Netzwerk Datenschutzexpertise GbR
Dr. Thilo Weichert
Waisenhofstr. 41
D-24103 Kiel
Tel.: +49 431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

Landtag von Baden-Württemberg
Ausschuss für Inneres, Digitalisierung und Migration
Vorsitzender Herrn MdL Karl Klein
Konrad-Adenauer-Straße 3

70173 Stuttgart

Kiel, den 30.05.2018

**Stellungnahme zum Entwurf der Landesregierung für ein „Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679“ vom 19.04.2018, LT-Drs. 16/3930**
Anhörung im Landtag am 04.06.2018; Ihre Einladung vom 16.05.2018, Az. I/2.5

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für Ihre in der Bezugszeile genannte Einladung, der ich, wie schon mitgeteilt, gerne nachkomme. Zu dem im Betreff genannten Gesetzentwurf nehme ich vorab schriftlich Stellung:

Hintergrund des Gesetzentwurfs ist die Anpassung des allgemeinen Datenschutzrechts des Landes Baden-Württemberg an das europäische Recht, insbesondere an die Europäische Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 v. 27.04.2016, ABl. L 119 v. 04.05.2016, S. 1 ff. (DSGVO), die vom 25.05.2018 an direkt anwendbar ist.

## 1 Allgemeines

Der Regierungsvorschlag verwendet bei der **Benennung der Datenschutz-Grundverordnung** durchgängig, ebenso wie der Bundesgesetzgeber, deren bürokratische Bezeichnung „Verordnung (EU) 2016/679“. Dadurch wird der ohnehin schon komplexe und schwer verständliche Normentext für Laien noch schwerer nachvollziehbar. Der bayerische Gesetzgeber nimmt dem gegenüber im Gesetz einmal eine Quellenangabe vor (Art. 2 BayDSG) und verwendet dann die Bezeichnung bzw. das Kürzel „DSGVO“ (vgl. BayLT-Drs. 17/19628 v. 12.12.2017). Auch die Verwendung des ausgeschriebenen Namens „Datenschutz-Grundverordnung“ ist bürgerfreundlicher und verständlicher. Ein solches Vorgehen wurde vom niedersächsischen Gesetzgeber gewählt (§ 1 Abs. 1 S. 1 NDSG, vgl. NdsLT-Drs. 18/548 v. 28.03.2018). Ein entsprechendes Vorgehen ist für die Bezeichnung der „Richtlinie (EU) 2016/680“ sinnvoll, die z. B. als „Datenschutzrichtlinie Polizei-Justiz“ oder „DSRl-JI“ bezeichnet werden könnte. Das Problem der Verständlichkeit zeigt sich exemplarisch bei der umständlichen und unleserlichen Regelung des § 2 Abs. 4 LDSG-E, der den Anwendungsbereich von DSGVO und DSRl-JI näher festlegt.

Der Entwurf beschränkt sich weitgehend auf eine Umsetzung der DSGVO. Fast zeitgleich mit der DSGVO ist auch die **Richtlinie (EU) 2016/680** „zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ (ABl. EU v. 04.05.2016, L 119/89, künftig zitiert als DSRl-JI)

anwendbar. Der Bundesgesetzgeber sowie viele Landesgesetzgeber haben statt einer getrennten eine gemeinsame Gesetzgebung vorgezogen. Möglich sind beide Vorgehensweisen. Es bedarf einer Umsetzung der Richtlinie (EU) 2016/680 auf Landesebene. Die Anwendung des Rechts setzt voraus, dass der Anwender zwischen dem Anwendungsbereich der DSGVO und der DSRl-JI zu unterscheiden in der Lage ist. Eine Aufnahme dieser Unterscheidung im bereichsspezifischen Recht, z. B. im Polizeirecht sowie in einem spezifischen Justizdatenschutzrecht, würde die Anwendbarkeit erleichtern.

In Deutschland wird bisher nicht versucht, die inhaltliche Umsetzung der DSGVO-Regelungen im bereichsspezifischen Recht vorzunehmen. Dies hat zur Folge, das oft Regeln aus drei Ebenen anzuwenden sind: 1. DSGVO, 2. umsetzende allgemeine nationale oder Landesnormen, 3. bereichsspezifisches Recht. Das BDSG bzw. die Landesdatenschutzgesetze (LDSG) werden zu einer Art **Scharnierrecht**, in dem oft lediglich die Öffnungsklauseln der DSGVO paraphrasiert werden. Dieses Vorgehen wurde z. B. vom Bund für die Umsetzung der DSRl-JI in den §§ 45 ff. BDSG gewählt. Auf solches Mehrebenenrecht sollte, soweit dies gesetzestechnisch möglich ist, verzichtet werden.

Erfreulich am vorliegenden Gesetzentwurf ist, dass er die sog. **Spezifizierungs- bzw. Öffnungsklauseln** der DSGVO zumeist korrekt umsetzt und die dort vorgesehenen Abwägungsklauseln im mitgliedstaatlichen Recht abbildet. Zudem wird von den durch diese Öffnungsklauseln ermöglichten Regelungsoptionen zurückhaltend Gebrauch gemacht, so dass der Flickenteppich unterschiedlicher Regelungen in Deutschland nicht unnötig vergrößert wird und dabei die europäischen Vorgaben in datenschutzwidriger Weise strapaziert werden. Damit hebt sich der vorliegende Entwurf positiv vom Bundesrecht und vielen (teilweise noch nicht abschließend behandelten) Landesgesetzen ab.

Zu begrüßen ist weiterhin, dass der Entwurf das **bisherige Regelungskonzept des LDSG** mit dem neuen Recht der DSGVO so verbindet, dass Anwender des Datenschutzrechtes bei der Umsetzung des neuen Rechts an ihre bisherigen Erfahrungen anknüpfen können.

Es ist zu bedauern, dass die Gesetzesvorschläge, ebenso wie sämtliche sonstigen bekannten Entwürfe zur Anpassung bzw. Umsetzung des europäischen Datenschutzrechts **keinerlei innovative Elemente** enthalten und sich auf für notwendig erachtete Regelungen beschränken. Seit den 70er Jahren war das deutsche Landesdatenschutzrecht international Vorreiter, etwa mit dem weltweit ersten Datenschutzgesetz von Hessen im Jahr 1970 oder mit dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) aus dem Jahr 2000 (vgl. dazu unten unter 4).

Wegen des äußerst umfangreichen Gesetzentwurfes beschränken sich die weiteren Bemerkungen auf besonders **hervorzuhebende Aspekte**.

## 2 Zu den einzelnen Regelungen des Entwurfes eines Landesdatenschutzgesetzes (LDSG-E)(Art. 1)

Zu § 1 LDSG-E

Die Regelung sollte ergänzend die Definition der „Datenschutz-Grundverordnung“ oder der „DSGVO“ als **Kurzbezeichnung** übernehmen, die im weiteren Gesetz dann anstelle der Bezeichnung „Verordnung (EU) 2016/79“ verwendet wird (s. o. 1).

Zu § 2 Abs. 7 LDSG-E

Die Regelung, dass die „Ausübung des **Begnadigungsrechts**“ vollständig aus dem Anwendungsbereich des LDSG angenommen ist, ist problematisch, aber wohl hinnehmbar

angesichts des Umstands, dass die DSGVO vollständig anwendbar bleibt. In der Begründung wäre ein Hinweis hierauf dringend nötig.

Zu § 6 Abs. 1 Nr. 2 LDSG-E

Die Regelung erlaubt die zweckändernde **Übermittlung personenbezogener Daten an nichtöffentliche Stellen** schon bei der Darlegung eines „berechtigten Interesses". Diese unbestimmte Regelung ist zu weitgehend und eröffnet für die Betroffenen nicht kontrollierbare Gefährdungen ihrer informationellen Selbstbestimmung. Es wird angeregt, eine Übermittlung nur bei Vorliegen eines „rechtlichen Interesses" zu erlauben. Soweit darüber hinausgehend Übermittlungen an Private erlaubt werden sollen, sollte dies bereichsspezifischem Recht überlassen bleiben.

Zu § 6 Abs. 3 LDSG-E

Gemäß Art. 5 Abs. 2 DSGVO bleibt die Verantwortung für eine **Datenübermittlung im automatisierten Abrufverfahren** bei der übermittelnden Stelle und kann nicht auf dem Empfänger abgewälzt werden. Zur Sicherstellung der Verantwortlichkeit und der Zweckbindung beschränkt sich der Entwurf auf eine nicht näher präzisierte Verpflichtung zu einem „geeigneten Stichprobenverfahren". Dies genügt den Anforderungen der Art. 5 Abs. 2, 32 Abs. 1, 2 DSGVO nicht. Es bedarf einer Konkretisierung der Maßnahmen zur Sicherstellung von Verantwortlichkeit, Zweckbindung bzw. generell eines angemessenen Schutzniveaus bei dieser Art der Übermittlung.

Zu § 7 Abs. 1 S. 3-7 LDSG-E

Die Regelung zur **Datenverarbeitung in der gemeinsamen Dienststelle** ist nicht mit dem Konzept der DSGVO in Einklang zu bringen, das Arbeitsteilung lediglich in Form einer Auftragsverarbeitung (Art. 28 DSGVO) oder als gemeinsame Verantwortlichkeit vorsieht. Die Regelung zur „gemeinsamen Dienststelle" knüpft an handelnde Einzelpersonen an und nicht an rechtliche Einheiten (öffentliche Stellen). Die Begründung enthält keine weiteren Erläuterungen. Es muss in jedem Fall sichergestellt werden, dass die in Satz 6 vorgesehene „gemeinsame interne Dienstanweisung" den Anforderungen des Art. 28 Abs. 3 DSGVO genügt.

Zu § 12 Abs. 2 Nr. 2 LDSG-E

Gemäß der Regelung, die u. a. auf § 5 Abs. 1 Nr. 3 LDSG-E verweist, ist eine **zweckändernde Übermittlung bei Berufsgeheimnissen** schon erlaubt für Zwecke der „Verhütung" von „Ordnungswidrigkeiten von erheblicher Bedeutung" sowie auch für die Verfolgung und Vollstreckung solcher Rechtsverstöße. Die äußerst unbestimmte Regelung ermöglicht die Durchbrechung von Berufsgeheimnissen in unverhältnismäßiger Weise. Als Erheblichkeitsschwelle sollte zumindest der Verdacht oder die Gefahr einer „schwerwiegenden Ordnungswidrigkeit" vorliegen. Berufsgeheimnisse dienen nicht nur dem Schutz des Geheimnisträgers, sondern vorrangig den Patienten, Mandanten bzw. sonstigen betroffenen Hilfesuchenden. Die Zustimmung des Geheimnisträgers ist nicht geeignet, diesen Schutzzweck zu überspielen.

Zu § 13 LDSG-E

Die **Forschungsklausel** zeichnet sich – gegenüber anderen entsprechenden Klauseln im deutschen Recht – durch eine Beschränkung auf europarechtlich vorgegebene Konditionen aus und stellt insofern keine übermäßige Beeinträchtigung von Forschungsprojekten dar, die in mehreren Bundesländer oder grenzüberschreitend durchgeführt werden. Anstelle der Fortsetzung des bestehenden Regelungschaoses mit einer Vielzahl von Forschungsklauseln

im allgemeinen und spezifischen Bundes- und Landesrecht ist es wünschenswert, über einen Bund-Länder-Staatsvertrag in Deutschland ein einheitliches Forschungsrecht festzuschreiben, das auch der Sensitivität von Daten nach Art. 9 Abs. 1 DSGVO gerecht wird.

Die geplante Regelung berücksichtigt nicht, dass etwa im medizinischen Bereich wichtige Forschungsprojekte nur durchgeführt werden können, wenn eine Offenbarungsbefugnis zu **Berufsgeheimnissen**, also z. B. zur ärztlichen Schweigepflicht, mit entsprechenden Sicherungen vorgesehen ist (vgl. Art. 9 Abs. 3 DSGVO). So behindert die geplante Regelung weiterhin unangemessen die Durchführung medizinischer Forschungsprojekte (Art. 5 Abs. 3 GG, Art. 13 Europäische Grundrechte-Charta - GRCh). Nur über eine einheitliche bundesweite Regulierung können die in Art. 89 DSGVO geforderten Garantien praktikabel realisiert werden. Ein problemadäquater Vorschlag für eine Bund-Länder-Regulierung unter Berücksichtigung von Berufsgeheimnissen zumindest für medizinische Forschungsprojekte liegt seit September 2017 vor und sollte von Bund und Ländern umgehend in Angriff genommen werden (https://www.netzwerk-datenschutzexpertise.de/dokument/medizinische-forschung-und-datenschutz).

Zu § 14 LDSG-E

Es sollte geprüft werden, ob und inwieweit die Regelung zur **Verarbeitung für Archivzwecke** im Interesse einer höheren Anwendungsfreundlichkeit nicht im Landesarchivrecht geregelt werden kann (s. o. 1 generell zum spezifischen Recht).

Zu § 15 LDSG-E

Die Regelung zur Verarbeitung bei Dienst- und Arbeitsverhältnissen ist zu begrüßen. Im Interesse größtmöglicher Einheitlichkeit im deutschen Recht und zwecks normativer Klarstellung sollte der Regelungsgehalt des § 26 Abs. 3 BDSG (neu) mit einer Präzisierung der Anforderungen an **Einwilligungen im Beschäftigungsverhältnis** übernommen werden.

Analog zu § 26 Abs. 7 BDSG sollte, da insofern die DSGVO nicht direkt anwendbar ist, klargestellt werden, dass diese und die Landesregelungen zum Beschäftigungsdatenschutz auch gelten, wenn Daten nicht in einem Dateisystem, also insbesondere in **Akten**, verarbeitet werden.

Zu § 16 LDSG-E

Gegen eine gewisse Privilegierung der Verarbeitung für Zwecke **öffentlicher Auszeichnungen und Ehrungen** ist nichts einzuwenden. Diese wird durch eine strenge Zweckbindung kompensiert. Verfassungsrechtlich nicht akzeptabel und ein klarer Verstoß gegen Art. 8 Abs. 2 S. 2 GRCh ist aber der vollständige und ohne Kompensationen erfolgende Ausschluss des Auskunftsrechtes.

Zu § 17 LDSG-E

Eine Rechtsgrundlage für die Überprüfung von Personen, die „in **sicherheits- oder sicherheitstechnisch relevante Bereiche** gelangen sollen“, ist grds. zu begrüßen. Was unter diese Bereiche fallen soll, ist aber unklar; die verwendete Begrifflichkeit ist für sich selbst zu unbestimmt. Es bedarf eines normativ festgelegten förmlichen Verfahrens der Bestimmung dieser Bereiche, bei dem die Grundrechte der Betroffenen berücksichtigt werden, wozu auch die Pressefreiheit gehört, soweit Journalisten betroffen sind. Hierbei sollten die Art der Überprüfung, die dabei beteiligten Stellen und die einbezogenen Datenkategorien präzisiert werden. Deren Festlegung kann nicht ausschließlich einer Einwilligung übertragen werden, deren Freiwilligkeit in vielen Fällen nicht gegeben ist.

Zu § 18 LDSG-E

Es wird vorgeschlagen – zusätzlich und über den Bereich der öffentlichen Stellen hinausgehend – eine **Meldepflicht von Videoüberwachung** im öffentlichen Raum auf einem Internet-Portal vorzusehen um zu gewährleisten, dass die Kombination von Videoüberwachung verschiedener Stellen nicht zur einer Totalüberwachung des öffentlichen Raums ausartet, und um die öffentliche Transparenz zu stärken.

Zu § 19 Abs. 3 LDSG-E

Die Regelung zur **Auskunft bei künstlerischer oder literarischer Offenlegung** greift zu kurz, indem sie lediglich ein Recht vorsieht, Auskunft zu verlangen. Vielmehr muss gemäß den Art. 15, 85 DSGVO eine Auskunft erteilt werden, soweit eine Verweigerung nicht erforderlich ist, „um die Freiheit der Meinungsäußerung und der Informationsfreiheit“ zu wahren. Dies gilt nicht nur bei der künstlerischen oder literarischen Offenlegung, sondern auch schon bei der einer Offenlegung vorausgehenden Speicherung von personenbezogenen Daten.

Zu § 22 Abs. 1 LDSG-E

Die Regelung, wonach der Landtag die Landesbeauftragte oder den Landesbeauftragten ohne Aussprache wählt, verstößt gegen das in Art. 53 Abs. 1 DSGVO Erfordernis eines „**transparenten Verfahrens“ bei der Benennung der Leitung der Aufsichtsbehörde**. Transparenz kann hergestellt werden durch eine Ausschreibung der Stelle sowie durch eine offizielle Anhörung der möglichen Kandidatinnen und Kandidaten. Auch gegen eine öffentliche Aussprache im Parlament über die Stellenbesetzung ist angesichts der hohen Bedeutung des Amtes nichts einzuwenden (dazu ausführlich Netzwerk Datenschutzexpertise, Zum Auswahlprozess von Datenschutzbeauftragten als Leitung der Aufsichtsbehörden, 03.02.2017, S. 5 ff.; https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi6.pdf).

Zu § 22 Abs. 3 LDSG-E

Trotz der sechsjährigen Amtszeit mit zweimaliger Wiederwahlmöglichkeit sollte auf die **Beschränkung der Wiederwahl** im Interesse einer höchstmöglichen Qualifikation verzichtet werden. Es steht dem Parlament jederzeit frei, eine Amtsinhaberin bzw. einen Amtsinhaber nicht wiederzuwählen.

Zu § 25 Abs. 4 LDSG-E

Die Regelung, die § 16 Abs. 1, 2 BDSG entspricht, ändert das Verfahren bei der Feststellung und Ahndung von Datenschutzverstößen. Bevor von der Datenschutzaufsicht Maßnahmen nach Art. 58 Abs. 2 lit. b-g, j DSGVO ergriffen werden, wird diese verpflichtet, den Verstoß der zuständigen **Rechts- oder Fachaufsicht anzuzeigen** und dort eine Stellungnahme anzufordern. Ein Grund für diese Verfahrensänderung ist nicht erkennbar. Diese Verfahrensregeln sind in der DSGVO nicht vorgesehen, beeinträchtigen die Datenschutzaufsicht in ihrer Unabhängigkeit und sind deshalb europarechtswidrig.

Zu § 25 Abs. 5 LDSG-E

Gegen eine Gleichbehandlung von **Notaren** mit Rechtsanwälten bei der Datenschutzkontrolle ist im Grundsatz nichts einzuwenden. Da jedoch § 29 Abs. 3 BDSG, gegen Art. 8 Abs. 3 Europäische Grundrechte-Charta verstößt, kann und darf § 29 Abs. 3 BDSG nicht angewendet werden. Der Wesensgehalt des § 29 Abs. 3 BDSG besteht darin,

dass ein Verantwortlicher eine Datenschutzkontrolle allein mit dem Hinweis auf eine Beeinträchtigung seines Berufsgeheimnisses verweigern kann. Zudem verstößt die Regelung auch gegen die durch nationales Verfassungsrecht vorgegebenen Anforderungen an eine unabhängige Datenschutzkontrolle. Auf die Regelung sollte vollständig verzichtet werden. Ein Konflikt zwischen dem Notargeheimnis und der Datenschutzkontrollkompetenz der Datenschutzaufsicht war in der Vergangenheit, während der keine solche Kontrolleinschränkung bestand, nicht erkennbar. Ein solcher Konflikt ist auch in der Zukunft unrealistisch und kann im Rahmen der geltenden Regelungen gelöst werden (ausführlich hierzu Schuler/Weichert, Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern nach § 29 Abs. 3 BDSG-neu ist grundrechtswidrig, netzwerk-datenschutzexpertise.de 22.05.2017).

## 3 Zu weiteren Gesetzesänderungen

Zu § 10a Abschiebungshaftvollzugsgesetz-E

Die Regelung, wonach „das Einrichtungsgebäude sowie das Innere des Einrichtungsgebäudes“ im Abschiebungshaftvollzug uneingeschränkt offen mittels Videotechnik überwacht werden kann, ist unverhältnismäßig und damit verfassungswidrig. Entgegen der in der Begründung genannten „engen Voraussetzungen zur Zulässigkeit“ sind diese weder im Entwurf noch in der Begründung erkennbar. Die Regelung erlaubt eine **visuelle Totalüberwachung** von Personen, die weder Straftäter noch Gefahrenpersonen sind. Eine Erforderlichkeit in diesem Ausmaß ist nicht begründet und nicht begründbar. Eine Abwägung mit Betroffeneninteressen findet bei der Beobachtung nicht statt. Selbst eine in Art. 35 DSGVO grds. vorgesehene Datenschutz-Folgenabschätzung soll nicht vorgenommen werden müssen.

## 4 Abschließende Bemerkung

Der Schutzgegenstand des Datenschutzrechts ist nach Art. 1 Abs. 1 DSGVO weiter als der reine Schutz des „Persönlichkeitsrechts“ (so bisher § 1 LDSG BaWü-alt), indem er generell auf „die Grundrechte und Grundfreiheiten natürlicher Personen“ verweist. Davon erfasst sind also auch der Schutz des Telekommunikationsgeheimnisses (Art. 7 GRCh), vor Diskriminierung (Art. 21 GRCh) und der Meinungs- und Informationsfreiheit (Art. 11 GRCh), das Recht auf Zugang zu Dokumenten (Art. 42 GRCh) sowie auch die Schutzrechte für Arbeitnehmer oder Verbraucher (Art. 27 ff., 38 GRCh) bei der Verarbeitung personenbezogener Daten. Die unabhängigen Aufsichtsbehörden können und dürfen sich also nicht auf ein enges Verständnis beschränken, sondern müssen bei ihrer Aufgabenbeschreibung einem **umfassenden Grundrechtsansatz** folgen, der auch gesellschaftliche Funktionen wie Demokratie, Gewaltenteilung und Solidarität mit einschließt. Diese umfassende Kontrollzuständigkeit ist von der kontrollierten Exekutive wie auch von der beaufsichtigten Privatwirtschaft zu respektieren.

Die zunehmende Digitalisierung von Verwaltung, Wirtschaft und Alltagsleben führt nicht nur zu einer Gefährdung der bestehenden Grundrechte, sondern begründet den Bedarf der Entwicklung neuer rechtlicher Instrumente. Mit einer „**Charta der Digitalen Grundrechte** der Europäischen Union“ wurde hierzu ein erster Diskussionsvorschlag vorgelegt (digitalcharta.eu). Dabei geht es auch um einen sozial und freiheitlich verträglichen Einsatz von Algorithmen sowie von auf sog. künstlicher Intelligenz basierenden Verfahren. Für die Regulierung und Kontrolle derartiger Verfahren bedarf es dem Gemeinwohl verpflichteter, wirtschaftlich und politisch unabhängiger Instanzen mit rechtlicher, technischer sowie sonstiger wissenschaftlicher Kompetenz und ausreichender Ausstattung. Für diese Funktion bietet sich der Ausbau der bestehenden Datenschutzaufsicht, die oft auch schon Aufgaben im Bereich der Informationsfreiheit wahrnimmt, an.

Es stünde einem technolgiefreundlichen Bundesland wie Baden-Württemberg gut an, insofern die Datenschutzaufsicht nicht nur personell und finanziell, sondern auch mit **zusätzlichen Aufgaben und Befugnissen** auszustatten. Kurzfristig kann dies darin bestehen, der Datenschutzaufsicht die Wahrnehmung der in Art. 40 DSGVO vorgesehenen Zertifizierung praktisch zu ermöglichen. Eine weitere – weitgehend kostenneutrale (weil über Fördergelder zu finanzierende) und zugleich innovationsfördernde – Aufgabe kann darin bestehen, die Datenschutzaufsicht mit der Durchführung von Forschungsprojekten im Bereich des digitalen Grundrechtsschutzes zu beauftragen. Eine solche Aufgabe wird seit ca. 2000 in Schleswig-Holstein vom dortigen Unabhängigen Landeszentrum für Datenschutz wahrgenommen.

Für Fragen stehe ich – insbesondere im Rahmen der in der Bezugszeile genannten Anhörung – gerne bereit.

Mit freundlichen Grüßen

Dr. Thilo Weichert