vereinbarungen gemäß Art. 26 DSGVO. Seit der Gesetzesänderung wird es Fälle geben, in denen die abgeschlossene Vereinbarung die datenschutzrechtlichen Rollen der Beteiligten nicht mehr korrekt beschreibt. Handelte die den länderübergreifenden Onlinedienst betreibende Behörde beispielsweise vor dem Inkrafttreten des OZG-Änderungsgesetzes als Auftragsverarbeiter für die nachnutzenden Behörden und hat sie mit diesen hierzu eine Auftragsverarbeitungsvereinbarung abgeschlossen, ist diese Vereinbarung mit dem Inkrafttreten des OZG-Änderungsgesetzes als überholt anzusehen. Denn nunmehr ist die den Onlinedienst betreibende Behörde Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO kraft gesetzlicher Zuweisung nach § 8a Abs. 4 OZG. Die abgeschlossene

[13] Siehe auch Ziffer 3. „Rechtsgrundlagen der Verarbeitung in einem länderübergreifenden Onlinedienst".

[14] Siehe Ziffer 1 oben.

Vereinbarung ist nach den zivilrechtlichen Grundsätzen aufzuheben.[15]

5.3 Einsatz von Auftragsverarbeitern und Beispiel für die Verteilung der datenschutzrechtlichen Rollen

Der neue § 8a OZG macht das Konstrukt der Auftragsverarbeitung bei länderübergreifenden Onlinediensten nicht obsolet: Es wird auch Fälle geben, in denen sich die den länderübergreifenden Onlinedienst betreibende Behörde eines IT-Dienstleisters bedient. Dieser handelt auch nach der Gesetzesänderung als Auftragsverarbeiter.[16]

Beispiel: Ist nach dem Landesrecht das Landesdigitalministerium die den länderübergreifenden Onlinedienst betreibende Behörde im Sinne des § 8a Abs. 1 OZG und bedient sich diese Behörde beim Betrieb des Onlinedienstes der Dienste des Landes-IT-Dienstleisters[17], ergibt sich folgende datenschutzrechtliche Rollenverteilung:

- Landesdigitalministerium: Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO
- Landes-IT-Dienstleister: Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO
- Für den Antrag zuständige Fachbehörden (auch aus den anderen Bundesländern): Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO

Die Rechtsgrundlagen der Verarbeitung sind dann wie folgt:

- Das Landesdigitalministerium erhebt die Antragsdaten gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO in Verbindung mit § 8a Abs. 1 S. 1 Alt. 1 OZG.
- Der Landes-IT-Dienstleister handelt gemäß Art. 28 DS-GVO als Auftragsverarbeiter des Landesdigitalministeriums. Er benötigt hierfür keine eigene Rechtsgrundlage.
- Das Landesdigitalministerium übermittelt die Antragsdaten (unter Einsatz des Auftragsverarbeiters) gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO in Verbindung mit § 8a Abs. 1 S. 1 Alt. 2 OZG an die Fachbehörden.

Die Fachbehörden verarbeiten personenbezogene Antragsdaten entsprechend der Rechtsgrundlage aus ihrem jeweiligen Fachrecht, welche auch ohne die Verwendung des Onlinedienstes maßgeblich ist.

---

[15] In der 36. Abteilungsleiterrunde des IT-Planungsrats wurde festgelegt, keine neuen Vereinbarungen gemäß Art. 28 und Art. 26 DSGVO mehr abzuschließen (Beschluss 2024/17-AL vom 10.12.2024). Bereits abgeschlossene Vereinbarungen seien auf Grund von Geltung von § 8a Abs. 4 OZG nicht zwingend aufzuheben. Die DSK hält - schon aus Gründen der Klarstellung – eine Aufhebung der § 8a Abs. 4 Satz 1 OZG widersprechenden Vereinbarungen für erforderlich.

[16] Auch nach der Gesetzesbegründung muss die den länderübergreifenden Onlinedienst betreibende Behörde den tatsächlichen Betrieb nicht selbst vornehmen, sondern darf sich Dritter bedienen, vgl. BT-Drs. 20/8093, S. 45.

[17] Der Landes-IT-Dienstleister könnte z. B. den Onlinedienst in seinem Rechenzentrum hosten und den technischen Support dafür erbringen.

6 Die den länderübergreifenden Onlinedienst betreibende Behörde als Fachbehörde

Die den länderübergreifenden Onlinedienst betreibende Behörde kann gleichzeitig auch die zuständige Fachbehörde sein. Das ist zum Beispiel dann der Fall, wenn eine Behörde den länderübergreifenden Onlinedienst in ihrem Rechenzentrum betreibt (oder durch einen Auftragsverarbeiter betreiben lässt) und diesen Dienst gleichzeitig als Fachbehörde für die Anträge der Nutzerinnen und Nutzer, für die sie fachlich zuständig ist, verwendet. Hier ist – auch in organisatorischer Hinsicht – streng zwischen den beiden Funktionen dieser Behörde zu trennen. Ferner gelten für beide Bereiche unterschiedliche Rechtsgrundlagen der Verarbeitung, die auch in der datenschutzrechtlichen Dokumentation zu berücksichtigen sind.[18]

7 Nutzerkonto / BundID / DeutschlandID

7.1 Nutzerkonto

Für viele Onlinedienste wird eine Identifizierung und Authentifizierung des Nutzers erforderlich sein. Dies ist mithilfe eines Nutzerkontos im Sinne des § 2 Abs. 5 OZG möglich.

Ein Nutzerkonto ist gemäß § 2 Abs. 5 OZG eine zentrale IT-Komponente zur einmaligen oder dauerhaften Identifizierung und Authentifizierung der Nutzer zu Zwecken der Inanspruchnahme von Verwaltungsleistungen der öffentlichen Verwaltung sowie zur vorgangsbezogenen sicheren Kommunikation über ein Postfach im Sinne des § 2 Abs. 7 OZG. Ein Nutzerkonto wird als Bürger- oder Organisationskonto bereitgestellt. Das „Bürgerkonto“ ist ein Nutzerkonto, das natürlichen Personen zur Verfügung steht. Das „Organisationskonto“ ist ein Nutzerkonto, das Unternehmen im Sinne des § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes sowie Behörden zur Verfügung steht.

Nutzerkonten gab es bereits vor dem Inkrafttreten des geänderten Onlinezugangsgesetzes. Eine wesentliche Änderung besteht darin, dass das Bürgerkonto künftig als zentrales Nutzerkonto vom Bund und nicht mehr dezentral durch die Länder bereitgestellt wird. Zudem wird das zentrale Bürgerkonto des Bundes (bisher „BundID“ genannt) gemäß § 12 Abs. 1 S. 3 OZG zur DeutschlandID weiterentwickelt. Für den Parallelbetrieb von bisherigen Bürgerkonten der Länder gilt gemäß § 12 Abs. 1 S. 1 OZG eine Übergangsfrist von 3 Jahren ab Vorliegen der Voraussetzungen für eine automatisierte Migration der Länderkonten auf die DeutschlandID. Das Vorliegen dieser Voraussetzungen gibt das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem IT-Planungsrat im Bundesgesetzblatt bekannt.

Neben dem Bürgerkonto sieht das Onlinezugangsgesetz auch ein Organisationskonto für Unternehmen und Behörden vor (siehe oben). Damit können sich Organisationen im Sinne von § 2 Abs. 5 S. 4 OZG für die Beantragung von elektronischen Verwaltungsleistungen identifizieren

[18] Siehe auch Ziffer 9 „Dokumentationspflichten“.

und authentifizieren. Behörden können das Organisationskonto nicht nur als Anbieter von Verwaltungsleistungen im Portalverbund (§ 3 Abs. 3 OZG) nutzen, sondern auch als Antragsteller, beispielsweise bei Förderanträgen. Als Anbieter von Verwaltungsleistungen sind Behörden zur Nutzung des Organisationskontos verpflichtet, es sei denn die Verwaltungsleistung erfordert ein Identifizierungsmittel auf dem Sicherheitsniveau „hoch“ (§ 12 Abs. 3 OZG).

7.2 Datenschutzrechtliche Verantwortlichkeit für ein Nutzerkonto

Die datenschutzrechtliche Verantwortlichkeit für das Nutzerkonto obliegt gemäß § 8 Abs. 10 OZG der jeweils zuständigen Stelle. Die Bestimmung der zuständigen Stelle, die das zentrale Bürgerkonto des Bundes bereitstellt, obliegt gemäß § 3 Abs. 1 S. 3 OZG dem Bundesministerium des Innern und für Heimat im Wege einer Rechtsverordnung. Die Bestimmung der zuständigen Stelle für die übergangsweise weiter betriebenen Nutzerkonten der Länder richtet sich nach dem Landes-(organisations-)recht. Die Bereitstellung des zentralen Organisationskontos obliegt dem Freistaat Bayern und der Freien Hansestadt Bremen.[19]

7.3 Rechtsgrundlagen der Verarbeitung in einem Nutzerkonto

§ 8 OZG[20] regelt als zentrale Norm die Rechtsgrundlagen für die Verarbeitung personen-bezogener Daten in einem Nutzerkonto und zu Identifizierungszwecken. Neu gegenüber dem § 8 OZG alte Fassung ist unter anderem, dass die bisherige „Einwilligung“ in bestimmte Verarbeitungen (beispielsweise in eine dauerhafte Speicherung der Identitätsdaten in einem Nutzerkonto) durch eine „Veranlassung“ des Nutzers ersetzt wird. Damit wird gegenüber der alten Fassung des § 8 OZG klargestellt, dass es sich bei der erforderlichen Willensbekundung des Nutzers nicht um eine Einwilligung im Sinne des Art. 4 Nr. 11 DS-GVO handelt.[21] Wesentliche Anforderungen an eine wirksame „Veranlassung“ aus datenschutzrechtlicher Sicht sind, dass die Veranlassung nachweislich durch ein aktives Handeln des Nutzers erfolgt und dem Nutzer die Verarbeitungen seiner personenbezogenen Daten, die durch die jeweilige Handlung veranlasst werden, transparent sind. Die Verwendung des Bürgerkontos ist Bürgerinnen und Bürger weiterhin freigestellt (§ 3 Abs. 1 Satz 2 OZG).

8 Once-Only-Prinzip und der neue § 5 EGovG

Nach dem Once-Only-Prinzip sollen Bürger und Unternehmen bei der Inanspruchnahme von elektronischen Verwaltungsleistungen ihre Nachweise im Verwaltungsverfahren nur einmal

[19] Verordnung nach § 3 Absatz 2 des Onlinezugangsgesetzes vom 22. September 2021 (BGBl. I S. 4370), die durch Artikel 7 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nummer 245) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/ozg_3abs2s2v/BJNR437000021.html.

[20] In Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO.

[21] Somit ist die Rechtsgrundlage für die Verarbeitung weiterhin Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO in Verbindung mit der einschlägigen Regelung des § 8 OZG, und nicht etwa Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DS-GVO.

an die „Verwaltung“ übermitteln müssen. Das bedeutet beispielsweise, dass wenn für die Bearbeitung eines Antrags die Geburtsurkunde der antragstellenden Person erforderlich ist, die antragstellende Person entscheiden kann, ob sie die Geburtsurkunde selbst an die Behörde, die die Geburtsurkunde für die Antragsbearbeitung benötigt, übermittelt oder bei der ausstellenden Behörde abrufen lässt. Die Rechtsgrundlage dafür schafft der neue § 5 EGovG des Bundes.[22] Zum Nachweisabruf berechtigt sind gemäß § 5 Abs. 2 S. 2 EGovG sowohl die Stellen, die für die fachliche Entscheidung zuständig sind (Fachbehörden), als auch Stellen, die dafür zuständig sind, Nachweise einzuholen und an die Fachbehörden weiterzuleiten (zum Beispiel die den länderübergreifenden Onlinedienst betreibenden Behörden). Die Verantwortung für die Zulässigkeit des Nachweisabrufs trägt die nachweis-anfordernde Stelle (§ 5 Abs. 1 S. 3 EGovG). Bevor der Nachweis durch die Behörde, die diesen für die Antragsbearbeitung benötigt, abgerufen wird, erfolgt eine Vorschau des Nachweises für die antragstellende Person (§ 5 Abs. 5 S. 1 EGovG).

9 Dokumentationspflichten

Verarbeitet die den länderübergreifenden Onlinedienst betreibende Behörde personen-bezogene Daten, unterliegt sie – wie bei jeder Verarbeitung – der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO und bestimmten Dokumentationspflichten. Diese haben sich mit dem OZG-Änderungsgesetz nicht verändert.

So muss die den länderübergreifenden Onlinedienst betreibende Behörde zunächst das Verzeichnis der Verarbeitungstätigkeiten im Sinne von Art. 30 DS-GVO um einen den Onlinedienst beschreibenden Eintrag erweitern.

Ferner bedarf es der Dokumentation der getroffenen technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DS-GVO. Wird bei der Verarbeitung ein Auftragsverarbeiter eingesetzt, reicht es für den Verantwortlichen nicht, darauf zu verweisen, dass dieser technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO ergriffen habe. Vielmehr muss sich der Verantwortliche selbst mit den vom Auftragsverarbeiter getroffenen Maßnahmen befassen und die Bewertung dieser Maßnahmen dokumentieren.

Ebenso ist die den länderübergreifenden Onlinedienst betreibende Behörde verpflichtet, mögliche Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu analysieren und Abhilfemaßnahmen zu bestimmen, die hinsichtlich dieser Risiken ein angemessenes Sicherheitsniveau für die Betroffenen sicherstellen. Stets ist zu prüfen, ob die geplante Verarbeitung personenbezogener Daten voraussichtlich zu einem hohen Risiko führt (Schwellwertanalyse). Sollte dies der Fall sein, ist die den länderübergreifenden Onlinedienst betreibende Behörde verpflichtet, vor der Inbetriebnahme des Onlinedienstes eine Datenschutz-Folgenabschätzung im Sinne des Art. 35 DS-GVO nachzuweisen.

[22] Dieser gilt für die Landesbehörden allerdings nur soweit sie Bundesrecht ausführen (§ 1 EGovG). Daher bedarf es noch einer „Umsetzung“ der Regelung im Landesrecht.

Im Rahmen eines „Datenschutzkonzepts“ sind ferner – soweit nicht bereits von der Datenschutz-Folgenabschätzung umfasst – die im Rahmen des Onlinedienstes stattfindenden Verarbeitungen darzustellen; diesen ist jeweils eine Rechtsgrundlage zuzuordnen. Ein weiterer Bestandteil des Datenschutzkonzepts sollte zudem die Abbildung der Prozesse zur Erfüllung der Betroffenenrechte sowie die Darstellung der getroffenen technischen und organisatorischen Datenschutzmaßnahmen sein – soweit diese nicht bereits im Rahmen der Datenschutz-Folgenabschätzung dargestellt worden sind.