Bayerisches Landesamt für
Datenschutzaufsicht

Ansbach, den 3. März 2017

Pressemitteilung

Vorstellung des 7. Tätigkeitsberichts 2015/2016

Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA), Thomas Kranig, hat heute im Museum für Kommunikation in Nürnberg den neuen Tätigkeitsbericht des BayLDA für die Jahre 2015 und 2016 in Nürnberg der Öffentlichkeit vorgestellt. In dem Bericht werden neben einer umfangreichen statistischen Auswertung der Arbeit des BayLDA exemplarische Fälle aus den letzten beiden Jahren dargestellt und ein Ausblick auf das kommende neue Datenschutzrecht gegeben.

Der Tätigkeitsbericht gibt auf 158 Seiten einen Überblick über die Arbeit der Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich in Bayern. Detaillierte statistische Angaben (S. 12), Berichte über anlasslose, das heißt nicht aufgrund von Beschwerden durchgeführte Prüfungen und Kontrollen (S. 21), sowie die Darstellung zahlreicher exemplarischer Fälle aus den unterschiedlichsten Bereichen (S. 35) geben Einblick in die tägliche Arbeit der Aufsichtsbehörde.

Das BayLDA ist für ca. 700.000 verantwortliche Stellen im nicht-öffentlichen Bereich (d. h. Unternehmen, Vereine, Verbände, freiberuflich Tätige etc.) in Bayern zuständig.

Die Vorstellung des Tätigkeitsberichts erfolgte im Raum „Netzwelten" des Museums für Kommunikation, in dem für die Besucher die Themen, mit denen die Datenschutzaufsichtsbehörde sich im Zusammenhang mit dem Internet befasst, aus einer ganz anderen Warte sehr plakativ und informativ dargestellt sind.

Einige Kernpunkte des Tätigkeitsberichts sind in dem folgenden Überblick enthalten. Der vollständige Tätigkeitsbericht kann ab heute von jedem Interessierten auf unserer Webseite heruntergeladen werden:

www.lda.bayern.de/media/baylda_report_07.pdf

Thomas Kranig
Präsident

Anschrift
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

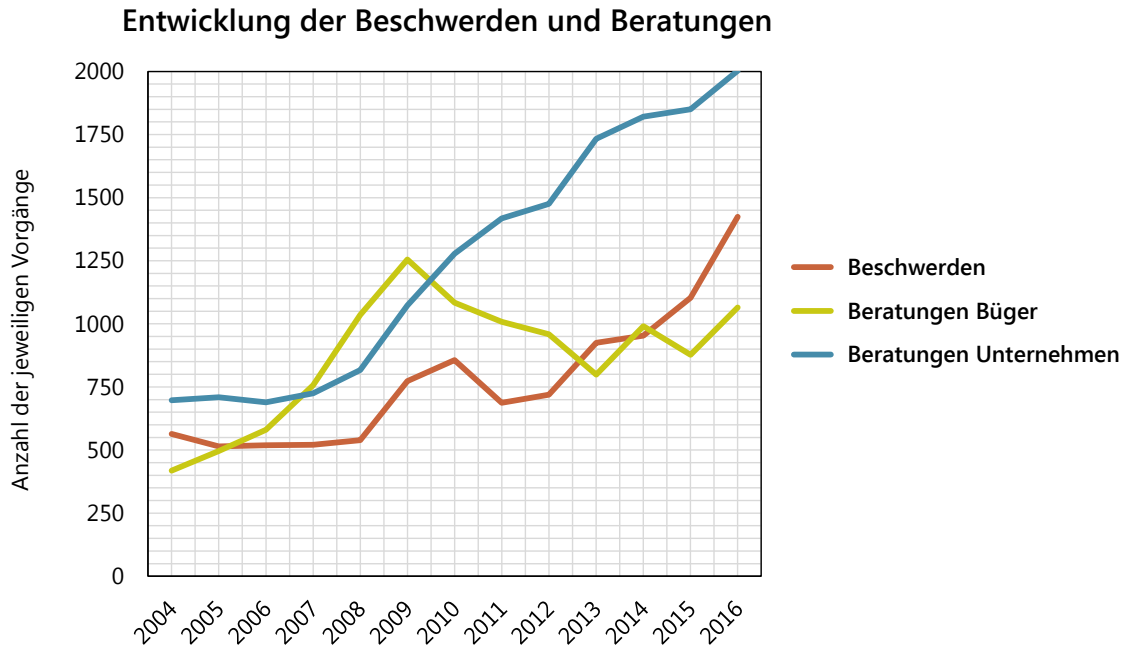
Telefon +49 (0) 981 53 1300
Telefax +49 (0) 981 53 98 1300
E-Mail presse@lda.bayern.de
Webseite www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien

Überblick über den 7. Tätigkeitsbericht für 2015/2016

I. Allgemeines zur Statistik

Als bayerische Datenschutzaufsichtsbehörde sind wir für ca. 700.000 verantwortliche Stellen im nicht-öffentlichen Bereich (d. h. Unternehmen, Vereine, etc.) in Bayern zuständig. In den letzten Jahren haben sich nicht nur die Beratungsanfragen dieser Stellen gehäuft, sondern auch die bei uns eingehenden Datenschutzbeschwerden von Betroffenen. Wir konnten feststellen, dass es sich dabei nicht nur um einen kurzfristigen Trend, sondern – gerade in Bezug auf die vergangenen Jahre – um eine nachhaltige Entwicklung handelt. Der Verlauf kann den nachfolgenden Grafiken entnommen werden:

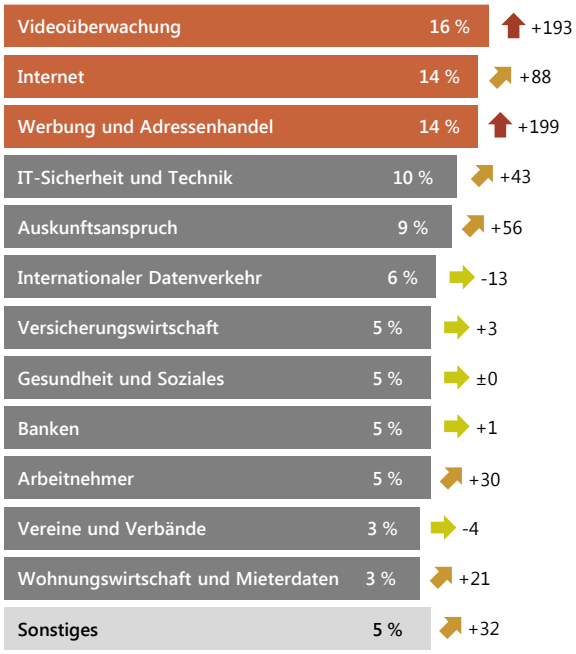


Statistik im Vergleich zum vorherigen Berichtszeitraum

	2013	2014	2015	2016	Tendenz
Beschwerden	925	953	1103	1424	↑
Beratungen Bürger	799	991	877	1065	↗
Beratungen Unternehmen	1733	1821	1850	2003	↑
Bußgeldverfahren	53	64	94	79	↗
Datenpannen	32	21	28	85	↑

- **Grund für Steigerung der Beratungsanfragen und Beschwerden:**
  Die Steigerung des Beratungs- und Beschwerdeeingangs mag darin liegen, dass wir durch unsere intensive Vortragstätigkeit und Öffentlichkeitsarbeit bekannter geworden sind.

- **Begründetheit der Beschwerden:**
  Wir sind fast allen Beschwerden nachgegangen. Bei etwa der Hälfte der Beschwerden war eine Datenschutzverletzung festzustellen, die in aller Regel auch eine Ordnungswidrigkeit darstellt. Aus Kapazitätsgründen wurden nur in Ausnahmefällen Bußgeldverfahren eingeleitet.

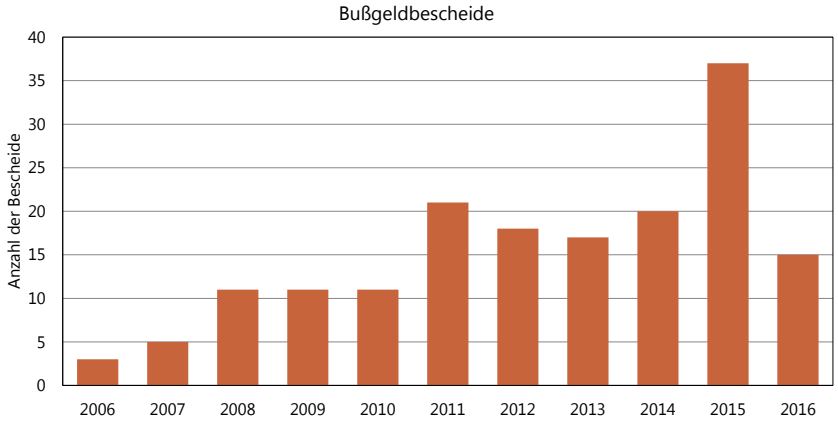


- **Themen der Beschwerden:**
  Bei den Themen der Beschwerden liegt Videoüberwachung mittlerweile an der ersten Stelle. Ursache dafür sind zum einen die sehr preiswerten Überwachungskameras, sog. Wildkameras, Dashcams usw., und auf der anderen Seite ein gesteigertes Sicherheitsbedürfnis durch Videoüberwachung, die nicht nur (zulässigerweise) auf das eigene Grundstück, sondern (in aller Regel unzulässig) auf angrenzende Grundstücke oder öffentliche Verkehrsflächen erstreckt wird.

- **Bearbeitungsdauer:** Nach der DS-GVO (Art. 78) kann in Zukunft jeder Beschwerdeführer, der nicht innerhalb von drei Monaten von der Aufsichtsbehörde über den Stand oder das Ergebnis seiner Beschwerde in Kenntnis gesetzt wurde, gegen die Aufsichtsbehörde bei Gericht klagen. Um einzuschätzen, ob und inwieweit wir diese Voraussetzungen schon heute erfüllen, haben wir erstmals die Laufzeiten unserer Beschwerdebearbeitung erfasst und veröffentlicht.

Dauer	25%	25%	25%	25%
Beschwerden	4 Tage	14 Tage	52 Tage	141 Tage
Beratungen Bürger	1 Tag	3 Tage	11 Tage	36 Tage
Beratungen Unternehmen	3 Tage	19 Tage	47 Tage	122 Tage

- **Bußgeldbescheide:**
  Wegen erheblicher Arbeitsbelastung durch andere Aufgaben musste die Zahl der eingeleiteten Bußgeldverfahren auf gravierende Fälle beschränkt werden. Dies wird sich in Zukunft, auch um die Vorgaben des neuen Datenschutzrechts zu erfüllen, ändern müssen.

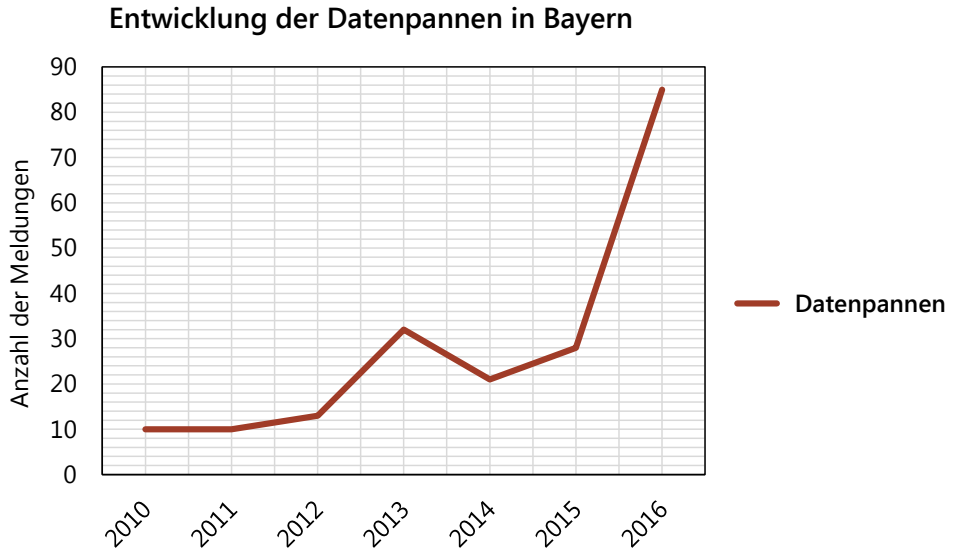


- **Personalausstattung:**
  Die oben genannten Aufgaben wurden in den Jahren 2015 und 2016 von 17 Mitarbeiterinnen und Mitarbeitern, für die das BayLDA über 16 Planstellen verfügt, erfüllt. Für die nächsten beiden Jahre hat der Bayerische Haushaltsgesetzgeber dem BayLDA vier neue Stellen und damit insgesamt 20 zuerkannt (gegenüber sieben neuen Stellen für den Bayer. Landesbeauftragten für den Datenschutz, d. h. die Datenschutzbehörde für den öffentlichen Bereich in Bayern, wodurch diesem 38 Stellen für 2017 und 41 Stellen für 2018 zur Verfügung stehen).

II. Einzelne Themenbereiche

1. Hacking-Angriffe in Bayern

Eine zentrale Vorschrift im Datenschutzrecht ist die Meldung von Sicherheitsvorfällen, umgangssprachlich „Datenpannen" genannt. Bislang sieht das Bundesdatenschutzgesetz in § 42a BDSG eine Meldepflicht solcher Datenpannen vor, wenn insbesondere zwei Voraussetzungen erfüllt sind: Die betroffenen personenbezogenen Daten sind zum einen sehr sensibel – z. B. Bankdaten, Patientendaten oder schlecht gesicherte Passwörter – und es drohen zum anderen zusätzlich schwerwiegende Beeinträchtigungen für die betroffenen Personen.



Während sich klassische Datenpannenszenarien wie *Verlust*, *Diebstahl* oder *Fehlversendung* im Berichtszeitraum 2015/2016 eher im gleichbleibenden Umfang ereigneten bzw. uns mitgeteilt wurden, haben wir gerade im Bereich *Cybercrime* einen starken Anstieg in Bayern registriert. Immer häufiger werden Unternehmen gezielt Opfer von Attacken. Folgende Kategorien von Vorfällen ergaben sich dabei insbesondere:

- **Hacking von Webseiten** mit Nutzerdaten, um mit den erbeuteten Daten der Nutzer z. B. Identitätsdiebstahl oder Kreditkartenbetrug zu betreiben. Wir hatten hierbei mehrere Fälle, bei denen Nutzerdaten im fünf oder gar sechsstelligen Bereich von Unternehmen gestohlen wurden. Dass es auch zu noch größeren Ausmaßen kommen kann, hat der Vorfall bei Yahoo gezeigt (bis zu 1 Milliarde gestohlener Nutzerkonten weltweit).

- **Sicherheitslücken bei Webshops** konnten wir ebenso vermehrt feststellen. In manchen Fällen wurden diese Lücken von Angreifern ausgenutzt, um Schadcode zum Abfangen von Bankdaten der Webseitennutzer heimlich im jeweiligen Webshop zu platzieren.

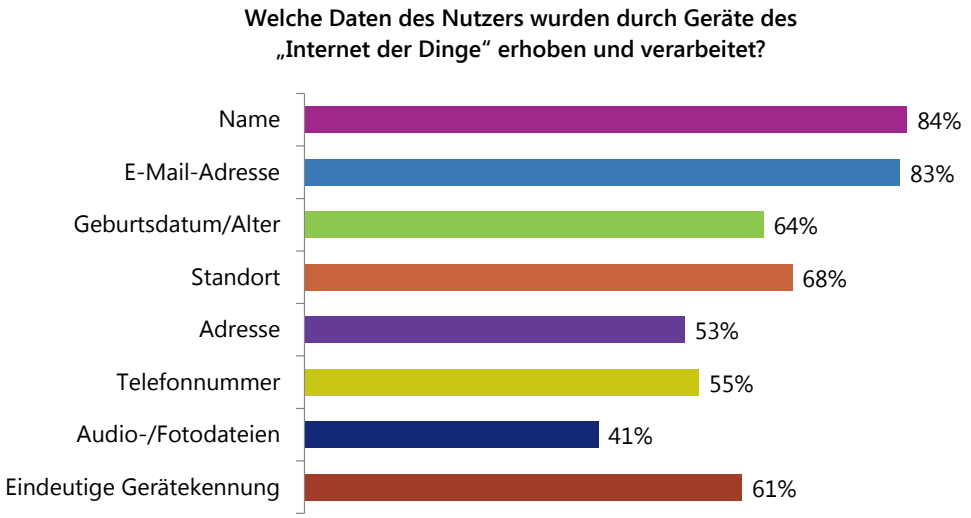
- **Verschlüsselungstrojaner und Malware** fanden zuletzt vermehrt Verbreitung. Auch in unserer Zuständigkeit haben sich Unternehmen solchen Schadcode eingefangen, konnten dann nicht mehr arbeiten und wurden zur Zahlung von Lösegeld aufgefordert.

In Zusammenarbeit mit dem Bayerischen Landesamt für Verfassungsschutz und der Polizei haben wir zum einen mehrfach Informationsveranstaltungen für Unternehmen durchgeführt, um auf die Gefahren hinzuweisen und deutlich zu machen, wer bei welchen Angriffen der zuständige Ansprechpartner in Bayern ist. Das BayLDA ist neben der o. g. Bearbeitung bei Meldungen von Datenpannen einerseits zuständig, präventiv Unternehmen zu beraten und bei festgestellten Mängeln im Rahmen von Kontrollen Unternehmen auch zu zwingen, angemessene Sicherheitsstandards vorzuhalten. Soweit dem nicht freiwillig Rechnung getragen würde, haben wir entsprechende Anordnungen erlassen, die dann doch alle befolgt wurden. Klagen dagegen wurden nicht erhoben.

2. Vernetzung im Alltag

Wir hatten zuletzt verstärkt mit der Vernetzung von Alltagsgegenständen zu tun. So haben wir 2016 einerseits an einer globalen Prüfung zum Thema „Internet of Things" teilgenommen, anderseits aber auch selbst eine Datenschutzprüfung von sog. „Wearables", d. h. Smart Watches und Fitness-Armbändern, angestoßen.

- **Internet of Things (IoT)**
  Bei unserer IoT-Prüfung war festzuhalten, dass ein Großteil der Datenschutzbestimmungen von smarten Geräten keine oder nur unzureichende Informationen über den Umgang mit den personenbezogenen Daten des Nutzers enthält. Alle geprüften Geräte hatten eine erhebliche Menge an persönlichen Daten gesammelt und diese oft zu gezielten Nutzerprofilen zusammengefügt.



- **Wearables**

  Unsere Prüfung von Wearables ergab, dass die untersuchten Smart Devices durchwegs Datenschutzmängel hatten. Obwohl die Geräte zum Teil äußerst sensible Daten der Nutzer wie Herzfrequenz, Körpertemperatur oder Schlaf- und Aktivitätsrhythmus verarbeiten, bleiben wesentliche Datenschutzaspekte unberücksichtigt. Durchgängig fehlte es an der Transparenz über die Datenverarbeitungsvorgänge, so dass Nutzer eigentlich nicht wissen können, welche Daten von ihnen zu welchem Zweck erhoben und an wen übermittelt werden.

- **Connected Cars**

  Da wir für zwei bayerische Automobilkonzerne datenschutzrechtlich zuständige Aufsichtsbehörde sind, haben wir auch regelmäßig mit neu aufkommenden Fragestellungen zu vernetzten bzw. „intelligenten" Fahrzeugen zu tun. So hatten wir bspw. einen Fall, bei dem in einem Strafverfahren die Fahrzeugdaten den betroffenen Fahrer belasteten und nachwiesen, dass der Fahrer mit deutlich überhöhter Geschwindigkeit innerorts unterwegs war. Unsere Prüfung der Datenaufzeichnungen im Auto ergab, dass neben der Geschwindigkeit weitere Daten wie die GPS-Positionen des Fahrzeugs detailliert erfasst wurden.

3. Neue Versicherungsmodelle

Im Freistaat Bayern sitzen einige sehr relevante Versicherungsunternehmen, die sich im Beratungsweg an uns gewandt haben, um unsere Einschätzung zu verhaltensabhängigen Versicherungsmodellen zu erfahren. Dabei ging es einerseits um die Bewertung des Fahrverhaltens für Tarifmodelle der Kraftfahrtversicherung und andererseits um gesundes Verhalten bzw. gesunde Ernährung in Verbindung mit privaten Krankenversicherungsverträgen. Unsere Beratung ging im Wesentlichen in die Richtung, dass Versicherungsgesellschaften sehr transparent machen müssen, welche Daten der Versicherten von welcher Gesellschaft zu welchem Zweck erhoben und wie lange sie gespeichert werden. Wenn insoweit die entsprechenden Voraussetzungen gegeben sind, haben wir diese Tarifmodelle unter datenschutzrechtlichen Gesichtspunkten nicht als unzulässig bewertet. Ob derartige Modelle gesellschaftspolitisch wünschenswert sind oder nicht, war dabei nicht Gegenstand unserer datenschutzrechtlichen Überprüfung.

III. Die Datenschutz-Grundverordnung (DS-GVO)

Am 25. Mai 2016 ist die Datenschutz-Grundverordnung als in allen Mitgliedstaaten der Europäischen Union unmittelbar geltendes Recht in Kraft getreten. Wirksam wird sie zwei Jahre später, das heißt am 25. Mai 2018. Bis zu diesem Zeitpunkt haben alle Unternehmen und auch Aufsichtsbehörden Zeit, sich zu überlegen, was die neuen Anforderungen bedeuten und sich darauf einzustellen.

Selbst wenn viele Grundprinzipien des Datenschutzes unverändert weitergelten, werden insbesondere für die IT-Sicherheit in Zukunft deutlich strengere Anforderungen bestehen. Daneben müssen die Unternehmen im Umgang mit den Betroffenenrechten, d. h. dem Recht auf Auskunft, Berichtigung, Löschung usw. Prozesse vorhalten, um die entsprechenden Ansprüche zeitnah erfüllen zu können. Auch schon relativ geringe Verletzungen des Datenschutzes und der Datensicherheit sind in Zukunft den Aufsichtsbehörden zu melden. Ein ganz wesentlicher

neuer Grundsatz ist, dass Unternehmen, die mit personenbezogenen Daten umgehen, nachweisen müssen, dass sie dies rechtmäßig und sicher machen. Diese Beweislastumkehr wird eine große Herausforderung.

Bezüglich der betrieblichen Datenschutzbeauftragten wird es in Zukunft dabei bleiben, dass dann, wenn in einem Unternehmen ständig mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein Datenschutzbeauftragter zu bestellen ist. Neu ist, dass alle Datenschutzbeauftragten der Aufsichtsbehörde gemeldet werden müssen. Dies werden wohl auch in unserem Zuständigkeitsgebiet einige tausend Meldungen sein, die entgegengenommen und verarbeitet werden müssen.

Wir Aufsichtsbehörden sind gehalten, die Zusammenarbeit auf europäischer Ebene deutlich zu verstärken und gemeinsam sicherzustellen, dass das neue Datenschutzrecht in Europa auch gegenüber international tätigen Unternehmen, insbesondere denen, deren Geschäftsmodell im Wesentlichen auf der Vermarktung personenbezogener Daten beruht, einheitlich und konsequent angewendet wird. Dazu stehen den Aufsichtsbehörden in Zukunft bei Datenschutzverstößen Sanktionsmöglichkeiten von bis zu 20 Millionen bzw. 4 % des Weltjahresumsatzes als Geldbuße zur Verfügung.

Die Aufsichtsbehörden sind momentan dabei, durch Erarbeitung gemeinsamer Papiere auf europäischer Ebene sich darauf zu verständigen, wie die neuen Vorschriften zu verstehen und zu vollziehen sind. Aufsichtsbehörden sollen nach dem neuen Rechtsvorschriften zertifizieren, Codes of Conduct begleiten, Standardvertragsklauseln für den internationalen Datenverkehr vorgeben, bei riskanten Datenverarbeitungen und entsprechenden Anfragen innerhalb von acht Wochen eine schriftliche Begutachtung abgeben, Datenschutzprüfungen vornehmen, Beschwerden von Bürgern bearbeiten, alle Bürger, Unternehmen, staatliche Stellen und die Öffentlichkeit beraten und nicht zuletzt in der Regel alle Datenschutzverstöße **wirksam, verhältnismäßig und abschreckend**, wie es Art. 83 Abs. 1 DS-GVO ausdrücklich vorgibt, sanktionieren.

Eine wahre Herausforderung, der wir uns mit den Ressourcen, die uns der Haushaltsgesetzgeber zuteilt, stellen werden.