

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 21. Oktober 2025

zum Entwurf des zweiten Staatsvertrags zur Änderung des Staatsvertrags zur Neuregulierung des Glücksspielwesens in Deutschland (2. Änderungsglücksspielstaatsvertrag 2021)

1. Zu § 4b Abs. 2 S. 2 f. GlüStV-E

Die Datenschutzkonferenz erkennt zunächst an, dass im Austausch gegen die Erweiterung der Informationsquellen auf ausländische Strafverfolgungs- und Sicherheitsbehörden datenschutzrechtliche Verbesserungen eingetreten sind, namentlich:

- die Subsidiarität der Einholung von Informationen gegenüber der Feststellung anderer Versagungskriterien hinsichtlich der Konzessionserteilung, zumindest soweit diese bereits feststehen,
- die ausdrückliche Festlegung auf den Zweck, Zweifelsfälle zu beseitigen, der dem Grunde nach nicht erforderliche Abfragen weiter vermindern sollte sowie
- die als Satz 3 der Vorschrift eingefügte ausdrückliche und datenschutzrechtlich unbedenkliche Löschfrist.

Auch wenn insbesondere die Festlegungen zur Löschung angesichts der allgemeinen Bindung der Löschung an die Erforderlichkeit weitgehend deklaratorischen Charakter haben, sind diese Verbesserungen ausdrücklich zu begrüßen. Da jedoch die Zweckbindung gemäß dem Entwurf lediglich die Erhebung der Daten und deren Nutzung zum Treffen der Entscheidung über die Zulässigkeit umfasst, sollte zusätzlich eine einschränkende Zweckbestimmung für die Nutzung der nach Satz 2 erhobenen Daten im Zeitraum nach Erteilung der (ablehnenden) Entscheidung und bis zur Löschung auf Zwecke der (gerichtlichen) Überprüfung der ablehnenden Entscheidung in den Entwurfstext aufgenommen werden.

Nicht voraussetzungslos mit dem Datenschutz vereinbar ist die neu vorgesehene Übermittlung personenbezogener Daten in Staaten, die weder Mitgliedsstaaten der Europäischen Union sind oder sonst dem Europäischen Wirtschaftsraum angehören, noch einen Angemessenheitsbeschluss gemäß Art. 45 der Datenschutz-Grundverordnung (DS-GVO) vorweisen können. Dieser Komplex ist in den Art. 44 ff. DS-GVO geregelt. Während für die Mitgliedsstaaten der Europäischen Union, bzw. des Europäischen Wirtschaftsraums ein dem Inland im wesentlichen gleichrangiges

Datenschutzniveau vorausgesetzt werden kann und dieses in Staaten, für die ein Angemessenheitsbeschluss als Übermittlungsinstrument im Sinne von Art. 44 ff. DS-GVO vorliegt, abhängig von dessen Anwendungsbereich ebenfalls der Fall sein kann, gilt dies für andere Staaten nicht. In Übermittlungen in solche Staaten kann damit ein besonders tiefer Grundrechtseingriff für die Daten betroffener Personen liegen, und sie sind nur unter engen Voraussetzungen möglich.

Bei derartigen Drittlandsübermittlungen ist von der verantwortlichen übermittelnden Stelle, neben der für alle Übermittlungen unabhängig von ihrem Auslandsbezug erforderlichen Prüfung erster Stufe (etwa Vorliegen einer ausreichenden Rechtsgrundlage, Erforderlichkeit, Vorliegen technisch-organisatorischer Maßnahmen), als Teil der Übermittlungsvoraussetzungen der Art. 44 ff. DS-GVO in einem zweiten Schritt zu prüfen, ob in diesen Fällen zumindest geeignete Garantien gemäß Art. 46 Abs. 2 und Abs. 3 DS-GVO vorliegen oder geschaffen werden können. Beispiele finden sich in den „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ des Europäischen Datenschutzausschusses vom 18. Juni 2021, insbesondere in den Randnummern 55 ff. Bei der Auswahl der Garantien ist darauf zu achten, dass diese gerade von öffentlichen Stellen umsetzbar sind.

Zwar erlaubt Art. 49 Abs. 1 Buchst. d) in Verbindung mit Abs. 4 DS-GVO, ausgeführt in Erwägungsgrund 112, auch in Fällen, in denen keine geeigneten Garantien zur Verfügung stehen, eine aus wichtigen Gründen des öffentlichen Interesses auf das Recht des Mitgliedstaates gestützte, notwendige Datenübermittlung. An der Hinderung ungeeigneter Anbieter an der Marktteilnahme besteht sicherlich in einer sensiblen Branche wie dem Glücksspiel ein öffentliches Interesse. Ob dieses jedoch auch als „wichtiges“ öffentliches Interesse i. S. d. Art. 49 Abs. 1 lit. d DSGVO angesehen werden kann, muss mit Blick auf das konkrete Drittland und hinsichtlich der mit diesem Drittland bestehenden internationalen Abkommen oder Übereinkünften geprüft werden. Der Umstand, dass ein bestimmtes Interesse im Unionsrecht oder Recht des Mitgliedsstaats genannt ist, begründet noch keine Rechtfertigung sämtlicher Übermittlungen zu diesem Zweck (vgl. Europäischer Datenschutzausschusses, Leitlinien 02/2018, S. 12 f.). Zudem müssen vorhandene oder herstellbare Garantien zwingend ausgeschöpft werden, wie Art. 49 Abs. 1 S. 1 DS-GVO deutlich macht. Eine Übermittlung ohne entsprechende Garantien darf zudem keinesfalls in großem Umfang und systematisch erfolgen. Sie muss vielmehr stets ihren Ausnahmecharakter behalten und bleibt spezifischen, eng definierten Situationen vorbehalten, in denen sie streng erforderlich ist (vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679).

Näheres zu den Übermittlungen in Drittländer findet sich in dem Kurzpapier Nr. 4 „Datenübermittlung in Drittländer“ der Datenschutzkonferenz, verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf

In jedem Fall muss die Übermittlung personenbezogener Daten gerade in Drittländer ohne Angemessenheitsbeschluss in dem Sinne erforderlich sein, dass nicht auf sie verzichtet werden kann, ohne dass die Aufgabenerfüllung schlechterdings unmöglich würde. Die Erforderlichkeit ist bereits Voraussetzung jeder Übermittlung zur Erfüllung öffentlicher Aufgaben und somit auf erster

Stufe zu prüfen (hier: gemäß Art. 6 Abs. 1 Buchst. c) bzw. e) DS-GVO). Die Erforderlichkeit ist aber bei Drittlandübermittlungen aufgrund des regelmäßig tieferen Grundrechtseingriffs streng auszulegen. Diese strenge Erforderlichkeit ist stets im Einzelfall zu prüfen und zu begründen. Die Übermittlung personenbezogener Daten in solche Drittländer ist also nicht nur im Hinblick auf die anderen Versagungskriterien subsidiär, sondern auch gegenüber allen Ermittlungsmaßnahmen, welche ohne Übermittlung personenbezogener Daten in diese Länder auskommen.

Im Übrigen bleibt die übermittelnde inländische Stelle bei ihrem eigenen Handeln voll an die Pflichten der Datenschutz-Grundverordnung gebunden. Für alles Vorstehende ist die übermittelnde Stelle darlegungspflichtig, Art. 5 Abs. 2 DS-GVO.

Die Datenschutzkonferenz empfiehlt dringend, die zuständigen Behörden vor der Übermittlung personenbezogener Daten nach § 4b GlüStV insbesondere in Staaten ohne gleichwertiges Datenschutzniveau auf geeignetem Wege von ihren datenschutzrechtlichen Prüfpflichten zu unterrichten, da der Normtext diese schon wegen des europarechtlichen Wiederholungsverbots nicht vollständig reflektieren kann.

2. Zu § 8 Abs. 3 S. 5 GlüStV-E

Die Zugangskennung ist betriebsbezogen und nicht personenbezogen und die Vorschrift hat nur einen ordnungsrechtlichen, aber keinen datenschutzrechtlichen Gehalt.

3. Zu § 9 GlüStV-E

Die Anpassungen zu Buchstabe a) an die neue telemedienrechtliche Rechtslage sind nachvollziehbar.

Hinsichtlich der Geeignetheit von Sperrmethoden (Nr. 3a zu § 9 Abs. 3 Nr. 5 des Entwurfs) ist Folgendes anzumerken: In der Begründung wird beschrieben, dass Internetanbieter durch eine DNS-Sperre Einfluss auf die Erreichbarkeit eines Dienstes nehmen können. In diesem Fall soll der Anbieter in seinen DNS-Servern die Auflösung einer spezifischen Domain zu der zugehörigen IP-Adresse des Servers entfernen bzw. sperren (DNS-Sperre). Gemäß der Begründung ist diese Maßnahme aber nur erfolgreich, wenn Nutzende auch die DNS-Server des Internetzugangsanbieters nutzen. Diese werden zwar bei der Einrichtung des Modems bzw. des Routers standardmäßig vom Provider übermittelt. Es ist jedoch prinzipiell möglich, sowohl im Router als auch im Endgerät andere DNS-Server anzugeben (bspw. Google), um die Auflösung von Domains durchführen zu lassen. In diesem Fall würden die Änderungen in den DNS-Servern des Zugangsanbieters einfach ignoriert. Auch ist es möglich, über verschiedene Webseiten Anfragen an verschiedene DNS-Server zu schicken, um die dort hinterlegten Informationen zu einer Domain zu erhalten. Mit der so erlangten IP-Adresse wäre je nach Konfiguration des zugehörigen Servers ebenfalls ein Zugriff auf die Webseite möglich.

Auch die Nutzung von VPN-Anbietern würden solche DNS-Sperren beim Provider je nach Konfiguration umgehen. Solche Apps lassen sich mittlerweile problemlos installieren und nutzen, auch ohne tiefere technische Kenntnisse. Zwar sind DNS-Sperren regelmäßig angewandte

Maßnahmen, allerdings dürften diese nur eingeschränkt auf eine zuverlässige Sperrung hinwirken. Es würde sich lohnen, noch einmal die Geeignetheit dieser Maßnahmen zu überprüfen.

Hinsichtlich der Erweiterung des Kreises der Empfänger personenbezogener Daten auf ausländische öffentliche Stellen im Entwurf zu § 9 Abs. 3a GlüStV ergeben sich Abweichungen in der Einschätzung zu § 4b GlüStV-E, soweit personenbezogene Daten übermittelt werden sollen. Der Verweis auf die Begründung zu § 4b hinsichtlich der Verhältnismäßigkeit von § 9 wird den Unterschieden zwischen den Normen nicht gerecht.

In § 9 des Entwurfs werden Datenaustauschbefugnisse nicht wie in § 4b des Entwurfs an einen konkreten Verarbeitungszweck, sondern an die in der Norm ausdrücklich nicht abschließend aufgeführten, allgemeinen Aufgaben der Glücksspielaufsicht geknüpft. Die Datenschutzkonferenz erkennt nicht, dass § 4b des Entwurfs möglicherweise auch deswegen isoliert enger gefasst ist als § 9, da es sich bei den Voraussetzungen der Konzessionsgewährung um eine Berufszugangsbeschränkung im Sinne von Art. 12 des Grundgesetzes handeln kann, während § 9 überwiegend die Berufsausübung regelt. Dennoch ist der mit dem Datenaustausch verbundene Grundrechtseingriff bei Maßnahmen nach § 9 regelmäßig nicht weniger einschneidend. Dies gilt insbesondere vor dem Hintergrund, dass § 4b Abs. 2 explizit nur die Abfragebefugnis regelt, während der Begriff „Datenaustausch“ eine umfangreichere Verarbeitung nahelegt und generalklauselartigen Charakter hat. Jedenfalls fehlt es insofern an einer Legaldefinition des Begriffs „Datenaustausch“, was Rechtsunsicherheit im Hinblick auf die im Rahmen der Novelle geplanten Datenverarbeitungen schafft. Aus hiesiger Sicht liegt hier insofern ein Wertungswiderspruch zu § 4b vor.

Die relative Unbestimmtheit der möglichen Anlässe für Datenübermittlungen in § 9 GlüStV-E im Vergleich zu § 4b GlüStV-E hat aber auch Auswirkungen auf die Befugnis zur Übermittlung personenbezogener Daten in Drittländer.

Vorgelagerte Voraussetzung für jede Übermittlung ist auf erster Stufe – also vor jeglicher Prüfung einer Datenübermittlung in Drittländer – auch in diesem Fall das Vorliegen der Tatbestandsvoraussetzungen der Rechtsgrundlage nach Art. 6 DS-GVO nebst einem feststehenden, legitimen Übermittlungszweck (vgl. Art. 5 Abs. 1 Buchst. b) DS-GVO), an den auch die empfangende Stelle – z. B. bei der Festlegung geeigneter Garantien im Sinne von Art. 46 DS-GVO – gebunden werden kann.

Dies gilt besonders für Fälle von Art. 49 DS-GVO, bei denen die Übermittlungszwecke aufgrund der spezifischen, auf zweiter Stufe zu prüfenden und über die Kriterien der ersten Stufe hinausgehenden Übermittlungserfordernisse – hier insbesondere zur Wahrung des Ausnahmecharakters solcher Übermittlungen – besonders scharf umrissen werden müssen.

Nach den oben zitierten Ausführungen des Europäischen Datenschutzausschusses ist gerade eine enge Zweckfestlegung als Teil einer restriktiven Praxis konstitutiv dafür, dass eine Drittlandübermittlung ausnahmsweise denkbar sein kann. Der Entwurf gibt allerdings, anders als § 4b des Entwurfs, gerade keine solche eng definierten Zwecke vor. Durch die derzeitige Formulierung

der Norm, durch die solche Übermittlungen jeder anderen Form der Auskunftseinholung gleichgestellt werden, werden die Normanwender vielmehr dazu bestimmt, von der Möglichkeit der Übermittlung in Drittländer ohne Angemessenheitsbeschluss ohne Rücksicht auf ihren Ausnahmecharakter Gebrauch zu machen. Es obliegt dem Normgeber, bereits in der Norm selbst den Ausnahmecharakter solcher Übermittlungen klarzustellen, um rechtswidrige Datenübermittlungen zu verhindern.

Die Datenschutzkonferenz hält es daher für dringend geboten, den mit dem § 9 Abs. 3 a GlüStV-Entwurf vorgesehenen Datenaustausch mit den dort genannten Behörden hinsichtlich Tatbestandsvoraussetzungen und Rechtsfolge, einschließlich einer Nennung der konkreten jeweils zur Übermittlung bzw. zum Empfang befugten Behörde und des jeweiligen Zwecks, normenklar im Sinne der Wesentlichkeitstheorie zu regeln. Für die erforderlichen technisch-organisatorischen Vorkehrungen sollte auf die entsprechenden Normen der DS-GVO verwiesen werden. Dasselbe gilt für die Darlegungslast des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO. Im Übrigen gelten die Ausführungen zu § 4b Abs. 2 S. 2 f. des Entwurfs (Nr. 1) entsprechend.

Abschließend wird darauf hingewiesen, dass entsprechende Übermittlungen zur Verfolgung von Ordnungswidrigkeiten einschließlich bestimmter Maßnahmen im Vorfeld den Voraussetzungen der aufgrund der Richtlinie (EU) 2016/680 ergangenen Normen unterliegen, welche eine Übermittlung der dann besonders schutzbedürftigen personenbezogener Daten weiter einschränkt.

Soweit ersichtlich, besitzt keiner der sonstigen Änderungsbefehle datenschutzrechtlichen Gehalt.