

Einführungsthema

Der Tod und das soziale Netzwerk

Als Digitaler Nachlass werden Accounts und Daten im Internet bezeichnet, die nach dem Tode des Benutzers weiter bestehen bleiben. Die Behauptung „Jede Minute sterben drei Facebook-Mitglieder“ unterstreicht die Bedeutung des Digitalen Nachlasses. Nach § 1922 BGB geht im Rahmen der Universalsukzession das Vermögen als Ganzes auf die Erben über. Betroffen sind alle Vermögenswerten Positionen, alle körperlichen Gegenstände aber auch Immaterialgüter wie Urheberrechte und Dauerschuldverhältnisse, wie z. B. ein Providervertrag. Postmortale Persönlichkeitsrechte hingegen – wie das Namensrecht, der allgemeine Achtungsanspruch – gehen nicht auf den Erben über, sondern werden von nahen Angehörigen „verwahrt“. Spannend daher die Frage, ob ein Provider verpflichtet werden kann E-Mails herauszugeben? Wie immer wenn Juristen sich treffen gibt es mehrere Meinungen. Die wohl überwiegende findet sich in DAV-Stellungnahme zum digitalen Nachlass (<http://anwaltverein.de/downloads/stellungnahmen/SN-DAV34-13.pdf>). Demnach sind nur höchstpersönliche Rechte ausgenommen. Ansonsten sollen Erben alle Rechte haben. Hier wird ein Vergleich zur Offline-Welt gezogen: Die Liebesbriefe im Schrank werden ja auch mitgeerbt. Mangels Rechtsprechung darf momentan davon ausgegangen werden, dass Erben von Speichermedien auf die dort verfügbaren Daten zugreifen dürfen. Streitig sind höchstpersönliche Emails wie Liebesmails und noch nicht abgerufene Emails. Klar ist, dass eine Homepage voll vererblich ist und das Impressum innerhalb von sechs Wochen aktualisiert werden muss (oder nach Infos durch die DENIC eG wird). Die Provider gehen höchst unterschiedlich mit dieser Fragestellung um. Einige löschen den Account nach einer gewissen Zeit der Nichtnutzung (z. B. Yahoo), oder fragen nach sechs Monaten über Versand einer Kontrollemail an eine Ersatzmailadresse nach und verschaffen ggf. die volle Erbenstellung (web.de/gmx.de/1und1), eröffnen einen Gedenkstatus (Facebook), entscheiden faktisch nach Tagesform und Durchhaltevermögen in Bezug auf das komplizierte Prozedere, das Anfragenden abverlangt wird (Google) oder frieren ein Konto ein (PayPal). Dienste wie semno.de helfen bei der Recherche, wenn die verstorbene Person nicht selbst schon einen „Notfallkoffer“ mit allen wichtigen Zugangsinformationen zusammengestellt hat. Ein digitales Testament entfaltet keine Wirkung. Doch können in einem normalen Testament auch Wünsche zum „digitalen Erbe“ festgelegt werden. Ein Passwortcontainer – wie KeePass – kann für die Hinterlegung konkreter und aktueller Zugangsdaten hilfreich sein. Nur die Sicherheitsabfrage muss dann im Testament hinterlegt werden. Digitale Vererbungsdienste (wie z. B. afterstepps.com) übernehmen im Versterbensfall die Aufgabe, dass benannte Accounts gelöscht werden. Der letzte Schrei sind digitale Ruhestätten (styalive.com), Dokumentation der aktuellen Grabesgärtnerarbeiten (grabsicht.de) oder Last-Message-Dienste (welche Infos möchte ich nach meinem Tod an wen versenden? z. B. deathswitch.com).

(ausführlicher zum Thema: Brinkert/Stolze/Heidrich, Der Tod und das soziale Netzwerk – Digitaler Nachlass in Theorie und Praxis, in: ZD 4/2013 ab S. 153)

A. Gesetzesinfos

1. Orientierungshilfe Krankenhausinformationssysteme (Novelle)

Am 25.03.2014 wurde die Novellierung der Orientierungshilfe Krankenhausinformationssysteme veröffentlicht. Die erstmal im März 2011 publik gemachten Vorgaben der deutschen Datenschutzaufsichtsbehörden zum datenschutzkonformen Betrieb einer Krankenhaus-IT wurde moderat und praxisnah fortentwickelt. Auf der Seite der niedersächsischen Aufsichtsbehörde wird auf die Novellierung selbst, auf eine Synopse zum ersten Teil (betrifft die Frage, wer darf auf welche Patientendaten im Krankenhaus zugreifen?) sowie auf die Erläuterungen der Deutschen Krankenhausgesellschaft verlinkt:

http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13016&article_id=95681&_psmand=48

2. Neue Anordnung über den kirchlichen Datenschutz!

Die Vollversammlung des Verbandes der Diözesen Deutschlands hat die Inkraftsetzung einer neuen „Anordnung über den Kirchlichen Datenschutz (KDO)“ beschlossen.

http://www.datenschutz-kirche.de/recht_erbistum_hamburg

3. Geplantes IT-Sicherheitsgesetz

eco – der Verband der deutschen Internetwirtschaft e.V – hat ein lesenswertes Papier zur aktuellen Planung für weitere gesetzliche Regelungen in Bezug auf IT-Sicherheit veröffentlicht:

<http://www.eco.de/wp-content/blogs.dir/positionspapier-it-sicherheit-in-der-18-wp.pdf>

4. Offenes W-Lan und Haftung der Anbieter

Der Deutsche Anwaltsverein hat zum Thema „Offenes W-Lan und Haftung der Anbieter“ und der ins Auge gefassten Gesetzesinitiative Stellung genommen: <http://anwaltsverein.de/downloads/DAV-SN13-14.pdf>

B. Urteile und Beschlüsse von Gerichten

1. Voraussetzung für eine Übertragung der ärztlichen Eingriffs- und Risikoaufklärung an einen Medizinstudenten im Praktischen Jahr

„Die ärztliche Aufgabe der Eingriffs- und Risikoaufklärung kann einem Medizinstudenten im praktischen Jahr übertragen werden, wenn sie seinem Ausbildungsstand entspricht und unter Anleitung, Aufsicht und Verantwortung des ausbildenden Arztes stattfindet. Dies setzt nicht unbedingt voraus, dass der Arzt bei jedem Aufklärungsgespräch anwesend ist“, so der Leitsatz des OLG Karlsruhe vom 29.01.2014 (Az.: 7 U 163/12). Dieses Urteil überrascht vor dem Hintergrund der im Rahmen des Patientenrechtegesetzes eingeführten Facharztstandards im Rahmen einer Aufklärung.

2. Nutzung von Trackingtools ohne Hinweis auf Widerspruchsmöglichkeit begründen abmahnfähigen Wettbewerbsverstoß

Das Landgericht Frankfurt hat mit seinem Urteil vom 18.02.2014 (Az.: 3-10 O 86/12) bei der Verwendung des Tracking-Tools „Piwik“ entschieden, dass auch in diesem Fall – die Daten liegen nicht zwingend wie bei dem bekannten Tracking-Tool Google Analytics bei einem Dritten – eine

Belehrung und ein Hinweis auf eine bestehende Widerspruchsmöglichkeit gemäß §§ 15 Abs. 3, 13 Abs. 1 TMG erfolgen muss. Anderenfalls liegt ein abmahnfähiger Wettbewerbsverstoß vor.

3. Abo-Fallen erfüllen den Straftatbestand des Betrugs

Der BGH hat in seinem Urteil vom 05.03.2014 (Az.: 2 StR 616/12) bestätigt, dass sogenannte Internet-Abo-Fallen, in der die Kostenpflichtigkeit angebotener Leistungen systematisch verschleiert wird und damit auf die Täuschung der Nutzer abgezielt wird, eine Täuschungshandlung im Sinne von § 263 StGB darstellt.

4. Zur Eigenschaft von Domaininhaber und Admin-C

Domaininhaber und Admin-C sind nicht zwingend Dienste-Anbieter im Sinne von § 2 Abs. 1 Nr. 1 TMG. Die Domaininhaberschaft gestattet nicht den Schluss, dass der Inhaber diejenige Person ist, welche unter der Domain eine Webseite betreibt. Die Nutzungsrechte können auch Dritten überlassen worden sein, so das LG Wiesbaden im Urteil vom 18.10.2013 (Az.: 1 O 159/13).

5. Verpflichtung zur Nutzung einer elektronischen Signaturkarte

Ein Arbeitgeber kann bei ihm Beschäftigte verpflichten, eine elektronische Signaturkarte (z. B. einen Arztausweis mit elektronischer Signaturkarte) zu verwenden, so das BAG im Urteil vom 25.09.2013 (Az.: 10 AZR 270/12).

6. Löschung von Outlook-Daten kann außerordentliche Kündigung rechtfertigen

Die eigenmächtige Löschung von Daten durch den Arbeitnehmer kann eine außerordentliche Kündigung rechtfertigen, weil das Vertrauen in die Integrität des Arbeitnehmers zerstört wurde, so das Hess. LAG in seiner Entscheidung vom 07.03.2014 (Az.: 7 Sa 1060/10). Dabei kann sich der Arbeitnehmer nicht darauf berufen, dass in seinem Outlook-Account auch private Daten enthalten waren. Der Grund für die Kündigung liegt in der vertragswidrigen Entziehung von kundenbezogenen Daten vor dem unmittelbaren Zugriff des Arbeitgebers.

7. Dieb gefilmt – Kündigung folgt

Das LAG Hamm hat in seinem Urteil vom 27.03.2014 (Az.: 16 Sa 1629/13) deutlich gemacht, dass Videoaufnahmen, die den Diebstahl eines Mitarbeiters festhalten, verwertbar sind und eine Kündigung begründen.

8. Privates Fahndungsfoto kann gegen Persönlichkeitsrecht verstoßen

Das OLG Koblenz entschied mit Urteil vom 15.01.2014 (5 U 1243/13), dass ein privates Fahndungsfoto gegen das Persönlichkeitsrecht verstößt, wenn eine Drohung dahin gehend geäußert wird das Foto erst nach Erteilung eines Schuldanerkenntnisses aus dem Netz zu nehmen.

9. Beleidigende Postings bei Facebook sind öffentlich und Kündigungsgrund

Postings über Kollegen in einem sozialen Netzwerk – wie Facebook – mit den Worten „Speckrollen“ und „Klugscheisser“ sind beleidigend. Ein Posting bei Facebook macht das Ganze öffentlich. Das ArbG Duisburg hat mit Urteil vom 26.09.2012 (Az.: 5 Ca 949/12) im Nachgang zu den Urteilen des ArbG Bochum (Az.: 3 Ca 1283/11) und des ArbG Hagen vom 16.05.2012 (Az.: 3 Ca 2597/11) festgestellt, dass eine solche Äußerung auch ohne Abmahnung zu einer Kündigung aus wichtigem Grund berechtigt.

Überdies hatte es unterstrichen, dass ein Posting, egal ob öffentlich oder nur für die „Kontakte“ sichtbar, stets öffentlich ist, wenn ein großer Teil der Arbeitskollegen den Post lesen kann.

10. Videoüberwachung – Regelungen konkret ausgestalten

Das Landgericht Koblenz hat in seinem Urteil von 28.11.2013 Klauseln aus einem Fitnessstudio-Vertrag, darunter auch solche zur Kameraüberwachung und Speicherung von Aufnahmen für unzulässig erklärt (Az. 3 O 205/13). Formulierungen wie „Überwachung von Teilbereichen“ sind nicht hinreichend konkret.

11. Google Maps darf zur Reisekostenabrechnung verwendet werden

Das BAG hat in seinem Beschluss vom 10.12.2013 (Az.: 1 ABR 43/12) die Verwendung von Google Maps zur Datenermittlung bei Reisekostenabrechnungen als zulässig angesehen.

12. Funkbasierte Heizkostenmessgeräte datenschutzrechtlich okay

Der Einbau von funkbasierten Heizkosten- und Warmwassermessgeräten ist datenschutzrechtlich nicht zu beanstanden, so das AG Dortmund in seinem Urteil vom 26.11.2013 (Az.: 512 C 42/13).

C. Sonstiges

1. Impressum bei Facebook

Facebook hat die Vorgaben der LG Regensburg (Urt. v. 31.01.2013, Az.: 1 HK O 1884/12) und LG Aschaffenburg (Urt. v. 19.08.2011, Az.: 2 HK O 54/11) umgesetzt, indem es nun unter Stichwort „Info“ die Möglichkeit anbietet ein „Impressum“ anzugeben. Krankenhäuser und soziale Träger, die eine Facebook-Seite betreiben, sollten hier für Vervollständigungen Sorge tragen.

2. Compliance Hand Out

Die Rechtsanwaltskanzlei Dr. Thomas Helbing hat eine sehr übersichtliche Checkliste mit Erläuterungen und Best Practices zum Thema Compliance veröffentlicht:

<http://www.thomashelbing.com/sites/default/files/Datenschutz%20bei%20Compliance%20Programmen%20-%20Checkliste,%20Erl%C3%A4uterungen,%20Best%20Practices.pdf>

3. Orientierungshilfe Videoüberwachung

Der Düsseldorfer Kreis hat eine neue Orientierungshilfe zum Thema Videoüberwachung veröffentlicht. Dieser angehängt ist eine hilfreiche Checkliste: <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-V%C3%9C-durch-nicht-%C3%B6ffentliche-Stellen.pdf>

4. Neues BITKOM- und GDD-Muster zur Auftragsdatenverarbeitung

Der Branchenverband BITKOM hat ein neues Muster (Version 4) zur Auftragsdatenverarbeitung veröffentlicht: http://www.bitkom.org/de/themen/50792_78385.aspx

Auch der GDD hat ein neues Muster online gestellt:

https://www.gdd.de/aktuelles/arbeitshilfen/Mustervereinbarung%20a7%2011%20BDSG_final1.doc/view

5. Jahresbericht 2013 der Berliner Aufsichtsbehörde

Im Jahresbericht der Berliner Aufsichtsbehörde finden sich Anmerkungen zum Gesundheitsdatenschutz, Jugendhilfe und Personaldatenschutz.

<http://www.datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte/bericht-13>

6. Datenerhebungen bei der Vermietung von Wohnraum

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat in einer Übersicht aufgelistet, welche Daten von Wohnungssuchenden durch potentielle Vermieter erhoben werden dürfen:

<http://www.datenschutz-hamburg.de/news/detail/article/datenerhebung-bei-der-vermietung-von-wohnraum.html>

7. Unzulässigkeit von Dash-Cams in Autos

Der Düsseldorfer Kreis hat die Unzulässigkeit von Dash-Cams in Autos formuliert und begründet.

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschiessungssammlung/DuesseldorferKreis/26022014_UnzulaessigkeitDashcams.pdf?__blob=publicationFile

8. Webtracking

Der BUNDESVERBAND DIGITALE WIRTSCHAFT (BVDW) E.V. hat ein sehr informatives Papier rund um das Thema Webtracking bereitgestellt. Nach dem Urteil des LG Frankfurt (s.o.) zum Webtracking-Tool Piwik rückt diese Fragestellung wieder ein wenig in den Focus (<http://www.bvdw.org/medien/bvdw-veroeffentlicht-kostenfreies-whitepaper-zur-datenschutzkonformen-webanalyse?media=4007>).

Das Fraunhofer-Institut hat einen „Web-Tracking-Report 2014“ vorgestellt, der die Praxis des Trackens ausleuchtet

(file:///L:/Datenschutz/ARBEITSMATERIALIEN/Webanalyse%20und%20Tracking/Web_Tracking_Report_2014.pdf).

Die Aufsichtsbehörde in Baden-Württemberg hat sich gleichfalls zum Thema geäußert:

<http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Der-Einsatz-von-Reichweiteanalysediensten-im-Internet.pdf>

Die Hamburger Aufsichtsbehörde hat alle Anforderungen an die Verwendung von Google Analytics zusammengestellt: <http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html>

Das ULD in Kiel hat eine sehr umfangreiche Handreichung zu Piwik veröffentlicht:

<https://www.datenschutzzentrum.de/tracking/piwik/20110315-webanalyse-piwik.pdf>

9. Neue Seite mit Informationen zum Patientendatenschutz

Die KV Rheinland-Pfalz hat eine sehr informative Seite zu Themen wie „Behandlungsdokumentation“ oder der „Übermittlung von Informationen an Dritte unter datenschutzrechtlichen Aspekten“ online gestellt:

<http://www.mit-sicherheit-gut-behandelt.de/>