# Orientierungshilfe

**der Konferenz der unabhängigen Datenschutzaufsichtsbehörden**

**des Bundes und der Länder**

---

**Ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes**

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

**Version 1.0**

Stand: November 2024

Am 24.7.2024 ist das OZG-Änderungsgesetz in Kraft getreten.[1] In diesem Dokument 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.[2] Nicht Gegenstand dieser Anwendungshilfe sind ferner fachgesetzliche Regelungen, wie z. B. solche des Sozialgesetzbuches.

## 1. Hintergrund der datenschutzrechtlichen Änderungen

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

---

[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).

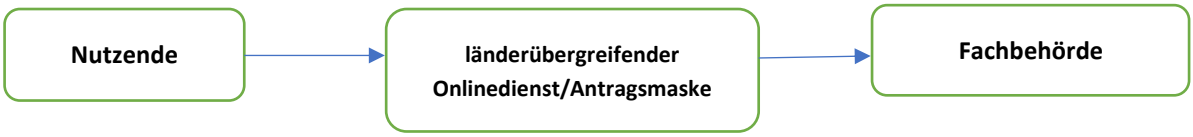
[2] Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nummer 245) geändert worden ist und E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert worden ist. Zum E-Government-Gesetz siehe auch Ziffer 7 „Once-Only-Prinzip und der neue § 5 EGovG“.

2022 zu digitalisieren.[3] So sollte es beispielsweise möglich werden, den Anwohnerparkausweis, 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 Behörde, die für die jeweilige Antragsbearbeitung örtlich und fachlich zuständig ist.

Abbildung 1:

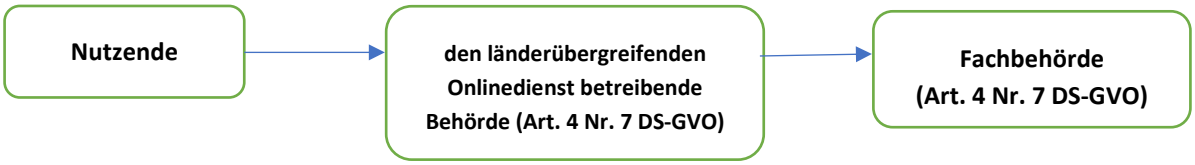



Aus datenschutzrechtlicher Sicht stellte sich hierbei die Frage, wer für die personenbezogenen Daten im Antragsformular, das vom länderübergreifenden Onlinedienst bereitgestellt wird, datenschutzrechtlich Verantwortlicher ist und auf welcher Rechtsgrundlage diese personenbezogenen Daten verarbeitet werden.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

Die Frage der 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 Verantwortliche in der Kette hintereinander.

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

Abbildung 2:




Wer konkret die den länderübergreifenden Onlinedienst betreibende Behörde für welche Verwaltungsleistung ist, richtet sich nach dem jeweiligen Landes-(organisations-)recht. Hier sind die Länder gefragt, die den jeweiligen länderübergreifenden Onlinedienst betreibende Behörde zu benennen. Das könnte beispielsweise das für die Onlinedienste zuständige Ministerium sein.

**2. Rechtsgrundlagen der Verarbeitung in einem länderübergreifenden Onlinedienst**

In den Absätzen 1 bis 3 regelt § 8a OZG die Rechtsgrundlagen der Verarbeitung innerhalb eines länderübergreifenden Onlinedienstes.[4]

§ 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.

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.

[4] 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).

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.[5]

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 Nutzer 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.[6] Die praktische Relevanz dieser Konstellation und die tatsächliche Notwendigkeit einer längeren Zwischen-speicherung wird sich noch zeigen müssen. Nach derzeitiger Einschätzung dürfte es sich bei den einschlägigen Fällen um besonders zu begründende Ausnahmefälle handeln.

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

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

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.

## 3. Rechtsgrundlagen der Verarbeitung für nicht länderübergreifend angebotene Onlinedienste

Die Rechtsgrundlagen des neuen § 8a OZG (s. o.) sind auf länderübergreifende Onlinedienste beschränkt. Sie gelten nicht für Onlinedienste, die dezentral betrieben werden und zum Beispiel nur den Nutzerinnen und Nutzern des betreibenden Landes zur Verfügung stehen.

Für die Dienste, die nicht länderübergreifend angeboten werden, bleibt es 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.

## 4. Konsequenzen der neuen datenschutzrechtlichen Regelungen

### a) 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.[7] 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.

[7] Siehe auch Ziffer 2. „Rechtsgrundlagen der Verarbeitung in einem länderübergreifenden Onlinedienst“.

**b) 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.[8]

Beispiel: Bestimmt das Landesrecht das Landesdigitalministerium zu der den länderübergreifenden Onlinedienst betreibenden Behörde im Sinne des § 8a Abs. 1 OZG und bedient sich diese Behörde beim Betrieb des Onlinedienstes der Dienste des Landes-IT-Dienstleisters[9], 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.

**5. 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

[8] 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.

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

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.[10]

## 6. Nutzerkonto / BundID / DeutschlandID

### a) 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. 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.[11] 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.

### b) 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.[12]

---

[10] Siehe auch Ziffer 8 „Dokumentationspflichten“.

[11] Vom Bürgerkonto (§ 2 Abs. 5 S. 3 OZG) ist das Organisationskonto (§ 2 Abs. 5 S. 4 OZG), auch Unternehmenskonto genannt, zu unterscheiden. Die Bereitstellung eines einheitlichen Organisationskontos ist bereits vor der hier beschriebenen Gesetzesänderung in das Onlinezugangsgesetz aufgenommen worden.

[12] 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.

### c) Rechtsgrundlagen der Verarbeitung in einem Nutzerkonto

§ 8 OZG[13] regelt als zentrale Norm die Rechtsgrundlagen für die Verarbeitung personenbezogener 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.[14] 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.

## 7. 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 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.[15] 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 nachweisanfordernde 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).

## 8. Dokumentationspflichten

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

---

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

[14] 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.

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

OZG-Änderungsgesetz nicht verändert. In der Regel wird beispielsweise vor der Inbetriebnahme des Onlinedienstes die Erstellung einer Datenschutz-Folgenabschätzung im Sinne des Art. 35 DS-GVO erforderlich sein. 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. 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.

Darüber hinaus muss die den länderübergreifenden Onlinedienst betreibende Behörde Art. 30 DS-GVO beachten und das Verzeichnis der Verarbeitungstätigkeiten um einen den Onlinedienst beschreibenden Eintrag erweitern.