

An den  
Landtagsklub der SPÖ  
Landtagsklub der KPÖ Plus  
Landtagsklub Die Grünen

Chiemseehof  
5020 Salzburg

per E-Mail an Herrn Klubdirektor Dr. Dominik Öllerer  
[dominik.oellerer@salzburg.gv.at](mailto:dominik.oellerer@salzburg.gv.at)

Mödling, 27. April 2024

Sehr geehrte Damen und Herren!

Ich beziehe mich auf die E-Mail vom 26. und 30. März 2024 von Herrn Klubdirektor Dr. Öllerer. Sie haben mir aus Anlass des Urteils des EUGH vom 16.01.2024 einige Fragen betreffend parlamentarischer Kontrolltätigkeit vorgelegt und mich beauftragt, diese näher zu erörtern.

Ich erstatte nachstehende

## **Rechtsgutachten.**

# **Die Anwendbarkeit der DSGVO auf parlamentarische Kontrollrechte**

Mir wurden im Zusammenhang mit dem Urteil des EuGH vom 16. Jänner 2024, Rs C-33/22, betreffend ein Vorabentscheidungsersuchen durch den Verwaltungsgerichtshof, mehrere Fragen gestellt, die allfällige Konsequenzen für Kontrollrechte im Salzburger Landtag zum Inhalt haben. In der Folge beantworte ich diese Fragen in der mir vorgegebenen Reihenfolge:

**Frage 1: Ist das Urteil des EuGH vom 16.01.2024, RS C-33/22, vor dem Hintergrund des in diesem Verfahren entschiedenen Sachverhalts einschlägig?**

Das zitierte Urteil des EuGH (in der Folge: „Urteil“) beantwortet einige Fragen, die sich für die Anwendung der DSGVO auf parlamentarische Kontrollrechte (im vorliegenden Fall: Untersuchungsausschüsse) ergeben. Das Urteil des EuGH ist zweifellos für den hier vorliegenden Zusammenhang einschlägig.

**Frage 2: Ist das nachgelagerte Pseudonymisieren (Schwärzen) von Akten der Interpellation (konkret Anfragen) durch die Landtagsdirektion zulässig? Welche rechtlichen Grundlagen kommen derzeit bei einer Anonymisierung von Anfragen und Anfragebeantwortungen durch die Landtagsdirektion zur Anwendung?**

Hier ist zunächst die Frage zu beantworten, wer für die Pseudonymisierung von Daten zuständig ist; gemäß Artikel 4 Z 7 DSGVO ist dies der Verantwortliche. Darunter ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Datenverarbeitung entscheidet, zu verstehen. Nach dem letzten Satz des Artikel 4 Z 7 kann das Recht der Mitgliedsstaaten einen bestimmten Verantwortlichen benennen. Solange das nicht der Fall ist, ist davon auszugehen, dass der Begriff des Verantwortlichen weit gefasst ist und sowohl

natürliche und juristische Personen, Behördeneinrichtungen oder sonstige Stellen erfasst. Entscheidend ist die Entscheidungsmacht. Demnach ist Verantwortlicher der oder die Stelle, die über die wesentlichen Aspekte der Mittel der Verarbeitung entscheidet (vgl. *Hödl*, Rz 83 zu Artikel 4 DSGVO in *Knyrim* [Hrsg] Praxiskommentar zum Datenschutzrecht – DSGVO und DSG).

Im vorliegenden Zusammenhang muss davon ausgegangen werden, dass das geltende nationale Recht keinen spezifischen Verantwortlichen bestimmt und daher auch die Frage, wer eine Pseudonymisierung von Daten vorzunehmen hat, offenlässt.

In Bezug auf parlamentarische Interpellationen wird man davon ausgehen müssen, dass eine allfällige Datenverarbeitung durch das Kollegialorgan Landtag erfolgt. Gemäß Artikel 4 Z 2 DSGVO erfolgt die Datenverwendung im Zusammenhang mit parlamentarischen Interpellationen durch das Kollegialorgan Landtag, das daher als Verarbeiter von Daten anzusehen ist. Daher ist der Landtag verantwortlicher Datenverarbeiter und hat eine allfällige Pseudonymisierung vorzunehmen (vgl. das Urteil des EUGH 9. Juli 2020, Rs C-272/19, in dem der EUGH einen Landtagsausschuss als „Verantwortlichen“ gem Art 4 Z 7 qualifiziert hat).

Dies bedeutet, dass die Beantwortung der Frage, welche Daten zu pseudonymisieren sind, durch Beschluss des Landtages zu erfolgen hat; da die DSGVO unmittelbar anwendbares Unionsrecht darstellt, sind diese Beschlüsse in nicht öffentlicher Sitzung zu verfassen. Gemäß § 14 des Landtags-Geschäftsordnungsgesetzes hat der Präsident des Landtages das Recht der Eröffnung und Zuteilung aller an den Landtag gelangenden Geschäftsstücke. Gemäß Absatz 4 ist der Präsident für die Einhaltung der Geschäftsordnung verantwortlich. Man wird daher davon ausgehen müssen, dass der Präsident des Landtages parlamentarische Anfragen, die an diesen gerichtet werden, in einer nicht öffentlichen Sitzung (§ 27 Abs 6) auf die Tagesordnung zu setzen hat und für einen Beschluss über eine allfällige Pseudonymisierung hinzuwirken hat. Da der Landtag als Verantwortlicher gemäß Artikel 4 Z 7 DSGVO anzusehen ist, hat eine Pseudonymisierung von diesem entschieden zu werden .

Eine schwierige Frage stellt sich dann, wenn der Landtag Beschlüsse fasst, die nach Auffassung des Präsidenten nicht der DSGVO entsprechen. Gemäß § 14 Abs 6 der Landtags-Geschäftsordnung hat der Präsident schriftliche Ausfertigungen, die vom Landtag ausgehen, zu unterzeichnen; er kann diese Unterzeichnung in einem von ihm zu bestimmenden Umfang dem Landtagsdirektor übertragen. Damit stellt sich die Frage, ob der Präsident des Landtages (oder der Landtagsdirektor) befugt ist, Beschlüsse des Landtages betreffend die Pseudonymisierung inhaltlich zu überprüfen und die Unterfertigung von Dokumenten zu verweigern, wenn er zum Ergebnis kommt, dass eine Verletzung der DSGVO gegeben ist.

Ein derartiges inhaltliches Prüfungsrecht ist abzulehnen; der Landtagspräsident hat sich vielmehr auf eine formale Prüfung in dem Sinn zu beschränken, dass er mit seiner Unterschrift beurkundet, dass eine Ausfertigung die gefassten Beschlüsse oder Dokumente richtig wiedergibt. Dies gilt in gleicher Weise für die Landtagsdirektor.

Zusammenfassend ist also festzuhalten, dass der Landtag für die Einhaltung der Datenschutzregelungen verantwortlich ist; da der Landtag ein Organ des Landes Salzburg ist, ist sein Handeln im Sinne der DSGVO dem Rechtsträger Land zuzuordnen. Das Land ist damit letztverantwortlich.

Festzuhalten ist auch, dass eine Pseudonymisierung lediglich dann erforderlich ist, wenn Ausfertigungen veröffentlicht werden, dh den Landtag verlassen. Im Innenverhältnis wird eine solche Pseudonymisierung nicht angebracht sein. Dafür spricht insbesondere der Erwägungsgrund 4 zur DSGVO (in der Folge kurz: „Erwägung“). In diesem Erwägungspunkt wird unter anderem ausgeführt, dass das Recht auf Schutz der personenbezogenen Daten „kein uneingeschränktes Recht“ ist; es müsse vielmehr im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Ausdrücklich genannt wird dabei unter anderem die „Informationsfreiheit“.

Nun ist zwar richtig, dass ein Landtag keine Grundrechte haben kann, dessen ungeachtet gehört die parlamentarische Kontrolle zu den wesentlichen Aufgaben parlamentarischer Demokratien; sie zählt damit zu den grundlegenden Werten der Europäischen Union gemäß Artikel 2 EUV. In der Literatur wird der Wert der „Demokratie“ darin gesehen, „dass alle Hoheitsgewalt in Willen des Volkes fundiert sein muss“ (Obwexer, Rz 25 zu Artikel 2 EUV in Jaeger/Stöger [Hrsg] Kommentar zu EUV und AEUV – mit weiteren Nachweisen).

Dies bedeutet, dass die Bestimmungen der DSGVO so auszulegen und anzuwenden sind, dass eine effektive Kontrolle der Vollziehung durch die parlamentarische Körperschaft möglich bleibt. Da sich die Kontrolle der Vollziehung notwendigerweise auf menschliches Verhalten bezieht, müssen die Betroffenen offen gelegt werden; dies gilt ebenso für Personen, auf die sich das Verhalten der Vollzugsorgane bezieht. Da die Transparenz staatlicher Vorgänge für ein demokratisches System von hoher Relevanz ist, wird eine Geheimhaltung nur in besonderen Fällen statthaft sein (vgl Erwägung 4). Sie darf eine effektive politische Kontrolle nicht beeinträchtigen. Im gegebenen Zusammenhang ist darauf hinzuweisen, dass gemäß Artikel 23 Abs 1 lit h DSGVO nationale Regelungen zulässig sind, die eine effektive Kontrolle ermöglichen.

**Frage 3: Liegen nach der DSGVO geschützte Daten auch dann vor, wenn diese zwar personenbezogen, aber nicht geheim sind, etwa weil sie aus öffentlichen Registern abfragbar sind oder bereits in anderen Quellen (Medien) genannt wurden? Geht es bereits dann um personenbezogene Daten im Sinn der DSGVO, wenn die Person nicht konkret genannt wird, aber eine Rückführbarkeit auf sie etwa durch die Erwähnung einer bestimmten Einlagezahl und der Katastralgemeinde im Grundbuch gegeben ist, wobei auch hier zu berücksichtigen ist, dass die Information über Grundstücksnummer und Einlagezahl öffentlich und kostenlos für alle zugänglich sind (SAGIS)?**

**3.1. Besteht ein Schutz nach der DSGVO auch dann, wenn im Namen einer juristischen Person der Name einer natürlichen Person vorkommt, und zwar für diese natürliche Person? Gilt die DSGVO auch**

**für juristische Personen wie etwa Firmen, wenn diese in ihrer Bezeichnung den Namen einer natürlichen Person tragen (z. B. Glock, McDonald's oder Mayr-Melnhof-Forstverwaltung, Friesacher GmbH)?**

### **3.2. Wo sind in einer parlamentarischen Anfrage die Grenzen der „Rückführbarkeit“ von Informationen (Daten) auf Einzelne?**

Hier ist zunächst festzuhalten, dass die Verfassungsbestimmung des Artikel 1 DSG bestimmt, dass allgemein verfügbare Daten nicht dem Datenschutz unterliegen, weil diese Daten nicht geheim gehalten werden können und daher auch kein schutzwürdiges Interesse an einer Geheimhaltung bestehen kann (vgl. *Eberhard*, Rz 46 zu § 1 DSG in *Korinek/Holoubek/ua* [Hrsg] Österreichisches Bundesverfassungsrecht). Die Verfassungsbestimmung des § 1 DSG gilt auch nach Inkrafttreten der DSGVO unverändert weiter. Die Ausnahme vom Geheimhaltungsschutz für allgemein verfügbare Daten findet sich in der DSGVO nicht explizit, ergibt sich aber aus dem Zusammenhang zwischen den Ziffern 2 und 7 des Artikel 4 DSGVO. Der durch Artikel 1 DSGVO normierte Datenschutz für natürliche Personen bedeutet Schutz vor Datenverarbeitung im Sinn des Artikel 4 Z 2. Wenn Artikel 4 Z 7 die Verantwortlichkeit dessen, der über die Verarbeitung von personenbezogenen Daten entscheidet, begründet, so heißt das, dass eine solche Verantwortung nur für die Verarbeitung geheimer Daten bestehen kann, da nur geheime Daten ein Schutzbedürfnis begründen. Die gegenteilige Auffassung von *Lachmayer* (Rz 112 zu Artikel 1 DSGVO in *Knyrim aaO*) ist daher unzutreffend.

Zu beachten ist aber, dass eine Verknüpfung allgemein verfügbarer Daten eine neue Datenqualität begründet und daher die Frage aufwirft, ob an diesen verknüpften Daten ein schutzwürdiges Interesse besteht. Als Beispiel sei genannt, dass ein Grundstückseigentümer über das Grundbuch allgemein leicht feststellbar ist; daher kann an der Geheimhaltung insoweit kein schutzwürdiges Interesse bestehen. Wird allerdings die Frage gestellt, welche Grundstücke im Eigentum einer bestimmten Person bestehen, so handelt es sich möglicherweise um eine Vielzahl einzelner und für sich jeweils allgemein verfügbarer Daten, die Verknüpfung ist aber nicht mehr allgemein verfügbar. Hier ist grundsätzlich ein

schutzwürdiges Interesse anzunehmen, das im jeweiligen Zusammenhang mit entgegenstehenden Interessen (vgl zB Artikel 23 Abs 1 DSGVO) abgewogen werden muss. Als Beispiel sei dazu auf § 6 Grundbuchsumstellungsgesetz verwiesen, nach welcher Bestimmung eine Abfrage des Personenverzeichnisses beschränkt ist.

Datenschutz im Sinne der DSGVO besteht zunächst für identifizierte Personen, das sind Personen, deren Identität aus der Information direkt abgeleitet werden kann. Personenbezogene Daten im Sinne der DSGVO liegen aber auch dann vor, wenn eine natürliche Person identifizierbar ist (Artikel 4 Z 1 DSGVO). Identifizierbarkeit ist dann gegeben, wenn eine natürliche Person aus einer bestimmten Information nicht unmittelbar ableitbar ist, aber durch eine Verknüpfung mit anderen Informationen festgestellt werden kann. Eine solche Identifizierbarkeit liegt zB dann vor, wenn in einer Information der Eigentümer eines bestimmten Grundstückes nicht namentlich genannt wird; diesfalls ergibt sich aus der Information allein die betroffene Person nicht, sie kann aber leicht durch eine Grundbuchsabfrage ermittelt werden. Artikel 4 Z 1 spricht im gegebenen Zusammenhang von „Zuordnung zu einer Kennung wie einem Namen ...“. Ist die betroffene Person identifizierbar, so handelt es sich um personenbezogene Daten.

Die Frage, wann eine Identifizierbarkeit gegeben ist, ist Gegenstand erheblicher literarischer Kontroversen (vgl dazu insb *Hödl* in *Knyrim* aaO, Rz 12ff zu Art 4 DSGVO). Aus den Erwägungsgründen 26 sind nur allgemeine Kriterien ableitbar, nach denen die Auslegung zu erfolgen hat. Es ist zu prüfen, ob eine andere Person „nach allgemeinem Ermessen wahrscheinlich“ die Mittel benützen wird, die für eine Identifizierung in Betracht kommen. Dabei ist insbesondere auch zu beurteilen, wie schwierig die Identifizierung ist und mit welchen Kosten und mit welchem Zeitaufwand sie verbunden ist. Auch die verfügbare Technologie und technologischen Entwicklungen sind zu berücksichtigen. Dies bedeutet: je schwieriger eine Identifizierung ist, je höher der Kosten- und Zeitaufwand ist, desto eher wird man eine Identifizierbarkeit verneinen, umgekehrt gilt: wenn eine Identifizierbarkeit leicht möglich ist, wird man die Identifizierbarkeit bejahen müssen und das Vorliegen personenbezogener Daten anzunehmen haben.

Zu beachten ist, dass die DSGVO einen Datenschutz ausschließlich für natürliche Personen gewährleistet. Dies ergibt sich klar aus Artikel 1 Abs 1 DSGVO, wo es heißt, dass die DSGVO „Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ...“ enthält. In den Erwägungen 14 wird dies ausdrücklich nochmals betont und auch festgehalten, dass die DSGVO „nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person“ gilt.

Hier besteht ein Unterschied zum DSG, das einen Datenschutz für „jedermann“ begründet (§ 1 Abs 1 DSG-Verfassungsbestimmung; vgl auch *Eberhard*, Rz 25 zu § 1 DSG aaO). Der Umstand, dass die DSGVO lediglich einen Datenschutz für natürliche Personen normiert, schließt nicht aus, dass der nationale Gesetzgeber auch juristische Personen in den Datenschutz einbezieht; dies freilich nur nach bestehenden nationalen Regelungen. In diesem Zusammenhang sei auch auf Artikel 8 Grundrechte-Charta hingewiesen, nach welcher Bestimmung „jede Person ... das Recht auf Schutz der sie betreffenden personenbezogenen Daten“ hat. Die Auslegung dieser Bestimmung – insbesondere die Frage, ob mit „jede Person“ auch juristische Personen umfasst sind – ist umstritten (vgl dazu zB *Riesz*, Rz 48 ff zu Artikel 8 GRC in *Holoubek/Lienbacher*, Charta der Grundrechte der Europäischen Union<sup>2</sup> [2019]). Als Zwischenergebnis ist festzuhalten, dass die DSGVO auf juristische Personen nicht anwendbar ist und daher deren personenbezogene Daten nicht schützt; durch nationales Recht kann aber ein solcher Schutz begründet werden, wie dies etwa § 1 DSG vorsieht. „Personenbezogene Daten“ juristischer Personen sind also gemäß nationalem Recht grundsätzlich in gleicher Weise geschützt wie personenbezogene Daten natürlicher Personen.

**Frage 4: Ist das genannte Urteil des EuGH dahingehend zu verstehen, dass alle der Staatsfunktion Gesetzgebung zuzurechnenden Akte grundsätzlich dem Anwendungsbereich der DSGVO unterstehen und ist dies nach Art des Akts zu differenzieren (Wortmeldung, Anträge, Anfragen, Petitionen, Ausschussveröffentlichungen, stenographische Protokolle, Ladung von**

**Auskunftspersonen, Landtagsverwaltung, Personalangelegenheiten, Verzeichnisse der Abgeordneten, Transparenzvorschriften udgl). Und die Nutzung welcher – neben den im Urteil genannten Öffnungsklauseln der DSGVO - kann vom Landes(verfassungs-)gesetzgeber in diesem Zusammenhang angestrebt werden?**

Die DSGVO differenziert nicht nach Staatsfunktionen oder nach der Zurechnung von Akten und auch nicht nach deren Art. Dies bedeutet, dass die DSGVO grundsätzlich für sämtliche Staatstätigkeiten Anwendung zu finden hat (vgl. EuGH 16. Jänner 2024, Rs C-33/32, Rz 43); dies freilich nur für solche Anwendungen, die in den Anwendungsbereich des Unionsrechtes fallen. Für die Rechtmäßigkeit der Datenverarbeitung (Artikel 4 Z 2) enthält Artikel 6 DSGVO eine Reihe alternativer Voraussetzungen. Im gegebenen Zusammenhang ist insbesondere Artikel 6 lit c und lit e von Relevanz. Nach Artikel 6 Abs 1 lit c ist die Verarbeitung von Daten dann rechtmäßig, wenn sie „zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt“, ist. Dies bedeutet, dass eine Datenverarbeitung immer dann zulässig ist, wenn sie für eine Aufgabe erfolgt, „die im öffentlichen Interesse liegt ...“.

Aus den zitierten Bestimmungen des Artikel 6 Abs 1 ergibt sich somit klar, dass der Landtag befugt ist, Daten zu verarbeiten, die er für die Erfüllung seiner Aufgaben, insbesondere auch für die Kontrolle der Verwaltung, benötigt. Es handelt sich dabei um gesetzliche Verpflichtungen, die auch im öffentlichen Interesse liegen.

Artikel 6 Abs 2 sieht vor, dass durch die nationale Gesetzgebung der Mitgliedsstaaten Vorschriften „zur Anpassung“ erlassen werden können. Hier besteht ein weiter Spielraum. Auch Artikel 23 Abs 1 sieht die Zulässigkeit nationaler Regelungen zum Beispiel dann vor, wenn diese zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses notwendig und verhältnismäßig sind (Artikel 23 Abs 1 lit e DSGVO). Auch Artikel 23 Abs 1 lit h gestattet nationale Regelungen zur Beschränkung von Verpflichtungen, die sich aus der DSGVO ergeben, wenn dies zum Zweck der Kontrolle, Überwachung öffentlicher Gewalt notwendig und verhältnismäßig ist.

**Frage 5: Überwiegt das öffentliche Interesse an der parlamentarischen Kontrolle (Interpellation) und deren Ergebnisse sowie deren Publizität die Interessen von Einzelnen, insbesondere Personen, die selbst in der Öffentlichkeit stehen?**

**5.1. Wann überwiegt das, der parlamentarischen Interpellation immanente, Interesse der Information der Öffentlichkeit jenes von Einzelnen auf Datenschutz?**

Hier ist festzuhalten, dass eine rechtmäßige Datenverarbeitung nach den vorhin genannten Kriterien jedenfalls zulässig ist, was bedeutet, dass der Landtag als Verantwortlicher von diesen Daten Kenntnis nehmen kann. Eine andere Frage ist, ob und inwieweit diese Daten auch veröffentlicht werden dürfen. Nach der DSGVO wird hier zu unterscheiden sein, ob der Zweck zum Beispiel der parlamentarischen Kontrolle nur erreichbar ist, wenn bestimmte personenbezogene Daten auch veröffentlicht werden. Hier wird man allenfalls differenzieren müssen und personenbezogene Daten solcher Personen, die nur am Rande des Geschehens stehen, geheim zu halten haben, während eine Veröffentlichung von Daten von Personen, die im Zentrum des Kontrollzwecks stehen, zulässig sein kann. Wann das Eine oder das Andere der Fall ist, kann allgemein nicht beantwortet werden; stets geht es um die Notwendigkeit und Verhältnismäßigkeit einer Veröffentlichung zur Erfüllung einer gesetzlichen Verpflichtung oder einer im öffentlichen Interesse liegenden Aufgabe.

Als Beispiel sei das Urteil des EuGH vom 09.11.2010, verbundene Rechtssachen C-92/09 und C-93/09, genannt; in diesem Urteil führt der EuGH zunächst aus, dass „die Verletzung des Rechts auf personenbezogene Daten ... bei juristischen Personen ein anderes Gewicht als bei natürlichen Personen ...“ hat. Gemeint hat der EuGH, dass juristische Personen weniger Geheimhaltungsschutz genießen als natürliche Personen (vgl dazu auch die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 25.01.2012 KOM [2012] 9 endgültig, Punkt 3).

Im zitierten Urteil hat der EuGH mehrfach ausgesprochen, dass die „bestmögliche Verwendung öffentlicher Mittel“ eine besondere Bedeutung hat und daher eine weitgehende Veröffentlichungspflicht anzunehmen ist. Daraus ist abzuleiten, dass in den Fällen, in denen es um die Verwendung öffentlicher Mittel geht, die Schutzwürdigkeit des Geheimhaltungsinteresses in der Regel geringer zu bewerten ist als das öffentliche Interesse an der Veröffentlichung.

**Frage 6: Inwiefern kann der Schutzzweck des Art. 57 B-VG (Erhaltung der Funktionsfähigkeit des Parlaments gegen Eingriffe durch die Verwaltung) im Wege der Nutzung von Öffnungsklauseln der DSGVO abgesichert werden?**

**6.1. Welche Öffnungsklauseln (Art 23 DSGVO, Bestimmungen zu Archiven, etc.) können genutzt werden, damit die (Kontroll-)Rechte der Abgeordneten und deren Immunität sowie das berechnigte Interesse der Öffentlichkeit an Transparenz der Regierungs- und Landtagsarbeit, gesichert sind?**

Hier ist zunächst zu betonen, dass für die Verarbeitung von Daten im Bereich des Landtages der Landtag zuständiges Organ ist und eine allfällige Schwärzung oder Anonymisierung von Daten durch den Landtagsdirektor unzulässig ist. Dies bedeutet, dass die Daten, die die Mitglieder des Landtages benötigen, um ihrer gesetzlichen Verpflichtung und der Erfüllung ihrer Aufgabe nachkommen zu können, ihnen jedenfalls zur Verfügung stehen müssen. Eine davon zu unterscheidende Frage ist, ob und inwieweit diese Daten auch veröffentlicht werden dürfen. Hier wird es möglicherweise nicht-öffentliche Sitzungen der Gremien geben müssen, in denen der Landtag (ein Ausschuss des Landtages) über eine allfällige Anonymisierung entscheidet. Ich verweise in diesem Zusammenhang nochmals auf Artikel 6 Abs 2 DSGVO.

**Frage 7: Wie kann eine Einschränkung der für die Staatsfunktion und demokratiepolitisch unbedingt erforderlichen parlamentarischen Kontrolle, insbesondere das Interpellationsrecht durch die DSGVO hintangestellt werden? Dabei ist zu berücksichtigen, dass die verfassungsgesetzlichen**

**werden? Dabei ist zu berücksichtigen, dass die verfassungsgesetzlichen Aufgaben ohne Kenntnis der dazu relevanten personenbezogenen Daten nicht wahrgenommen werden können (vgl. grundlegend auch VfSlg. 19.973/2015) und ein grundlegendes öffentliches Interesse an den Anfragegegenständen besteht.**

In diesem Zusammenhang ist wiederholend festzuhalten, dass die DSGVO kein uneingeschränktes Recht auf Schutz der personenbezogenen Daten normiert (vgl. die Erwägungsgründe 4). Dies bedeutet, dass allfällige Geheimhaltungsinteressen mit anderen Grundrechten und Freiheiten, wie zB auch mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit abgewogen werden müssen (vgl. so schon VfSlg 19.973). Dies bedeutet weiters, dass einem Parlament zur Ausübung der parlamentarischen Kontrolle alle Daten zur Verfügung gestellt werden müssen, die dieses Parlament benötigt, um seiner Aufgabe in öffentlichem Interesse nachkommen zu können.

Dies bedeutet aber nicht, dass das Parlament alle Daten, die ihm zur Verfügung stehen, öffentlich machen darf. Das Parlament hat als „Verantwortlicher“ (Art 4 Z 7 DSGVO) zu prüfen, inwiefern die Bekanntgabe, der ihm zur Verfügung stehenden personenbezogenen Daten an die Öffentlichkeit im öffentlichem Interesse erforderlich ist, um den Kontrollzweck zu erreichen; dabei ist eine Abwägung zwischen allfälligen Geheimhaltungsinteressen und dem öffentlichen Interesse an der Bekanntgabe von Kontrollergebnissen – unter Einbeziehung personenbezogener Daten – vorzunehmen. Wenn das öffentliche Interesse an der Bekanntgabe dieser Daten an die Öffentlichkeit zur Erreichung des Kontrollzwecks erforderlich ist, darf sie auch erfolgen. Diese Abwägung kann für verschiedene Personen auch verschieden ausfallen. Daher werden die Geheimhaltungsinteressen von Personen, die gleichsam im Zentrum des überprüften Sachverhalts stehen, eher geringer zu bewerten sein als die Bekanntgabe personenbezogener Daten solcher Personen, die nur am Rande eine Rolle spielen. Die Abwägung muss daher stets differenziert erfolgen und den Grundsatz des Gebots der Verhältnismäßigkeit beachten.

**Frage 8: Wer ist für die Veröffentlichung von im Salzburger Landtag gestellten parlamentarischen Anfragen im Sinne der DSGVO verantwortlich? Ist die Rechtsprechung des VfGH, VfSlg 19.112/2010 diesbezüglich anwendbar?**

Als Verantwortlicher für die Datenverarbeitung ist der Salzburger Landtag anzusehen. Dies ergibt sich klar aus Art 4 DSGVO und entspricht auch der Entscheidung, die der Verfassungsgerichtshof im Jahr 2010 in VfSlg 19.112 getroffen hat. Der Salzburger Landtag hat daher sowohl bei der Frage der Veröffentlichung einer parlamentarischen Anfrage wie auch bei seiner Berichterstattung abzuwägen, ob und inwieweit personenbezogene Daten veröffentlicht werden. Eine Befugnis des Landtagsdirektors diese Abwägung vorzunehmen und über die Veröffentlichung zu entscheiden, besteht nicht.

**Frage 9: Wie können die Abgeordneten vor einer die Ausübung des freien Mandats und der Sicherung der Meinungsfreiheit einschränkenden Inanspruchnahme durch „Einschüchterungsklagen“ effektiv geschützt werden?**

Einen spezifischen Schutz gegen Einschüchterungsklagen sieht die Rechtsordnung derzeit nicht vor. Pläne für eine Neuregelung sind nicht bekannt. Erscheint einem Beklagten die vom Kläger vorgenommene Bewertung des Streitgegenstandes zu hoch, so kann er dies gem § 7 RATG bei der ersten mündlichen Tagatzung bemängeln und eine Herabsetzung des Streitwertes durch das Gericht erreichen (vgl auch § 60 JN). In der Praxis der letzten Jahre scheinen Beklagte mit diesen Bestimmungen den Zweck von solchen Einschüchterungsklagen erfolgreich abgewehrt zu haben.

