Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

ULD • Postfach 71 16 • 24171 Kiel

Deutscher Bundestag
Ausschuss für Kultur und Medien
Unterausschuss Neue Medien
Der Vorsitzende Sebastian Blumenthal
Platz der Republik 1

11011 Berlin

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Dr. Thilo Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -61.41/11.001

Kiel, 14. Oktober 2011

Stellungnahme zum Öffentlichen Expertengespräch zum Thema „Datensicherheit bei Facebook und anderen sozialen Netzwerken in Anbetracht einer Entschließung der Datenschutzbeauftragten der Länder und des Bundes“ am 24.10.2011, PLH E.800
Ihre Einladung vom 13.10.2011, Gz. PA 22/1

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

an dem im Betreff genannten Gespräch mit Sachverständigen nehme ich gerne teil. Gemäß Ihrer Bitte beantworte ich die von Ihnen gestellten Fragen:

Fragen der Koalitionsfraktionen CDU/CSU und FDP

1. Welche Möglichkeiten sehen Sie zukünftig, einen besseren Ausgleich zwischen Datenschutzinteressen und Funktionalitäten eines sozialen Netzwerkes zu schaffen? Wie bewerten Sie in diesem Zusammenhang die vom Heise Verlag initiierte sogenannte Zwei-Klick-Lösung?

Theoretisch besteht kein Widerspruch zwischen den Funktionalitäten sozialer Netzwerke und dem Datenschutz. In der Praxis gibt es jedoch ein Spannungsverhältnis, weil die datenschutzrechtlichen Anforderungen in Europa und Deutschland insbesondere von den Marktführern, die ihre Produkte aus den USA heraus anbieten, in einem großen Umfang nicht beachtet werden. Gesetzeskonformität lässt sich zunächst dadurch erreichen, dass der Grundsatz des „Privacy by Default“ realisiert wird, d. h. dass die Grundeinstellungen so vorgenommen werden, dass Funktionalitäten, die mit einer Offenbarung und Auswertung personenbezogener Daten verbunden sind, durch eine bewusste Handlung der Nutzenden freigeschaltet werden müssen. Weitere Voraussetzungen sind größtmögliche Transparenz über die erfol-

gende Datenverarbeitung für die Nutzenden vor den entsprechenden Freischaltungen, Informationen über die Risiken (Verantwortlichkeiten, z. B. Haftungsrisiken), Möglichkeiten des Widerspruchs sowie der Einsatz datenschutzfreundlicher Technik (Beachtung der Grundsätze der Erforderlichkeit und der Datensparsamkeit, Sicherung der Vertraulichkeit usw.).

Die Zwei-Klick-Lösung des Heise-Verlages ist ein Weg in die richtige Richtung. Mit ihr soll eine wirksame Einwilligung in eine Datenübermittlung an Facebook in die USA sowie die Nutzung der Daten zur Profilbildung über die Nutzung der Webangebote erteilt werden. Für die Rechtswirksamkeit der Einwilligungserklärung bedarf es einer vorherigen Information über Umfang, Verantwortliche und Zweck der Datenverarbeitung. Diese Informationen liegen derzeit aber weder dem Heise-Verlag noch den Nutzenden, und auch noch nicht den Datenschutzaufsichtsbehörden vor. Die durch Facebook zur Verfügung gestellte Datenschutzerklärung (Datenverwendungsrichtlinien) sind hinsichtlich dieser Anforderungen zu ungenau. Das ULD befindet sich in Kontakt mit Facebook, um technische Informationen über die Art und den Umfang der Datenverarbeitung in einer überprüfbaren Form zu erhalten.

> 2. Im Arbeitspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD) ist die Rede davon, dass der Diensteanbieter "aufgrund des tatsächlichen Einflusses den Prozess der Datenverarbeitung steuern" kann. Auch beim Einbinden von You-Tube-Videos werden durch HTML-Codes Daten von allen Besuchern der Webseite übertragen – unabhängig davon, ob diese dann das Video auch tatsächlich aufrufen. Berücksichtigt man den Umstand, dass bei jeder Verlinkung – seien es Webseiten oder Dienste – Nutzerdaten erhoben werden (wie z. B. IP-Adressen) – wäre dann nicht die logische Konsequenz, dass Webseitenbetreiber auf jegliche Links oder Dienste Dritter verzichten müssen, um eine Mithaftung auszuschließen?

Die rechtlichen Ausführungen und Schlüsse des ULD in seinem Arbeitspapier haben Implikationen, die weit über den Einsatz von Fanpages und Social-Plugins von Facebook hinausgehen. Vergleichbare Technik, wie bei der Einbindung von Social-Plugins, kommt auch bei Google mit seinen Angeboten (z. B. auch You Tube), ja auch bei Anbietern aus Deutschland zum Einsatz. Diese Technik ist nicht gleichzusetzen mit der Nutzung einfacher Links. Die Übermittlung von technisch notwendigen Informationen bei der Einbindung einfacher Links erfolgt erst, wenn der Nutzer willentlich diesen anklickt. Davon zu unterscheiden ist die ausgelöste Übermittlung bei in iFrames – das ist die hinter den Social-Plugins stehende Technologie – eingebundenen Elementen. Der Übermittlungsvorgang wird bereits bei dem Aufruf der jeweiligen Internetseite ausgelöst, auf der sich der Social-Plugin befindet. Der Nutzer kann nicht unmittelbar steuern, ob die Datenübermittlung erfolgt. Social-Plugins können wie eine Internetseite in der Internetseite verstanden werden. Der Nutzer weiß daher häufig nicht, mit welchen weiteren Diensteanbietern sich der Browser verbindet, wenn die originäre Seite aufgerufen wird.

Im Unterschied zum Setzen von Links findet häufig bei der direkten Einbindung von Drittinhalten wie die in der Frage erwähnten Youtube-Videos bei den SocialPlugins von Facebook oder dem +1-Button von Google bereits eine Datenverarbeitung auf Seiten von Youtube, Facebook oder Google statt. Der Nutzer einer Webseite, die solche Dritt-Inhalte eingebunden hat, kann zumeist nicht selbst entscheiden, ob er der Datenverarbeitung bei diesen Dritten zustimmt und erhält auch keine Informationen über die Zwecke der Datenverarbeitung.

Für die rechtliche Bewertung der Einbindung von Social-Plugins ist relevant, dass der einzelne Webseitenbetreiber datenschutzrechtliche (Mit-)Verantwortung für die Gestaltung der Seite und alle daraus resultierenden Datenverarbeitungsprozesse trägt. Nach den derzeit geltenden rechtlichen Vorgaben des deutschen Rechts handelt es sich bei der Einbindung von externen Inhalten über iFrames in der Regel um eine Auftragsdatenverarbeitung. Der Webseitenbetreiber nutzt Inhalte Dritter um sein eigenes Angebot auszugestalten und löst durch das Setzen des Plugins die Übermittlung von Nutzerdaten an diesen Anbieter und die daran anschließende Nutzung z. B. im Rahmen eines Analyseverfahrens aus. Die rechtlichen Rahmenbedingungen hierfür sind festgelegt durch § 11 BDSG bzw. Art. 17 Abs. 2 Europäische Datenschutzrichtlinie (EU-DSRL). Soweit eine Datenweitergabe außerhalb Europas erfolgt, sind in jedem Fall die §§ 4b, 4c BDSG (Art. 25, 26 EU-DSRL) anwendbar.

> 3. Das ULD führt aus, dass durch das bloße Aufrufen einer Webseite mit einem „Gefällt mir“-Button bereits Nutzer-Profile erstellt werden. So wird u. a. die IP-Adresse übertragen. Welche Möglichkeiten gibt es, beim Aufrufen einer Webseite die Übertragung von IP-Adressen zu unterbinden?

Die Verwendung von IP-Adressen ist für die Nutzung des Internets unverzichtbar. Es ist jedoch möglich, die Übermittlung von Informationen u. a. durch die technische Konfiguration des Browsers zu beeinflussen. Die IP-Adresse ist für die datenschutzrechtliche Bewertung nicht der einzige Anknüpfungspunkt. Eine personenbeziehbare Datenübermittlung erfolgt nicht nur, wenn eine zuordenbare IP-Adresse als eindeutiger Identifikator vorliegt. Möglich ist auch die Nutzung anderer Identifikatoren wie z. B. Cookie-IDs. Um eine datenschutzrechtlich relevante Datenerhebung durch Diensteanbieter bzw. Webseitenbetreiber zu vermeiden, ist es erforderlich, dass im Einflussbereich des Nutzenden dafür gesorgt wird, dass die übermittelten Datensätze nicht mit einem solchen Identifikator (oder mehreren Identifikatoren) versehen sind.

Ein Schwerpunkt des rechtlichen Vorwurfs des ULD gegenüber Facebook ist die unzulässige Weiterverarbeitung der übermittelten Daten zu Nutzungsprofilen. Deren Erstellung unterliegen den Vorgaben des § 15 Abs. 3 TMG, die durch Facebook nicht beachtet werden.

> 4. An Facebook: Sie haben gegenüber dem Bundesinnenminister die Erarbeitung eines Kodexes für Datensicherheit angekündigt, der sich an das deutsche Datenschutzrecht anlehnen soll. Können Sie uns Angaben über den Stand der Arbeiten und die Grundzüge des Kodexes machen?
>
> 5. Welche Daten werden bei dem Besuch einer Seite mit Social Plug-Ins von Facebook und Google erfasst und gespeichert? Wie lange werden diese Daten gespeichert, an wen werden die Daten weitergegeben, wo werden diese Daten verarbeitet und zu welchem Zweck werden die Daten erhoben und verarbeitet? Welche Daten werden gelöscht, sofern ein User zur Löschung seiner Daten auffordert bzw. sein Profil löscht? Welche Möglichkeiten bieten sich für Datenschützer die Angaben zu überprüfen und welche Handhabe besteht für Datenschützer, die Behauptungen von Facebook, es erstelle keine „pseudonymen“ Profile von Nicht-FB-Nutzern, die eine Webseite mit einem Like-Button besuchen, zu überprüfen?

Insofern verweisen wir auf unsere ausführliche Ausarbeitung vom 19.08.2011, die im Internet unter

https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf

abrufbar ist. Die Darstellung des ULD von dem auf Webseiten erfolgenden Datenverkehr wurde von Facebook bestätigt. Hinsichtlich der bei Facebook erfolgenden Verarbeitung konnte das ULD nur Mutmaßungen äußern. In einer Erwiderung auf das ULD-Arbeitspapier hat Facebook dargestellt, dass hinsichtlich Nicht-Mitgliedern eine umgehende faktische Löschung der IP-Adresse (Ersetzen durch eine Länderkennung) und dass nach 90 Tagen eine Löschung der Datensätze erfolge.

https://www.datenschutzzentrum.de/facebook/kommunikation/20110916_Facebook_deutsch.pdf

Die Überprüfung dieser sowie weiterer Angaben war dem ULD bisher nicht möglich. Eine Verifikation kann entweder vor Ort (also in den USA, wo die Datenverarbeitung stattfindet) erfolgen, aber auch durch eine Auswertung von aussagekräftigen Verfahrensdokumentionen. Das ULD hat Facebook gebeten, derartige Dokumentationen für Verifizierungszwecke vorzulegen.

Fragen der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

> 6. Wie sind die Geschäftsmodelle kommerzieller Unternehmen im Bereich Sozialer Netzwerke hinsichtlich des Schutzes persönlicher Daten der Nutzerinnen und Nutzer zu bewerten? Welche Rolle spielt dabei die Integration von Drittanbietern, deren Applikationen ebenfalls auf die innerhalb der Plattform aggregierten persönlichen Daten zugreifen – bis hin zur Protokollierung des Medienkonsums auf anderen Websites?

Sämtliche Formen der Datenverarbeitung, bei denen den Betroffenen Umfang der Daten, verantwortliche Stelle und Zweck der Verarbeitung nicht mehr erkennbar sein können, sind mit deutschem und europäischem Datenschutzrecht nicht mehr in Einklang zu bringen.

Bei der Einbindung von Drittanbietern kommt es darauf an, ob eine wirksame Datenverarbeitung im Auftrag (§ 11 BDSG) erfolgt oder der Drittanbieter für den Nutzenden zu erkennen ist und er der Datenverarbeitung informiert zustimmt. Ist dies der Fall, so ist die Einbindung aus Datenschutzsicht unproblematisch. Erfolgen jedoch Auftragsdatenverarbeitungen, die den Anforderungen des § 11 BDSG nicht genügen bzw. erfolgen verdeckte Datenübermittlungen, so mangelt es regelmäßig an einer ausreichenden rechtlichen Grundlage. Die einzig in Betracht kommende gesetzliche Grundlage des § 28 Abs. 1 S. 1 Nr. 2 BDSG ist zumeist nicht anwendbar, weil die schutzwürdigen Betroffeneninteressen nicht hinreichend gewahrt werden (können).

> 7. In welcher Beziehung stehen die aggregierten persönlichen Daten zur Profilbildung im Sinne einer Verhaltensüberwachung (Behavioral Targeting)? Welche Maßnahmen ergreifen Unternehmen bisher, um die vorgenommene Verarbeitung persönlicher Daten gegenüber Nutzerinnen, Nutzern und staatlichen Kontrollinstanzen transparent zu machen? Wie wird in Zukunft sicher gestellt werden, dass über die Art und Weise des aggregierenden und analysierenden Umgangs mit persönlichen Daten a) für alle Seiten Klarheit besteht und b) klare Einschränkungen hinsichtlich der automatisierten Profilbildung durchgesetzt werden? Welche Maßnahmen werden von Unternehmensseite er-

griffen, um den Prinzipien einer „Privacy by Default“ mit datenschutzfreundlichen Grundeinstellungen Rechnung zu tragen?

In einigen datenschutzrechtlichen Zertifizierungen hat das ULD bestätigt, dass Online Behavioural Targeting und Datenschutz miteinander in Einklang zu bringen sind.

https://www.european-privacy-seal.eu/awarded-seals/nuggad
https://www.european-privacy-seal.eu/awarded-seals/de-080006p/

Zielgerichtete Werbung wird dadurch datenschutzkonform realisiert, dass Instrumente der Anonymisierung, Transparenz, Nutzerinformation und ausschließlicher Kategorisierung nichtsensitiver Art miteinander kombiniert werden.

Eine Form der Herstellung von Transparenz besteht darin, dass eine unabhängige Stelle ein Produkt auf seine Datenschutzkonformität hin überprüft und die Überprüfungergebnisse im Rahmen der Zertifizierung veröffentlicht, so dass diese nachvollzieh- und kritisierbar wird. Das ULD bietet sowohl eine deutsche (Datenschutz-Gütesiegel Schleswig-Holstein) wie auch eine europäische Zertifizierung (European Privacy Seal – EuroPriSe) an.

https://www.datenschutzzentrum.de/guetesiegel/index.htm
https://www.datenschutzzentrum.de/europrise/

Es besteht eine gewisse rechtliche Verunsicherung dadurch, dass in Deutschland Art. 5 Abs. 3 der E-Privacy-Directive trotz Fristablauf im Mai 2011 noch nicht umgesetzt ist. Diese Regelung verlangt eine Einwilligung des Betroffenen beim Setzen von Cookies, die nicht zur Erbringung des jeweiligen Dienstes erforderlich sind. Nach Ansicht des ULD ist seit dem Fristablauf diese europäische Regelung direkt anwendbar. Im Rahmen des EuroPriSe-Zertifizierungsverfahrens fordert das ULD praktische Schritte zur Umsetzung der europäischen Regelung:

https://www.datenschutzzentrum.de/europrise/Factsheet-Behavioural-Targeting-2010826-de.pdf
https://www.european-privacy-seal.eu/results/Position-Papers

8. Wie bewerten Sie vor diesem Hintergrund, aber auch angesichts verfassungsrechtlicher wie einfachgesetzlicher Vorgaben zum Schutz der Persönlichkeitsrechte der User die Andeutungen des Bundesinnenministers sowie des Unternehmens Facebook, wonach es freiwillige Selbstverpflichtungen geben werde? Wie können demgegenüber unabhängige Stellen, die beispielsweise Auditierungen durchführen und Gütesiegel vergeben, für mehr Vertrauen und Transparenz sorgen?

Das ULD hat auf die öffentlichen Äußerungen von Facebook und des Bundesinnenministers am 08.09.2011 wie folgt reagiert:

Der Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Dr. Thilo Weichert, reagiert irritiert auf die Pressemitteilung des Bundesinnenministers vom heutigen Tag, wonach nach einem Gespräch mit Richard Allan von Facebook „die Diskussion, inwieweit deutsches Datenschutz- und Telemedienrecht für Facebook gilt, deutlich ent-

schärft“ sei, nachdem Allan sich bereit erklärt hat, Initiativen zur Selbstregulierung der Anbieter sozialer Netzwerke zu unterstützen:

„Mir ist nicht klar, auf welcher rechtlichen Basis und aufgrund welcher realen Kenntnisse Herr Friedrich eine Diskussion entschärfen könnte. Er sollte als Bundesdatenschutzminister zumindest dafür eintreten, dass die geltenden Regelungen eingehalten werden. Die Kontrolle des Datenschutzes obliegt nicht ihm, sondern den Aufsichtsbehörden der Länder. Diese äußern sich nach eingehender Prüfung von Sachverhalten und nicht nach unverbindlichen Gesprächen, auch wenn es um Facebook geht. Zu begrüßen wäre zweifellos mittelfristig eine Selbstregulierung der Branche. Diese setzt nach § 38a Bundesdatenschutzgesetz aber eine Genehmigung der Inhalte durch die zuständige Datenschutzaufsicht und nicht durch den Bundesinnenminister voraus. Der BITKOM-Kodex zu Internet-Panoramadiensten ist ein Beispiel, wie es nicht geht. Herr Friedrich sollte seine Hausaufgaben machen und endlich einen validen Entwurf zum Datenschutzrecht zum Internet vorlegen und sich nicht in Dinge einmischen, für die er nicht zuständig ist. Sinnvolle Gesetzesvorschläge liegen vor und müssen diskutiert und vorangebracht werden.“

Die in der Frage angesprochenen Auditierungen und Zertifizierungen sind ein weiteres Mittel, wie über eine regulierte Selbstregulierung Datenschutzkonformität von Internet-Produkten und -Angeboten erreicht werden kann (s. o. Antwort zu Frage 5). Voraussetzung dafür ist aber eine umfassende Prüfung des Zertifizierungsgegenstands (Target of Evaluation) durch eine unabhängige Stelle, die sowohl ihre Prüfungskriterien und -verfahren wie auch ihre Prüfungsergebnisse veröffentlicht und somit eine qualifizierte Information der Nutzenden wie auch eine Hinterfragung durch Expertinnen und Experten ermöglicht, so wie dies bei den Angeboten des ULD der Fall ist.

> 9. Wie schätzen Sie die von Anbietern sozialer Netzwerke angebotenen Möglichkeiten ein, unbeteiligte Dritte namentlich in das Netzwerk dergestalt aufzunehmen, indem diese entweder über das Hochladen kompletter Adressbücher („Friend Finder“-Funktionalität) als Teil des Netzwerkes abgebildet werden oder durch das Tagging – d.h. das automatische Benennen von einer Person in Bildern – erfasst werden, insbesondere im Hinblick auf die nach deutschem Recht grundsätzlich verbürgte Freiheit, „selbst zu bestimmen, wer was wann über einen weiß“? In diesem Zusammenhang: Ist es richtig, dass Facebook von Irland aus Datenerhebung und -nutzung steuert und der Schwerpunkt der Tätigkeiten dort liegt? Bitte stellen Sie die arbeitsorganisatorischen Prozesse dar: vor dem Hintergrund der Anwendbarkeit irischen Rechts unter Berücksichtigung von Europarecht bzw. der Anwendbarkeit deutschen Rechts unter Berücksichtigung europäischen Rechts.

Inwieweit Facebook/Irland oder Facebook/USA als verantwortliche Stelle nach deutschem und europäischem Datenschutzrecht im Hinblick auf das Angebot des „Friend Finder“ anzusehen ist, ist derzeit noch nicht geklärt. Facebook meint, die Verantwortung läge bei Facebook/Irland; Facebook/USA, wo die gesamte tatsächliche Datenverarbeitung erfolgt, sei Auftragsdatenverarbeiter für das Unternehmen in Irland.

https://www.datenschutzzentrum.de/facebook/kommunikation/20110916_Facebook_deutsch.pdf

Eine Klärung findet insofern derzeit auf europäischer Eben statt. In jedem Fall legitimiert Auftragsdatenverarbeitung (vgl. Art. 17 Abs. 2 EU-DSRL) nicht die voraussetzungslose Daten-

weitergabe an Facebook/USA, da dieses Unternehmen sich im Drittausland befindet. Eine wirksame Berufung auf das Safe-Harbor-Abkommen ist nach der einheitlichen Ansicht der deutschen Datenschutzaufsichtsbehörden nicht möglich:

https://www.datenschutzzentrum.de/internationaler-datenverkehr/Beschluss_28_29_04_10neu.pdf

Ein Facebook entsprechendes Angebot von einem deutschen Anbieter wäre jedenfalls eine Verletzung des Grundrechts auf informationelle Selbstbestimmung wie auch ein Verstoß gegen das BDSG. Eine Berufung auf die Ausnahme der Nutzung zu ausschließlich persönlichen Tätigkeiten gemäß § 1 Abs. 2 Nr. 3 BDSG ist für geschäftsmäßige Anbieter ausgeschlossen. Die einzigen denkbaren gesetzlichen Grundlagen zur Übermittlung bzw. Rückübermittlung der Adressdaten sind die § 28 Abs. 1 S. 1 Nr. 2 BDSG und § 29 BDSG. Für beide Datenverarbeitungsprozesse liegen die rechtlichen Voraussetzungen nicht vor, da die schutzwürdigen Interessen der Betroffenen überhaupt nicht berücksichtigt werden (können). In diesem Zusammenhang muss darauf hingewiesen werden, dass deutschen Facebook-Angehörigen insofern eine datenschutzrechtliche Mitverantwortlichkeit zukommt, dass sie – ohne sich genau über die stattfindenden Prozesse klar zu sein – Facebook das Auslesen der eigenen Adressbücher ermöglicht. Auf eine Einwilligung kann sich jedenfalls Facebook nicht berufen, da diese nicht den Anforderungen des § 4a BDSG genügt und nicht von den Betroffenen (den Kommunikationspartnern des Facebook-Mitglieds) erklärt wird.

> 10. Wie bewerten Sie den sowohl von Google Plus als auch von Facebook in den Allgemeinen Geschäftsbedingungen vorgegebenen Klarnamenzwang – in Verbindung mit den bestehenden Grundeinstellungen für die Offenlegung des Profils – hinsichtlich des Schutzes von Persönlichkeitsrechten der User im Internet? Welche Maßnahmen sollen und werden die genannten Unternehmen ergreifen, um eine Nutzung in anonymer und pseudonymer Form zu ermöglichen, die angesichts der weltweiten Nutzung digitaler Sozialer Netzwerke in Menschenrechtsbewegungen, aber auch anhand der bestehenden Regelungen des deutschen Telemediengesetzes geboten ist?

Die Klarnamenverpflichtung stellt nach deutschem Recht einen Verstoß gegen § 13 Abs. 6 Telemediengesetz (TMG) dar. Dies wurde jüngst ausführlich und richtig von Thomas Stadler (Zeitschrift für Datenschutz, ZD, Heft 2/2011, 57 ff.) begründet. Nach dieser Regelung sind Anbieter wie Facebook und Google verpflichtet, ihren Nutzenden eine anonyme oder pseudonyme Nutzung zu ermöglichen.

Da die Grundeinstellungen bei Google+ und Facebook nicht den Anforderungen des „Privacy by Default“ entsprechen, verstoßen sie gegen deutsches und europäisches Datenschutzrecht. Voraussetzung nach diesem Datenschutzrecht für eine – hier stattfindende Datenübermittlung in die USA – ist eine informierte Einwilligung nach § 4a BDSG. Hieran fehlt es.

Zur Beantwortung und Erörterung weiterer Fragen stehe ich gerne im Rahmen des Expertengesprächs bereit.

Mit freundlichen Grüßen

Dr. Thilo Weichert