



Ausarbeitung

Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins

Zum Arbeitspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

aktualisierte Fassung vom 7. Oktober 2011

Birgit Schröder/Anne Hawxwell

Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins

Zum Arbeitspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Verfasser/in: Regierungsdirektorin Dr. Birgit Schröder/Oberregierungsrätin Anne Hawxwell/Rechtsreferendarin Heike Münzing

Aktenzeichen: WD 3 – 3000 - 306/11 neu

Abschluss der Arbeit: 7. Oktober 2011

Fachbereich: WD 3: Verfassung und Verwaltung

Telefon: +49-30-227-32325

Inhaltsverzeichnis

1.	Einleitung	4
2.	Die datenschutzrechtliche Bewertung des ULD	5
2.1.	Personenbezug der erhobenen Daten	5
2.1.1.	IP-Adressen	6
2.1.2.	Cookies	7
2.2.	Verantwortlichkeit	7
2.2.1.	Webseitenbetreiber	8
2.2.2.	Nutzer als verantwortliche Stelle	9
2.3.	Anwendbares Recht	10
2.4.	Zulässigkeit der Datenverarbeitung	12
2.5.	Weitere gesetzliche Regelungen für deutsche Webseitenbetreiber	14
2.5.1.	Informationspflichten	14
2.5.2.	Datensicherheit	15
3.	Formelle Voraussetzungen für Bußgeldverfahren gegen Webseitenbetreiber	16
3.1.	Zuständigkeit des ULD	16
3.2.	Verfahren nach dem OWiG	18
4.	Zusammenfassung – Konsequenzen für Webseitenbetreiber	19

1. Einleitung

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat am 19. August 2011 ein Arbeitspapier mit dem Titel „**Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook**“ veröffentlicht.¹ Auf Grundlage seiner technischen und rechtlichen Analyse kommt das ULD zu dem Ergebnis, dass sogenannte **Fanpages bei Facebook**² und **Social-Plugins**³ wie der „Gefällt mir“-Button gegen das Telemediengesetz (TMG)⁴ und gegen das Bundesdatenschutzgesetz (BDSG)⁵ verstoßen. In einer Pressemitteilung vom gleichen Tag fordert das ULD **alle Webseitenbetreiber in Schleswig-Holstein** auf, ihre Fanpages bei Facebook und Social-Plugins auf ihren Webseiten zu entfernen. Das ULD erwarte, dass sie umgehend die Datenweitergaben über ihre Nutzenden an Facebook in die USA einstellen, indem sie die **entsprechenden Dienste deaktivieren**. Erfolge dies nicht bis **Ende September 2011**, so werde das ULD weitergehende Maßnahmen – bei öffentlichen Stellen Beanstandungen nach § 42 LDSG SH⁶, bei privaten Stellen Untersagungsverfügungen nach § 38 Abs. 5 BDSG sowie **Bußgeldverfahren** – ergreifen.⁷

Die vorliegende Ausarbeitung untersucht zunächst, inwieweit der **Rechtsauffassung** des ULD zuzustimmen ist und Verstöße gegen datenschutzrechtliche Bestimmungen seitens Facebook vorliegen.⁸ Dabei findet eine abschließende datenschutzrechtliche Bewertung der durch das ULD festgestellten Sachverhalte nicht statt. Vielmehr werden die zu den im Rahmen des Arbeitspapiers angesprochenen rechtlichen Fragestellungen **vertretenen Auffassungen** überblicksartig dar-

1 Abrufbar unter: <https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf> (letzter Abruf: 13.09.2011).

2 Dabei handelt es sich um Seiten auf der Plattform Facebook, welche von Unternehmen oder Persönlichkeiten professionell betrieben werden und durch die Hilfe des Werkzeugs „Facebook Insight“ als Reichweitenanalysedienst die Möglichkeit haben, das Nutzerverhalten statistisch erfassen zu lassen, z.B. Nutzerzuwachs, Demographie, Nutzung und Erstellung von Inhalten.

3 Darunter versteht man von Facebook zur Verfügung gestellte Programmschnipsel, die der Betreiber der betreffenden Website in den Code der Webseite einbindet. Wie genau Facebook mit den Social Plugins arbeitet, unterscheidet sich je nach dem, ob der Nutzer parallel bei Facebook eingeloggt ist, ob er überhaupt ein Facebook-Profil besitzt und ob er das Social Plugin betätigt. Technisch handelt es sich jedoch um sog. „Inlineframes“ (iframes), welche direkt zwischen dem Computer des Nutzers und Facebook übermitteln. Die wichtigsten Social-Plugins von Facebook sind: Der Like-Button, Comment-Button, Send-Button, das Activity-Feed, der Recommendation-Button, die Like-Box, der Login-Button, Registration-Button, das Facepile und der Live-Stream (<http://developers.facebook.com/docs/plugins/>, zuletzt abgerufen am 14.09.2011).

4 Telemediengesetz (TMG) vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 1. Telemedienänderungsgesetz vom 31.05.2010 (BGBl. I S. 692).

5 Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66) zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009 (BGBl. I S. 2814).

6 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) vom 09.02.2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Artikel 12 des Gesetzes zur Neuregelung des Beamtenrechts in Schleswig-Holstein vom 26.03.2009 (GVOBl. Schl.-H. S. 93).

7 Pressemitteilung des ULD vom 19.08.2011, abrufbar unter: <https://www.datenschutzzentrum.de/presse/20110819-facebook.htm> (letzter Abruf: 31.08.2011).

8 Die Ausarbeitung orientiert sich hierbei an der Prüfungsreihenfolge des Arbeitspapiers.

gestellt. Die Darstellung konzentriert sich dabei vor allem auf die für die Verwender von Social-Plugins und die Betreiber von Facebook Fanpages relevanten Rechtsfragen. Anschließend werden die formellen Voraussetzungen für die angedrohten Bußgeldverfahren dargestellt. Abschließend wird geprüft, welche **Konsequenzen** sich auf Grundlage der rechtlichen Bewertung des ULD für **Webseitenbetreiber** ergeben, insbesondere ob diese **gezwungen** sind, ihre Fanpages bei Facebook und die Social-Plugins auf ihren Webseiten **zu entfernen**. Die technische Bewertung des ULD wird dem Gutachten zugrunde gelegt.

2. Die datenschutzrechtliche Bewertung des ULD

2.1. Personenbezug der erhobenen Daten

Das ULD geht zunächst davon aus, dass durch den Dienst „**Facebook Insight**“, welcher bei Fanpages und Social-Plugins zum Einsatz kommt, personenbezogene Daten erhoben und verarbeitet werden. So seien zum einen die durch die Facebook-Nutzer gespeicherten **persönlichen Informationen**, zum anderen auch die bei der Nutzung von externen Diensten und den Fanpages erhobenen und verarbeiteten **Internetprotokoll-Adressen (IP-Adressen)**⁹ sowie die durch Facebook genutzten **Cookies**¹⁰ Angaben mit Personenbezug.¹¹

Gemäß **§ 3 Abs. 1 BDSG** sind **personenbezogene Daten** Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (**Betroffener**).¹² **Einzelangaben** sind Informationen, die sich auf eine bestimmte Person beziehen oder geeignet sind, einen Bezug zu ihr herzustellen.¹³ Diese Einzelangaben müssen Aussagen enthalten über „**persönliche oder sachliche Verhältnisse**“ des Betroffenen; es muss sich also um Daten handeln, die Informationen über den Betroffenen selbst oder über einen auf ihn beziehbaren Sachverhalt enthalten.¹⁴ Daten sind außerdem nur dann personenbezogen, wenn sie einer Person zugeordnet werden können, eine Person also aufgrund des Datums **bestimmt oder bestimmbar** ist.¹⁵ **Bestimmtheit** in diesem Sinne ist gegeben, wenn sich die Daten direkt auf eine bestimmte Person beziehen, wenn sie also einen unmittelbaren Rückschluss auf die Identität einer Person zulassen.

9 Vergleiche zum technischen Hintergrund von IP-Adressen Krüger, Stefan/Maucher, Svenja-Ariane, Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, 433.

10 Als Cookies werden kleine Dateien bezeichnet, die von einem Web-Server erzeugt, an einen Web-Browser, der mit diesem Server eine Verbindung aufgebaut hat, gesendet und auf dem Rechner des Nutzers abgelegt werden; Schaar, Peter, Datenschutz im Internet, 2002, S. 64.

11 Arbeitspapier (Fn. 1), S. 15.

12 Diese Legaldefinition gilt auch für die Erhebung personenbezogener Daten i. S. d. TMG; vgl. KG, Beschluss vom 29.04.2011 - 5 W 88/11.

13 Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz Kommentar, 10. Auflage 2010, § 3 Rn. 3.

14 Gola/Schomerus (Fn. 13), § 3 Rn. 5.

15 Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios, Datenschutzrecht, 2. Auflage 2011, S. 80.

sen.¹⁶ **Bestimmbarkeit** liegt dagegen vor, wenn der Betroffene nicht allein durch die Daten identifiziert, jedoch mit Hilfe anderer Informationen und Zusatzwissen ein Personenbezug hergestellt werden kann.¹⁷ **Welche Anforderungen in diesem Zusammenhang an die Bestimmbarkeit einer Person zu stellen sind, ist umstritten.** So wird zum einen vertreten, dass Bestimmbarkeit bereits dann vorliegt, wenn es **objektiv möglich** ist, zwischen dem Datum und der Person eine Verbindung herzustellen.¹⁸ Nach anderer Ansicht kommt es dagegen auf die **individuellen Möglichkeiten** der verantwortlichen Stelle zur Herstellung der Verbindung an, der Begriff des Personenbezugs ist demzufolge **relativ** zu verstehen.¹⁹ Die **relative Bestimmbarkeit** bedeutet, dass Daten für eine datenverarbeitende Stelle personenbezogen sein können und für eine andere nicht. Geht man von einem **Begriff der absoluten Bestimmbarkeit** aus, so kommt es für den Personenbezug dagegen nur darauf an, dass irgendein Dritter eine Verbindung zwischen dem Datum und einer natürlichen Person herstellen kann.²⁰

Die im Rahmen der Registrierung bei Facebook durch die Nutzer gemachten Angaben wie Alter, Geschlecht und Beruf sind grundsätzlich als personenbezogene Einzelangaben zu betrachten und werden daher von § 3 Abs. 1 BDSG erfasst.²¹ Beim Anklicken eines Gefällt mir-Buttons durch einen in diesem Moment angemeldeten Facebook-Nutzer kommt es außerdem zu einer Verknüpfung mit seinem Facebook-Account, weswegen auch in diesem Fall eine eindeutige Identifizierung möglich ist.²² Fraglich ist jedoch, inwieweit den im Hinblick auf IP-Adressen und Cookies gemachten Einschätzungen des ULD zuzustimmen ist.

2.1.1. IP-Adressen

Im Hinblick auf die Frage, ob IP-Adressen personenbezogene Daten i. S. d. § 3 BDSG sind, ist zunächst zwischen statischen und dynamischen IP-Adressen zu unterscheiden. **Statische IP-Adressen** werden einem bestimmten Rechner bzw. Nutzer fest zugewiesen, **dynamische IP-Adressen** werden dagegen bei jeder neuen Sitzung („Session“) durch den **Access-Provider** – also den kommerziellen Anbieter, der dem Nutzer einen Internetzugang entgeltlich zur Verfügung stellt²³ – an den Kunden für diese eine Sitzung vergeben.²⁴ Teilweise wird vertreten, dass stati-

16 Krüger/Maucher (Fn. 9), MMR 2011, 433 (434).

17 Krüger/Maucher (Fn. 9), MMR 2011, 433 (434).

18 Weichert, Thilo, in: Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Kompaktkommentar zum BDSG, § 3 Rn. 13.

19 Gola/Schomerus (Fn. 13), § 3 Rn. 10.

20 Krüger/Maucher (Fn. 9), MMR 2011, 433 (434).

21 Vergleiche Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 169, S. 4, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf (letzter Abruf: 12.9.2011).

22 Ernst, Stefan, Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem, NJOZ 2010, 1917 (1918).

23 Wischmann, Tim, Rechtsnatur des Access-Providing, MMR 2000, 461.

24 Krüger/Maucher (Fn. 9), 343.

sche IP-Adressen grundsätzlich als personenbezogene Daten zu qualifizieren sind, da sich in Kombination mit dem Einsatz von Cookies spezifisch auf den jeweils den betreffenden Computer bedienenden Nutzer zugeschnittene Daten gewinnen lassen, die einen Personenbezug erlauben.²⁵ Andere fordern auch bei statischen IP-Adressen eine relative Beurteilung des Personenbezugs.²⁶ Im Hinblick auf dynamische IP-Adressen wird eine Zuordnung der IP-Adresse zu einer bestimmten Person regelmäßig nur für den Access-Provider als möglich angesehen.²⁷ Folgt man der **Theorie der absoluten Bestimmbarkeit**, so ist die Möglichkeit des Access-Providers zur Herstellung einer Verbindung einer IP-Adresse mit einer bestimmten Person als ausreichend zu betrachten und die IP-Adresse daher **als personenbezogenes Datum zu qualifizieren**. Geht man dagegen von der **Theorie der relativen Bestimmbarkeit** aus, so ist im Hinblick auf andere Diensteanbieter, wie beispielsweise Betreibern von Webseiten, deren Nutzung keine besondere Registrierung voraussetzt, von **keiner Identifizierbarkeit** allein anhand der IP-Adresse auszugehen. Die Landesdatenschutzbehörden wie auch die Artikel-29-Datenschutzgruppe bejahen einen Personenbezug einer IP-Adresse, gleichzeitig finden sich sowohl in der Rechtsprechung als auch in der rechtswissenschaftlichen Literatur prominente Stimmen, die einen Personenbezug verneinen.²⁸

2.1.2. Cookies

Die Verwendung von Cookies ermöglicht es den einzelnen Diensteanbietern im Internet, die verschiedenen Nutzer zu „markieren“, um ihren Weg durch ihr Netz verfolgen zu können.²⁹ Cookies selbst lassen keinen Rückschluss auf die bürgerliche Identität eines bestimmten Nutzers zu, eine Identifizierung ist jedoch mithilfe weiterer Daten wie beispielsweise einer Zugangskennung möglich.³⁰ Auch im Hinblick auf Cookies ist **umstritten**, ob ein genereller Personenbezug besteht oder nicht.³¹

2.2. Verantwortlichkeit

Neben Facebook als Dienstbetreiber und den durch Facebook genutzten „Content Delivery Networks (CDN)“ betrachtet das ULD **auch Webseitenbetreiber** – wie beispielsweise die Betreiber

25 Helfrich, in: Hoeren, Thomas/Sieber, Ulrich, Handbuch Multimediarecht, 28. Ergänzungslieferung 2011, Teil 16.1. Rn. 34.

26 Spindler, Gerald/Nink, Judith, in: Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien Kommentar, 2. Auflage 2011, § 11 TMG Rn. 8.

27 Schmitz, in: Hoeren/Sieber (Fn. 25), Teil 16.2 Rn. 80.

28 Vergleiche die Übersicht über die verschiedenen Ansichten in Rechtsprechung und Literatur bei Krüger/Maucher (Fn. 9), 434 f.

29 Schmitz, in: Hoeren/Sieber (Fn. 25), Teil 16.2 Rn. 87.

30 Schmitz, in: Hoeren/Sieber (Fn. 25), Teil 16.2 Rn. 87.

31 Schaar (Fn. 10), Rn. 186.

einer Seite, die einen Social-Plugin verwenden – sowie unter bestimmten Umständen auch **Nutzer von Facebook** als datenschutzrechtlich verantwortliche Stellen.³²

2.2.1. Webseitenbetreiber

Webseiten sind in der Regel den **elektronischen Informations- und Kommunikationsdiensten i. S. d. TMG** zuzuordnen.³³ Der Begriff des **Diensteanbieters** in § 2 S. 1 Nr. 1 TMG umfasst sowohl das Bereithalten eigener als auch fremder Telemedien; unerheblich ist dabei, ob der Bereitstellende über einen eigenen Server verfügt oder fremde Speicherkapazität genutzt wird.³⁴ **Für Webseitenbetreiber mit Sitz in Deutschland gilt daher grundsätzlich das TMG.** In §§ 7 ff. TMG finden sich besondere Bestimmungen über die Verantwortlichkeit von Telemedienanbietern. Diese Regelungen gelten jedoch nur für die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung; für die **datenschutzrechtliche Verantwortlichkeit von Telemedienanbietern gilt dagegen § 3 Abs. 7 BDSG.**³⁵ Gemäß § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Artikel 2 d) der **EU-Datenschutzrichtlinie (DS-RL)**³⁶ bestimmt darüber hinaus, dass verantwortlich nur ist, **wer über die Zwecke und Mittel der Datenverarbeitung entscheidet.** Es kommt somit nicht darauf an, dass jemand tatsächlich personenbezogene Daten erhebt, verarbeitet oder nutzt, sondern vielmehr, dass er die **Verfügungsmacht** über die Daten besitzt.³⁷

Im Hinblick auf das Anbieten eines Gefällt mir-Buttons auf einer Internetseite ließe sich wohl argumentieren, dass dieses Anbieten allein dem Webseitenbetreiber nicht die Verfügungsgewalt über die Daten, die beim Anklicken dieses Buttons erhoben und gespeichert werden, gewährt. Andererseits wird die Erhebung und Speicherung dieser Daten erst durch die Einbindung des Social-Plugins auf der Webseite **ermöglicht.** Da die **Einbindung durch den Webseitenbetreiber erfolgt,** lässt sich auf Grundlage dieser Argumentation wohl eine datenschutzrechtliche Verantwortlichkeit des Webseitenbetreibers begründen.³⁸ Insbesondere liegt keine **Auftragsdatenverarbeitung des Webseitenbetreibers für Facebook** im Rahmen des § 11 BDSG vor, bei deren Vorliegen die Verantwortlichkeit des Webseitenbetreibers ausscheiden könnte, da der Auftraggeber für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich ist. Dies ließe sich so konstruieren, dass der Betreiber der Webseite nur ein „Werkzeug“ für die Datenerhebung und Verar-

32 Arbeitspapier (Fn. 1), S. 17 f.

33 Holznagel, Bernd/Ricke, Thorsten, in Spindler/Schuster (Fn. 26), § 1 TMG Rn. 4.

34 Holznagel/Ricke, in Spindler/Schuster (Fn. 26), § 2 TMG Rn. 2.

35 Weichert, Thilo, in: Däubler/Klebe/Wedde/Weichert (Fn. 18), § 1 Rn. 57.

36 RL 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-RL), ABl. EG Nr. L 281 vom 23.11.1995, S. 31.

37 Jotzo, Florian, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232 (233).

38 Ernst (Fn. 22), NJOZ 2010, 1917 (1918).

beitung seitens Facebook ist. Zwar könnte durch die Implementierung des Social-Plugins noch ein „Erheben“ von Daten durch den Betreiber der Webseite gesehen werden, jedoch fehlt es an anderen Voraussetzungen des § 11 BDSG. Vor allem liegt zwischen Facebook und dem Webseiteninhaber kein „Auftrag“ irgendeiner Art vor.³⁹ Der Webseitenbetreiber ist insofern jedenfalls nicht gem. § 11 BDSG der Verantwortlichkeit enthoben.

Das ULD geht darüber hinaus davon aus, dass die Webseitenbetreiber für die durch Facebook erstellten **Reichweitenanalysen** verantwortlich sind. Dies ergebe sich aus der die Reichweitenanalyse regelnden Vorschrift des § 15 Abs. 3 TMG, sowie aus § 11 BDSG. Die Diensteanbieter würden Facebook als Dienstleister heranziehen und seien daher für die Handlungen dieses Dienstleisters datenschutzrechtlich verantwortlich.⁴⁰ Gemäß § 15 Abs. 3 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien **Nutzungsprofile** bei Verwendung von Pseudonymen erstellen, soweit der Nutzer dem nicht widerspricht. Auch in dieser Konstellation kommt eine Anwendung des § 11 Abs. 1 BDSG in Betracht, jedoch in umgekehrter Beziehung. Wie oben erläutert, bestimmt § 11 BDSG die Verantwortlichkeit des **Auftraggebers** für die Einhaltung der Vorschriften des BDSG für den Fall, dass personenbezogene Daten **im Auftrag durch eine andere Stelle erhoben, verarbeitet oder genutzt werden**. Voraussetzung für ein Auftragsverhältnis nach § 11 BDSG ist, dass die beauftragte Stelle **nur eine Hilfs- und Unterstützungsfunktion** hat und in diesem Rahmen in **völliger Abhängigkeit** von den Vorgaben der verantwortlichen Stelle tätig wird.⁴¹ In welcher **Rechtsform** das Auftragsverhältnis begründet wird ist unerheblich; eine Auftragsdatenverarbeitung wird zudem nicht dadurch ausgeschlossen, dass der Auftragnehmer ein über das i. d. R. finanzielle Interesse an der Durchführung des Auftrags hinausgehendes **Eigeninteresse** hat.⁴²

Ob im Hinblick auf die durch Facebook zur Verfügung gestellten Statistiken von einer Auftragsdatenverarbeitung i. S. d. § 11 BDSG ausgegangen werden kann, **erscheint fraglich**. Das ULD beschreibt die Erstellung der Reichweitenanalyse selbst dahingehend, dass es sich hierbei um eine kostenfreie Statistik-Funktion handle, welche untrennbar mit dem Einsatz von Social-Plugins einhergehe.⁴³ Facebook wird daher wohl gerade nicht in Abhängigkeit von den Vorgaben der verantwortlichen Stelle tätig, sondern bestimmt vielmehr selbst den Umfang und die Art der zur Verfügung gestellten Statistiken.

2.2.2. Nutzer als verantwortliche Stelle

Gemäß § 11 Abs. 2 TMG ist **Nutzer** im Sinne des datenschutzrechtlichen Abschnitts des TMG jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder

39 Ernst (Fn. 22), NJOZ 2010, 1917 (1918).

40 Arbeitspapier (Fn. 1), S. 18.

41 Wedde, in: Däubler/Klebe/Wedde/Weichert (Fn. 18), § 11 Rn. 5.

42 Gola/Schomerus (Fn. 13), § 11 Rn. 6, 7a.

43 Arbeitspapier (Fn. 1), S. 12, 17.

zugänglich zu machen. Da das Zugänglichmachen von Informationen eine Nutzung von Telemedien darstellt, kommt grundsätzlich eine Überschneidung des Nutzerkreises mit dem Kreis der verantwortlichen Stellen in Betracht. Dabei ist jedoch zunächst zu beachten, dass nach der sogenannten **Ausnahmeklausel für Privathaushalte** der EU-Datenschutzrichtlinie die Pflichten des für die Verarbeitung Verantwortlichen keine Anwendung auf die Verarbeitung solcher Daten finden, die eine natürliche Person zur Ausübung **ausschließlich persönlicher oder familiärer Tätigkeiten** vorgenommen hat.⁴⁴ Allerdings findet diese Ausnahmeklausel beispielsweise dann wiederum keine Anwendung, wenn die Nutzung des sozialen Netzwerks zur **Förderung kommerzieller, politischer oder karitativer Zwecke** stattfindet.⁴⁵ Dies zugrunde gelegt, könnte jedenfalls ein Facebook-Nutzer, der eine Fanpage mit entsprechender Zielsetzung betreibt, als verantwortliche Stelle betrachtet werden. Fraglich ist jedoch, ob die **Eigenschaft des Nutzers als Betroffener** – vorausgesetzt es handelt sich bei diesem um eine natürliche Person – dieser Einordnung nicht entgegensteht.

Der Wortlaut des § 3 Abs. 7 BDSG⁴⁶ steht einer derartigen Auslegung nicht entgegen, insbesondere wird der Betroffene nicht ausdrücklich vom Kreis der verantwortlichen Stellen ausgeschlossen. Eine derartige Auslegung der Vorschrift erscheint jedoch jedenfalls für den Fall verfehlt, in dem jemand Daten zu seiner eigenen Person verarbeitet, da der Gesetzgeber den Betroffenen nicht vor sich selbst schützen kann und dies auch grundsätzlich nicht will.⁴⁷ Das Betreiben einer Fanpage, welche sich wohl nicht ausschließlich auf persönliche oder familiäre Tätigkeiten bezieht, aber gleichzeitig lediglich mit der Verarbeitung eigener Daten einhergeht, dürfte daher wohl zu keiner Verantwortlichkeit nach § 3 Abs. 7 BDSG führen.

2.3. Anwendbares Recht

Die Abgrenzung der sachlichen Anwendungsbereiche datenschutzrechtlicher Regelungen erfolgt nach dem sogenannten „**Schichtenmodell**“: Die datenschutzrechtliche Behandlung des **Datentransports** (Telekommunikation) richtet sich nach dem **TKG**, die **Interaktion** zwischen Nutzer und Anbieter nach dem **TMG** und das Angebot solcher Dienste, bei denen der Teledienst lediglich das Übertragungsmedium für andere Leistungen ist – also der **Inhalt der Kommunikation** –, nach dem **BDSG**.⁴⁸

44 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 169, S. 6.

45 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 169, S. 6 f.

46 § 3 Abs. 7 BDSG: „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“

47 Dammann, Ulrich, in: Simitis, Spiros, Bundesdatenschutzgesetz, 7. Auflage 2011, § 3 Rn. 226.

48 Schaar (Fn. 10), Rn. 247 ff.

Ein soziales Netzwerk wie Facebook setzt sich aus einer **Vielzahl von Teilangeboten** zusammen.⁴⁹ Dabei fallen all diejenigen Daten, die für die Vertragsabwicklung erforderlich sind – wie die Login-Daten, ein Name, unter dem das Profil angezeigt wird und ggf. eine E-Mail-Adresse – als **Bestandsdaten** nach § 14 TMG in den Anwendungsbereich dieses Gesetzes.⁵⁰ Für sämtliche Inhaltsdaten, die nicht für die Vertragsabwicklung erforderlich sind – wie bspw. Wohnort, Alter, Geschlecht – ist **umstritten**, ob diesbezüglich das **BDSG anzuwenden ist oder diese als Unterfall der Nutzungsdaten** zu bewerten sind.⁵¹ So wird einerseits argumentiert, auch diese Daten stünden in einem unmittelbaren Zusammenhang mit der Erbringung des Telemediendienstes und eine entsprechende Anwendung des § 15 TMG sei daher sinnvoll und interessengerecht. Zudem würde es der abschließenden Natur des Telemedienschutzes widersprechen, wenn bestimmte Daten, die zwar online eingegeben und genutzt werden, die aber nicht unter den engen Begriff der Bestands- und Nutzungsdaten subsumiert werden können, nach den Vorschriften des BDSG behandelt werden würden.⁵² Andere argumentieren dagegen, es sei von einer Beurteilung nach dem BDSG auszugehen, da diese Daten gerade nicht für die Durchführung des Vertragsverhältnisses oder die Inanspruchnahme des Dienstes erforderlich seien, sondern lediglich bei der Nutzung übermittelt werden würden.⁵³ Im Falle einer Anwendung des BDSG ist als besonderer Ausschlussgrund § 1 Abs. 2 Nr. 3, 27 Abs. 1 S. 2 BDSG zu beachten, wonach die Erhebung, Verarbeitung oder Nutzung von Daten, die ausschließlich für **persönliche oder familiäre Tätigkeiten** erfolgt, vom Anwendungsbereich dieses Gesetzes ausgeschlossen ist.⁵⁴

Ausgangspunkt für die Bestimmung des **räumlichen Anwendungsbereichs** ist § 1 Abs. 5 S. 1 BDSG. Aus dieser Vorschrift ergibt sich, dass für die Anwendung des deutschen Datenschutzrechts grundsätzlich das so genannte „**Sitzprinzip**“ gilt. Solange der Datenumgang durch eine verantwortliche Stelle stattfindet, die ihre Niederlassung in einem EU-Mitgliedstaat bzw. einem EWR-Vertragsstaat hat, kommt es grundsätzlich zur Anwendung des jeweiligen nationalen Rechts, es sei denn die Verarbeitung erfolgt durch eine **Niederlassung** im Inland. Von einer Niederlassung ist auszugehen, wenn die Tätigkeit **effektiv und tatsächlich** von einer festen Einrichtung ausgeübt wird; die Rechtsform, in der die Niederlassung organisiert ist, ist nicht maßgeblich.⁵⁵ Nach § 1 Abs. 5 S. 4 BDSG gilt das Sitzprinzip für verantwortliche Stellen, die ihren Sitz außerhalb der EU bzw. des EWR haben nur, wenn Datenträger zum Zweck des Transits durch das Inland eingesetzt werden. In allen übrigen Fällen gilt das **Territorialprinzip**.⁵⁶ Auch der **räumli-**

49 Karg, Moritz/Fahl, Constantin, Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken, K&R 2011, 453 (456).

50 Karg/Fahl (Fn. 49), K&R 2011, 453 (457).

51 Heckmann, in: jurisPK-Internetrecht, 2. Auflage 2009, Kapitel 1.14 Rn. 9 ff.

52 Bauer, Stephan, Personalisierte Werbung auf Social Community-Websites - Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MMR 2008, 435 (436).

53 Karg/Fahl (Fn. 49), 458.

54 Siehe oben Punkt 2.2.2.

55 Gola/Schomerus (Fn. 13), § 1 Rn. 28.

56 Kühling/Seidel/Sivridis (Fn. 15), S. 104. Andere gehen von einer grundsätzlichen Geltung des Territorialprinzips aus und begreifen § 1 Abs. 5 BDSG als Ausnahme hiervon, vgl. bspw. Jotzo (Fn. 37), MMR 2009, 232 (233).

che Anwendungsbereich des TMG bestimmt sich nach § 1 Abs. 5 BDSG. § 3 Abs. 1 TMG beinhaltet wohl eine eigene Regelung für die Anwendung dieses Gesetzes, jedoch wird gemäß § 3 Abs. 3 Nr. 4 TMG das Recht, das für den Schutz personenbezogener Daten gilt, durch diese Regelung nicht berührt. Aufgrund des gemeinsamen europarechtlichen Ursprungs ist vielmehr § 1 Abs. 5 BDSG als Kollisionsnorm auch zur Bestimmung des räumlichen Anwendungsbereichs des TMG heranzuziehen.⁵⁷

Facebook unterhält eine **Niederlassung in Irland**, weswegen zunächst die Anwendung irischen Rechts nach § 1 Abs. 5 S. 1 BDSG in Betracht kommt. Das ULD beurteilt diese Niederlassung jedoch als **bloße Anlauf- und Beschwerdestelle** und sieht Facebook Inc. mit Sitz in **Kalifornien** als für die Datenverarbeitung verantwortliche Stelle.⁵⁸ Inwieweit diese Einschätzung zutreffend ist, lässt sich aus hiesiger Sicht nicht überprüfen. Über die Vorschrift des § 1 Abs. 5 S. 2 BDSG⁵⁹ führt die Beurteilung des ULD zur **Anwendbarkeit deutschen Datenschutzrechts** für die Datenverarbeitung von Facebook, da keine Ausnahme nach § 1 Abs. 5 S. 2 BDSG greift. Soweit auch Facebook-Nutzer und die Verwender von Social-Plugins mit Sitz in Deutschland als verantwortliche Stellen betrachtet werden, ist auch bezüglich dieser von der Anwendbarkeit deutschen Rechts auszugehen.⁶⁰

2.4. Zulässigkeit der Datenverarbeitung

Grundsätzlich darf ein Umgang mit personenbezogenen Daten nur erfolgen, wenn dies ausdrücklich gesetzlich erlaubt ist oder der Betroffene in die Datenerhebung, -speicherung und -verarbeitung einwilligt (**Verbot mit Erlaubnisvorbehalt**, „**Opt-In-Lösung**“).⁶¹ Nach § 4a BDSG ist eine Einwilligung nur wirksam, wenn sie auf der **freien Entscheidung** des Betroffenen beruht. Der Betroffene ist zudem auf den **vorgesehenen Zweck** der Erhebung, Verarbeitung oder Nutzung **hinzuweisen**. Der Betroffene muss wissen, auf **welche personenbezogenen Daten** sich die Einwilligung bezieht und **was** mit diesen Daten geschehen soll; die **pauschale Erklärung** des Betroffenen, er sei mit jeder weiteren Verarbeitung seiner Daten einverstanden, genügt nicht.⁶² Nach § 4a Abs. 1 S. 3 BDSG bedarf die Einwilligung der **Schriftform**, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Das Erfordernis der Einwilligung erstreckt sich auf **alle Phasen des Umgangs mit personenbezogenen Daten**.⁶³ Auf Grundlage dieser grundsätzlichen Anforderungen an eine datenschutzrechtlich wirksame Einwilligung ist die Bewertung der mit

57 Jotzo (Fn. 37), MMR 2009, 232 (234).

58 Arbeitspapier (Fn. 1), S. 19 f.

59 „Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt“.

60 Ernst (Fn. 22), NJOZ 2010, 1917 (1918).

61 Kühling/Seidel/Sivridis (Fn. 15), S. 106.

62 Gola/Schomerus (Fn. 13), § 4a Rn. 11.

63 Gola/Schomerus (Fn. 13), § 4a Rn. 1.

der Registrierung bei Facebook fingierten Einwilligung – gemäß dem Arbeitspapier des ULD – als unzureichend wohl nicht zu beanstanden.⁶⁴ Insbesondere fehlt es an der **notwendigen Transparenz** bezüglich Art, Umfang und Dauer der Datenverarbeitung sowie des Zwecks der Verwendung und an der Kenntnis, ob die Übermittlung innerhalb der EU oder in einen Drittstaat erfolgt.⁶⁵

Auch dürfte den Ausführungen des ULD im Hinblick auf die Einordnung und Bewertung der Nutzungsbedingungen von Facebook als **Allgemeine Geschäftsbedingungen** (AGB) zuzustimmen sein. Die Nutzungsbedingungen eines Plattformbetreibers für die Ausgestaltung der Rechtsbeziehungen zwischen ihm und den Nutzern stellen regelmäßig AGB i. S. d. §§ 305 ff. des Bürgerlichen Gesetzbuches (BGB)⁶⁶ dar.⁶⁷ Zudem müssen AGB auch im Bereich von Internetangeboten grundsätzlich in der Sprache zur Verfügung gestellt werden, in denen das Angebot – hier die angebotene Plattform – präsentiert wird.⁶⁸ Der Verweis auf die englischsprachige Version der AGB als maßgebliche Version dürfte daher tatsächlich als unzureichend zu bewerten sein.

Wenn man der Ansicht des ULD folgt, dass auch der **Webseitenbetreiber** verantwortliche Stelle ist und Daten verarbeitet, ist dies auch für den Webseitenbetreiber nur mit wirksamer **Einwilligung** des Nutzers möglich, **§ 13 Abs. 2 TMG**. Auch im Bereich dieser Norm handelt es sich um eine „Opt-In-Lösung“; die Einwilligung muss bewusst und freiwillig erfolgen. Neben der Einwilligung des Nutzers ist es ebenfalls möglich, die Erhebung von Daten über eine **Erlaubnisnorm** zu legitimieren. Im Fall des Webseitenbetreibers käme für die Daten, die durch den Social-Plugin für Facebook zugänglich gemacht werden, **§ 15 Abs. 1 TMG** in Betracht. Denn der Besuch einer Webseite und die Interaktion mit einem Social-Plugin sind sog. Nutzungsdaten, die den Anwendungsbereich des TMG eröffnen.⁶⁹ Gem. § 15 Abs. 1 TMG darf der Webseitenbetreiber die Daten erheben, sofern dies **erforderlich** ist, um die **Inanspruchnahme des Teledienstes zu ermöglichen**. Einerseits könnte deshalb argumentiert werden, dass auch die Übermittlung der Daten an Facebook erforderlich sei, weil nur so der Social-Plugin, der Teil des Webseitenangebotes ist, erbracht werden könne. Dagegen spricht, dass der Anwendungsbereich sich auf den Hauptzweck des durch die Webseite angebotenen Dienstes bezieht und nicht auf jede Applikation erweitert werden darf. Auch insofern lässt sich keine eindeutige Aussage treffen.

Auch im Hinblick auf den durch Facebook angebotenen **Reichweitenanalysedienst** „Facebook Insight“ kommt das ULD zu dem Ergebnis, dass die von Facebook eingeholte Einwilligung diesbezüglich den datenschutzrechtlichen Anforderungen nicht gerecht wird.⁷⁰ Nach **§ 15 Abs. 3**

64 Im Ergebnis so auch; Ernst (Fn. 22), NJOZ 2010, 1917 (1918 f.).

65 Vgl. Duchrow, Rebecca, Kritik an der Entscheidung des KG zum Facebook Like-Button, MMR-Aktuell 2011, 320091, m. w. Nw.).

66 Bürgerliches Gesetzbuch (BGB) in der Fassung der Bekanntmachung vom 02.01. 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 27.07.2011 (BGBl. I S. 1600) geändert worden ist.

67 Berberich, Matthias, Der „Content“ gehört nicht Facebook! AGB-Kontrolle der Rechteeräumung an nutzergenerierten Inhalten, MMR 2010, 736.

68 Graf von Westfalen, Vertragsrecht und AGB-Klauselwerke, 28. Auflage 2010, Teil „Vertragsrecht“ 37) Rn. 14.

69 Siehe bereits oben unter Punkt 2.3.

70 Arbeitspapier (Fn. 1), S. 22 f.

TMG darf der Diensteanbieter **Nutzungsprofile** unter Verwendung eines Pseudonyms für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein **Widerspruchsrecht** im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen, die Erlaubnis wird somit im Rahmen einer **Opt-Out Lösung** erteilt.⁷¹ Eine Erstellung von Nutzungsprofilen, die über die in § 15 Abs. 3 TMG normierte Erlaubnis hinausgeht, ist nur bei Vorliegen einer Einwilligung des Nutzers möglich.⁷² Geht man mit dem ULD davon aus, dass die Betreiber von Fanpages und Webseitenbetreiber, die Social-Plugins von Facebook auf ihren Seiten einbinden, datenschutzrechtlich auch für die Reichweitenanalysen verantwortlich sind, so ergibt sich hieraus eine **Pflicht auf die Widerspruchsmöglichkeit hinzuweisen**. Nach aktuellem Wissensstand des ULD besteht derzeit technisch gar nicht die Möglichkeit eine entsprechende Widerspruchserteilung zu implementieren,⁷³ weshalb schon allein deshalb von einem Verstoß gegen § 15 Abs. 3 S. 3 TMG ausgegangen werden kann. Im Übrigen ist auch der Bewertung der ULD im Hinblick auf einen Verstoß gegen das **in § 15 Abs. 3 S. 3 TMG normierten Trennungsgebot** zuzustimmen. Nach § 15 Abs. 3 S. 3 TMG dürfen die Nutzungsprofile **nicht** mit den Daten über den Träger des Pseudonyms **zusammengeführt** werden. Gemäß § 3 Abs. 6a BDSG ist **Pseudonymisieren** das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen mit dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Das soziale Netzwerk Facebook basiert jedoch gerade darauf, dass sich die Nutzer mit ihrem tatsächlichen Namen anmelden.⁷⁴ Laut ULD arbeitet Facebook im Rahmen der Profilbildung von authentifizierten und angemeldeten Nutzern mit dem Cookie „datr“, welche die Verbindung eines erlangten Nutzungsdatums mit dem angemeldeten Facebook-Nutzer ermöglicht. Da der Cookie „datr“ zwei Jahre aktiv ist, ist selbst dann eine eindeutige namentliche Zuordnung möglich, wenn sich ein zunächst nicht angemeldeter Nutzer innerhalb des Bestehens des Cookies bei Facebook anmeldet. Auf Grundlage dieser technischen Bewertung des ULD ist von einem Verstoß gegen das Trennungsgebot nach § 15 Abs. 3 S. 3 TMG auszugehen.

2.5. Weitere gesetzliche Regelungen für deutsche Webseitenbetreiber

2.5.1. Informationspflichten

Das ULD geht davon aus, dass auch die Betreiber einer **Unterseite auf Facebook** nach § 5 Abs. 1 TMG ein **Impressum** führen müssen. In diesem Zusammenhang ist anerkannt, dass beispielsweise die einzelnen Anbieter bei ebay, sofern sie geschäftsmäßige Teledienste anbieten, **für ihre Unterseiten impressumpflichtig sind**, obwohl sie den übergeordneten Teledienst ebay

71 Spindler, Gerald/Nink, Judith, in: Spindler/Schuster (Fn. 26), § 15 TMG Rn. 8.

72 Bauer (Fn. 52), 438.

73 Arbeitspapier (Fn. 1), S. 23.

74 Bauer (Fn. 52), 438.

nicht betreiben.⁷⁵ Fraglich ist jedoch, inwieweit Facebook Unterseiten wie beispielsweise Fanpages als **geschäftsmäßig angebotene Telemedien** zu verstehen sind. Ein Diensteanbieter handelt geschäftsmäßig, wenn er Telemedien aufgrund einer **nachhaltigen Tätigkeit** mit oder ohne Gewinnerzielungsabsicht erbringt; als nachhaltig ist eine Tätigkeit anzusehen, wenn sie auf einen **längeren Zeitraum** ausgerichtet ist und sich nicht auf einen Einzelfall beschränkt.⁷⁶ Bei einer derartig weiten Auslegung des Begriffs der Geschäftsmäßigkeit fällt wohl auch das langfristige Betreiben einer Facebook-Fanpage in den Bereich der geschäftsmäßig angebotenen Telemedien. Jedoch wird das Merkmal der Geschäftsmäßigkeit in § 5 Abs. 1 TMG dahingehend konkretisiert, dass das Telemedium **in der Regel gegen Entgelt** angeboten wird. Nach Sinn und Zweck der Vorschrift ist diese Einschränkung dahingehend zu verstehen, dass von § 5 TMG nur diejenigen Anbieter erfasst werden sollen, die die **Webseite als Einstiegsmedium** begreifen, mittels dessen sie dem Kunden im Ergebnis eine **entgeltliche Leistung** anbieten.⁷⁷ Im Hinblick auf eine Fanpage eines Unternehmens wird sich auf dieser Grundlage eine Impressumspflicht nach § 5 TMG wohl vertreten lassen. Für Fanpages, die dagegen in keinerlei Hinsicht einen Einstieg für eine entgeltliche Leistung begründen, gilt dagegen wohl nicht § 5 TMG, sondern vielmehr die **abgeschwächte Impressumspflicht nach § 55 Rundfunkstaatsvertrag (RStV)**⁷⁸, wobei auch hier von einer **selbstständigen Impressumspflicht für jede Unterseite** auszugehen ist.⁷⁹

Das ULD geht außerdem von einer Verletzung des § 13 Abs. 1 TMG aus, wonach der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten (...) zu unterrichten hat. Geht man mit dem ULD von einer Verantwortlichkeit der Verwender von Social-Plugins für die durch Facebook erstellten Reichweitenanalysen aus, so führt dies in der Konsequenz wohl tatsächlich zu einer Verletzung der Unterrichtungspflicht nach § 13 Abs. 1 TMG.

2.5.2. Datensicherheit

Zuletzt verweist das ULD auf die nach § 13 Abs. 4 TMG bestehende Pflicht eines Telemedienanbieters, bestimmte technische und organisatorische Vorkehrungen zu treffen. Inwieweit dieser Einschätzung zuzustimmen ist, hängt wiederum davon ab, ob man der Auffassung des ULD, dass Webseitenbetreiber mit Social-Plugins ebenfalls verantwortliche Stellen sind, folgt oder nicht.

75 OLG Düsseldorf, Urteil vom 18.12.2007 - I-20 U 17/07, abgedruckt in MMR 2008, 682.

76 Micklitz, Hans-W./Schirnbacher, Martin, in: Spindler/Schuster (Fn. 26), § 5 TMG Rn. 8.

77 Micklitz/Schirnbache, in: Spindler/Schuster (Fn. 26), § 5 TMG Rn. 10.

78 Staatsvertrag für Rundfunk und Telemedien vom 31.08.1991, in der Fassung des Dreizehnten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 10. März 2010 (vgl. GBl. S. 307), in Kraft getreten am 01.04.2010; http://www.die-medienanstalten.de/fileadmin/Download/Rechtsgrundlagen/Gesetze_aktuell/13._RStV_01.04.2010_01.pdf (letzter Abruf: 14.09.2011).

79 Vergleiche Held, Thorsten, in: Hahn, Werner/Vesting, Thomas, Beck'scher Kommentar zum Rundfunkrecht, 2. Auflage 2008, § 55 RStV Rn. 30.

3. Formelle Voraussetzungen für Bußgeldverfahren gegen Webseitenbetreiber

§ 43 BDSG enthält einen umfangreichen Katalog von Bußgeldtatbeständen, wobei sich die Tatbestände in Absatz 1 auf Verstöße gegen **Verfahrensvorschriften** beziehen, Absatz 2 dagegen auf **Verstöße gegen materielle Datenschutzbestimmungen** abstellt. Absatz 3 sieht für Verstöße nach Absatz 1 eine Geldbuße von bis zu **fünfundzigtausend Euro**, für Verstöße nach Absatz 2 Geldbußen von bis zu **dreihunderttausend Euro** vor. Für den Anwendungsbereich des TMG beinhaltet außerdem **§ 16 TMG** Bußgeldtatbestände; nach § 16 Abs. 3 TMG können diese Ordnungswidrigkeiten mit Geldbußen von bis zu **fünfundzigtausend Euro** geahndet werden.

3.1. Zuständigkeit des ULD

Die Bußgeldtatbestände des BDSG und des TMG enthalten keine Regelungen über die zuständige Verwaltungsbehörde, es gelten vielmehr die **allgemeinen Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG)**^{80, 81}. Nach § 36 Abs. 1 OWiG ist für die Verfolgung von Ordnungswidrigkeiten die Behörde **sachlich zuständig**, die durch Gesetz bestimmt wird bzw. mangels einer solchen die fachlich zuständige oberste Landesbehörde oder das fachlich zuständige Bundesministerium, soweit das Gesetz von Bundesbehörden ausgeführt wird.

Hinsichtlich der sachlichen Zuständigkeit für die Ahndung von Ordnungswidrigkeiten nach § 16 TMG ist zu differenzieren. Für die Ahndung von Ordnungswidrigkeiten nach § 16 Abs. 1 und Abs. 2 Nr. 1 TMG wurde die Zuständigkeit durch **§ 38 Abs. 6 Medienstaatsvertrag HSH**⁸² der **Medienanstalt Hamburg/Schleswig-Holstein** zugewiesen. Diese Ordnungswidrigkeiten betreffen die **Impressumpflicht** und das Verbot, den Absender oder kommerziellen Charakter einer E-Mail zu verschleiern.

Die übrigen Tatbestände des § 16 Abs. 2 TMG betreffen **Verstöße gegen datenschutzrechtliche Vorschriften des TMG**. Die **Zuständigkeit** für die Ahndung dieser Ordnungswidrigkeiten wird in der – ausschließlich in Online-Medien geführten Diskussion – **unterschiedlich beurteilt**.

Nach einer Auffassung⁸³ soll die Zuständigkeit mangels anderer ausdrücklicher gesetzlicher oder untergesetzlicher Regelung nach § 36 Abs. 1 Nr. 2 lit. a OWiG dem Landesinnenministerium als

80 Gesetz über Ordnungswidrigkeiten (OWiG) in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602) zuletzt geändert durch Artikel 2 des Gesetzes zur Regelung der Verständigung im Strafverfahren vom 29.07.2009 (BGBl. I S. 2353).

81 Klebe, Thomas in: Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 43 Rn. 23; Heckmann, in: jurisPK-Internetrecht, 2. Auflage 2009, Kap. 1.16 Rn. 17.

82 Staatsvertrag über das Medienrecht in Hamburg und Schleswig-Holstein (Medienstaatsvertrag HSH) vom 13.06.2006 in der Fassung des Staatsvertrags zur Änderung des Staatsvertrags über das Medienrecht in Hamburg und Schleswig-Holstein (Zweiter Medienänderungsstaatsvertrag HSH) vom 03./04.06.2008, abrufbar unter: http://www.ma-hsh.de/cms/upload/downloads/Rechtsvorschriften/1.1_MedienStV0908.pdf (Stand: 05.09.2011).

83 Diskussionsbeitrag von *Rocknrolla* vom 22. August 2011 zum Beitrag *Keine Zuständigkeit für Bußgeldbescheide* im Blog Socialmediarecht, abrufbar unter: <http://socialmediarecht.wordpress.com/2011/08/22/uld-facebook-keine-zustandigkeit-fur-busgeldbescheide/> (abgerufen am 7. Oktober 2011).

fachlich zuständiger oberster Landesbehörde zustehen. Demgegenüber beruft sich das ULD auf die Regelung des § 45 Abs. 1 LDSG⁸⁴, wodurch eine gesetzliche Zuweisung der ursprünglich dem Landesinnenministerium obliegenden Aufgaben an das ULD erfolgt sei. § 45 Abs. 1 LDSG bestimmt, dass die am 30. Juni 2000 dem bei dem Präsidenten des Schleswig-Holsteinischen Landtages eingerichteten Landesbeauftragten für den Datenschutz sowie der Datenschutzaufsichtsbehörde im Innenministerium obliegenden Aufgaben am 1. Juli 2000 auf das ULD übergehen.

Fraglich ist allerdings, ob hiervon auch die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten erfasst ist. Die Gesetzgebungsmaterialien, soweit sie allgemein zugänglich sind, enthalten zu dieser Frage keine Hinweise. Es dürfte zwar anzunehmen sein, dass die genannten Stellen für die Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten in der Vergangenheit zuständig waren. Dies kann allerdings nicht anhand des Wortlauts des Gesetzes nachvollzogen werden. Die übergebenen Aufgaben werden nicht näher bezeichnet. Zudem ist nicht ersichtlich, ob durch diese Übertragung auch typischerweise ministerielle Aufgaben dem ULD zufallen und dieses dadurch zur obersten Landesbehörde in Sachen Datenschutz werden sollte.

In der Diskussion werden daher Zweifel an der hinreichenden Bestimmtheit des § 45 Abs. 1 LDSG hinsichtlich der Zuständigkeitsübertragung geäußert.⁸⁵ Das in Art. 20 Abs. 3 GG verankerte Bestimmtheitsgebot fordert, dass staatliches Handeln – insbesondere bei Eingriffen in die Rechtsphäre des Einzelnen – für die Rechtsunterworfenen berechenbar sein muss.⁸⁶ Hierzu dürfte auch die Frage zählen, durch wen der Staat gegenüber dem Bürger tätig werden darf. Es erscheint jedenfalls zweifelhaft, ob die Regelung des § 45 LDSG diesen Anforderungen genügt, zumal die Zuständigkeit für die Ahndung anderer datenschutzrechtlicher Verstöße durch das ULD ausdrücklich in einer Zuständigkeitsverordnung⁸⁷ geregelt ist. Hieraus kann gefolgert werden, dass der Ordnungsgeber eine Regelung der Zuständigkeitsfragen für Verstöße gegen Datenschutzvorschriften für regelungsbedürftig hielt und nicht von einer „Generalzuständigkeit“ des ULD aufgrund von § 45 Abs. 1 LDSG ausging.

Schließlich ist anzumerken, dass die Verfolgung von Ordnungswidrigkeiten nach § 16 TMG eine Aufgabe ist, die erst mit dem Inkrafttreten des TMG im Jahr 2007 entstanden ist und daher keine Aufgabe ist, die durch die Regelung des § 45 Abs. 1 LDSG im Jahr 2000 auf das ULD übergegangen sein kann. Etwas anderes würde allenfalls gelten, wenn das ULD durch die Regelung in § 45 Abs. 1 LDSG zur obersten Landesbehörde geworden wäre und das Landesinnenministerium

84 Abrufbar unter: https://www.datenschutzzentrum.de/facebook/faq_de.html (abgerufen am 7. Oktober 2011).

85 Strunk („Kielanwalt“), Bußgeld-Androhung des ULD wegen angeblicher Verstöße gegen das TMG ist rechtswidrig, im Blog LEGALIT, abrufbar unter: <http://blawg.legalit.de/2011/08/22/bussgeld-androhung-des-uld-wegen-angeblichem-verstoss-gegen-das-tmg-rechtswidrig/> (abgerufen am 7. Oktober 2011).

86 Sommermann, Karl-Peter in v. Mangoldt/Klein/Starck, Grundgesetz, Band 2, 6. Auflage, 2010, Art. 20 Rn. 289.

87 Landesverordnung zur Bestimmung der zuständigen Behörden für die Verfolgung und Ahndung von Ordnungswidrigkeiten (Ordnungswidrigkeiten-Zuständigkeitsverordnung - OWiZustVO) vom 22.01.1988 (GVOBL. Schl.-H. 2008, S. 32).

keine Aufgaben im Bereich des Datenschutzes mehr wahrnehmen könnte. Dies wäre – jedenfalls auf Bundesebene – eine sehr ungewöhnliche Aufgabenverteilung bzw. -entziehung.

Folgt man der Auffassung, dass § 45 Abs. 1 LDSG keine Zuständigkeitsübertragung für die Ahndung von Ordnungswidrigkeiten nach dem TMG regelt, wäre das **ULD** für die Verhängung eines Bußgeldes nach § 16 Abs. 2 Nr. 2 bis 5 TMG **nicht zuständig**.⁸⁸ Stattdessen wäre das Landesinnenministerium nach § 36 Abs. 1 Nr. 2 lit. a OWiG zuständig.

Im Hinblick auf die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG ergibt sich die sachliche Zuständigkeit des ULD aus **Nr. 3.5.2 der Anlage** zur schleswig-holsteinischen Landesverordnung zur Bestimmung der zuständigen Behörden für die Verfolgung und Ahndung von Ordnungswidrigkeiten (**OWiZustVO**).⁸⁹

3.2. Verfahren nach dem OWiG

Die Ahndung von Ordnungswidrigkeiten nach dem BDSG setzt **keinen Antrag** eines Geschädigten voraus, vielmehr können Anzeigen durch jedermann erfolgen.⁹⁰ Gemäß § 47 Abs. 1 S. 1 OWiG liegt die Verfolgung der Ordnungswidrigkeit im **plichtgemäßen Ermessen** der Verfolgungsbehörde. Kommt die Behörde – im Rahmen des sogenannten **Vorverfahrens** – zu dem Ergebnis, dass ein Bußgeldtatbestand verwirklicht wurde, so kann sie gemäß § 65 OWiG einen entsprechenden **Bußgeldbescheid** erlassen, bei Geringfügigkeit der Ordnungswidrigkeit gemäß § 56 OWiG eine **Verwarnung** aussprechen oder das Verfahren gemäß § 47 Abs. 1 S. 2 OWiG **einstellen**. All diese Entscheidungen liegen im Ermessen der Behörde, das **Opportunitätsprinzip** beherrscht das Verfahren.⁹¹ Wird ein Bußgeldbescheid erlassen und wehrt sich der Betroffene hiergegen nicht, so führt dies dazu, dass der Bescheid **rechtskräftig und vollstreckbar** wird. Der Betroffene hat aber auch die Möglichkeit gegen den Bußgeldbescheid gemäß § 67 Abs. 1 OWiG innerhalb von **zwei Wochen** nach Zustellung **Einspruch** einzulegen. Der Einspruch leitet in das sogenannte **Zwischenverfahren** ein, in welchem die Verwaltungsbehörde, die Staatsanwaltschaft und das Gericht mit der Sache befasst werden können.⁹² Führt auch das Zwischenverfahren zu keiner Erledigung, so schließt sich gemäß den §§ 71 ff. OWiG das **gerichtliche Hauptverfahren** erster Instanz an.

88 So auch Härtling, Niko, Öffentlichkeitsarbeit einer Landesbehörde, CR 2011, 585, 588, abrufbar unter: http://www.computerundrecht.de/media/2011_08-22_Haerting_Oeffentlichkeitsarbeit_einer_Landesbehoerde.pdf (Stand: 05.09.2011).

89 Landesverordnung zur Bestimmung der zuständigen Behörden für die Verfolgung und Ahndung von Ordnungswidrigkeiten (Ordnungswidrigkeiten-Zuständigkeitsverordnung - OWiZustVO) vom 22.01.1988 (GVOBL. Schl.-H. 2008, S. 32).

90 Klebe, in: Däubler/Klebe/Wedde/Weichert (Fn. 18), § 43 Rn. 23.

91 Mitsch, Wolfgang, Recht der Ordnungswidrigkeiten, 2. Auflage 2005, § 22 Rn. 3.

92 Mitsch (Fn. 91), § 22 Rn. 4.

4. Zusammenfassung – Konsequenzen für Webseitenbetreiber

Das ULD zieht auf Grundlage seiner technischen und rechtlichen Analyse die Schlussfolgerung, dass das Betreiben von Facebook Fanpages sowie die Einbindung von Social-Plugins zwangsläufig zu Datenschutzverstößen führt und fordert die Webseitenbetreiber daher dazu auf, entsprechende Angebote zu entfernen. Tatsächlich bestehen an der datenschutzrechtlichen Zulässigkeit dieser Anwendungen erhebliche rechtliche Zweifel.⁹³ Aufgrund der **komplexen und unübersichtlichen Rechtslage** sowie der **Schwierigkeit einer zutreffenden Einordnung der technischen Abläufe** ist eine abschließende datenschutzrechtliche Bewertung aus hiesiger Sicht jedoch nicht möglich.

Festzuhalten ist Folgendes: Das Gutachten des ULD übergeht an einigen Stellen bestehende Streitigkeiten zur Beantwortung datenschutzrechtlicher Fragestellungen. Zudem ist die rechtliche Bewertung teilweise lückenhaft und nicht durchgängig nachvollziehbar. So wird zunächst der **Personenbezug von IP-Adressen und auch Cookies** entgegen der Darstellung der Verfasser des Arbeitspapiers nicht einhellig beantwortet. Vielmehr herrscht Streit über die Anforderungen an die Bestimmbarkeit einer Person. Das ULD blendet somit eine seit vielen Jahren kontrovers diskutierte Frage aus.⁹⁴ Im Hinblick auf die zur Verantwortlichkeit von Webseitenbetreibern gemachten Feststellungen erscheint jedenfalls die **Begründung einer Auftragsdatenverarbeitung** nach § 11 BDSG und einer daraus resultierenden Verantwortlichkeit der Webseitenbetreiber für die durch Facebook erstellten Statistiken nicht nachvollziehbar. Eine **Verantwortlichkeit von Facebook Nutzern** ist zudem entgegen der Bewertung des ULD wohl jedenfalls dann abzulehnen, wenn diese gleichzeitig Betroffene i. S. d. Datenschutzrechts sind und lediglich Daten zu ihrer eigenen Person verarbeiten. Im Rahmen der Darstellungen zum **anwendbaren Recht** geht das ULD ohne Weiteres davon aus, dass all solche Daten, die nicht als Bestands- oder Nutzungsdaten i. S. d. TMG zu qualifizieren sind, als Inhaltsdaten dem Anwendungsbereich des BDSG unterliegen. Wie dargestellt, sind **nach einer anderen Ansicht** solche Daten jedoch zur Wahrung der Einheitlichkeit des Telemedienschutzes ebenfalls nach § 15 TMG zu behandeln. Den Ausführungen zur Zulässigkeit der Datenverarbeitung ist im Ergebnis wohl zuzustimmen. Im Hinblick auf die Informationspflichten von Webseitenbetreibern geht das ULD davon aus, dass insoweit der Anwendungsbereich des § 5 TMG eröffnet ist. Wie dargestellt, lässt sich im Einzelfall bei entsprechender Begründung jedoch auch eine **abgeschwächte Impressumspflicht nach § 55 RStV** begründen. Insgesamt hängt die Bewertung der durch das ULD gemachten Ausführungen zu Informationspflichten und Datensicherheit davon ab, inwieweit man die Verwender von Social-Plugins als verantwortliche Stellen betrachtet.

Die Frage möglicher Konsequenzen für Webseitenbetreiber lässt sich im Ergebnis nicht eindeutig beantworten. Nach hiesiger Auffassung dürfte das Landesinnenministerium für die Verhängung von Bußgeldern nach § 16 Abs. 2 Nr. 2 bis 5 TMG zuständig sein.

93 So auch die Verbraucherschutzministerin Ilse Aigner, vgl. „Aigner fordert Facebook-freie Regierung“, Der Spiegel vom 12.9.2011.

94 Härting (Fn. 88), S. 3.

Im Übrigen geht das ULD in seiner Beurteilung überwiegend von vertretbaren Rechtsauffassungen aus, jedoch ist der durch das ULD erweckte Eindruck, die untersuchten Sachverhalte würden eindeutig gegen geltendes Datenschutzrecht verstoßen, unzutreffend.⁹⁵ Vielmehr ist das geltende Datenschutzrecht **von Unsicherheiten geprägt** und macht die eindeutige Beantwortung rechtlicher Fragen in diesem Bereich schwer.⁹⁶ Eine **gerichtliche Beurteilung** der untersuchten Sachverhalte steht bislang aus. Die zur Frage der Personenbezogenheit einer IP-Adresse auch in der Rechtsprechung vertretenen verschiedenen Auffassungen machen zudem deutlich, dass selbst im Falle einer richterlichen Entscheidung nicht von einer endgültigen Klärung datenschutzrechtlicher Kontroversen ausgegangen werden kann. Es kann daher keine abschließende Empfehlung hinsichtlich einer Entfernung der durch das ULD als datenschutzrechtlich unzulässig bewerteten Angebote gegeben werden.

(gez. Dr. Birgit Schröder)

(Anne Hawxwell)

(gez. Heike Münzing)

95 So auch Härting (Fn. 88), S. 6.

96 Karg/Fahl (Fn. 49), K&R 2011, 453 (458).