

Update

E-Commerce – Datenschutz

v. BOETTICHER HASSE LOHMANN

Zusammenfassung:

1. **Änderungen im Bestellprozess bei vielen Online-Shops nötig**
 - Der Eingang einer Online-Bestellung muss bestätigt werden. Name und Anschrift des Käufers haben in einer unverschlüsselten E-Mail allerdings nichts zu suchen.
2. **Aufsichtsbehörden geben Orientierungshilfe zu Cloud Computing**
 - Die Datenschutzbeauftragten zeigen mit einer Orientierungshilfe zulässige Wege in die Cloud auf – verstecken aber einen Hammer in einer Fußnote.
3. **Google Analytics kann jetzt „beanstandungsfrei“ gestaltet werden**
 - Analytics-Nutzer müssen aber ein paar Dinge beachten.
4. **Zahlungsfunktion bei Online-Portal nur mit BaFin-Genehmigung**
 - Wer ohne Erlaubnis nicht nur Bestellungen an Lieferanten vermittelt, sondern auch Zahlungen weiterleitet, macht sich strafbar.
5. **Über Nichtbestehen eines Widerrufsrechts muss informiert werden**
 - Über das Bestehen eines Widerrufsrechts muss informiert werden – und auch über das Nichtbestehen.

1. Änderungen im Bestellprozess bei vielen Online-Shops nötig

Der Eingang einer Bestellung im Online-Shop muss dem Kunden unverzüglich bestätigt werden – so weit, so klar, und heute nur noch selten ein Problem. Doch viele Shop-Betreiber bestätigen, indem sie eine E-Mail senden, in der alle Daten der Bestellung einschließlich Anschrift des Kunden noch einmal aufgeführt sind. Damit verstoßen sie gegen das Datenschutzrecht, denn personenbezogene Daten dürfen nicht unverschlüsselt übertragen werden. Angesichts des radikalen Kurswechsels in den Datenschutz-Aufsichtsbehörden drohen nicht nur Abmahnungen, sondern auch Bußgelder und Untersagungsverfügungen. Für finanzielle Schäden muss gegebenenfalls die Geschäftsleitung persönlich eintreten.

Dabei ist die gesetzeskonforme Lösung ganz einfach: Als Eingangsbestätigung genügt eine Bestätigungsseite am Ende des Bestellvorgangs. Da für die Bestellung ohnehin eine verschlüsselte HTTPS-Verbindung genutzt werden muss, können hier problemlos alle Angaben einschließlich Adresse, Bankverbindung und bestellten Artikeln aufgeführt werden.

Um die gesetzlichen Informationspflichten zu erfüllen (und insbesondere gegenüber Verbrauchern keine verlängerte oder gar unbegrenzte Widerrufsmöglichkeit zu riskieren), erhält der Kunde zudem eine E-Mail mit allen erforderlichen Angaben – und als Einleitung einem kurzen Dank für die eingegangene Bestellung, die aber nicht näher spezifiziert wird.

Alle Betreiber von Online-Shops – nicht nur im B2C-Bereich, sondern auch B2B – sollten ihre Bestellvorgän-

ge dringend an die datenschutzrechtlichen Anforderungen anpassen. Denn in den letzten Jahren hat sich in den Aufsichtsbehörden ein dramatischer Sinneswandel vollzogen: Während sich die Datenschutzaufsicht früher nur als Berater verstanden hat und als schwerste Konsequenz eines Datenschutzverstößes eine (folgenlose) „Beanstandung“ zu erwarten war, ist das Bußgeld quasi Standardmaßnahme geworden. Erweiterungen der Bußgeldtatbestände und Erhöhungen des Bußgeldrahmens durch den Gesetzgeber haben diese Entwicklung sicher ebenso befördert wie zusätzliches Personal für die Behörden. In Einzelfällen sind bereits Untersagungsverfügungen ausgesprochen worden, weil personenbezogene Daten per E-Mail versandt wurden.

Während die Kosten von Abmahnungen und Bußgeldern noch überschaubar sind und nur selten über vierstelligen Beträge hinausgehen dürften, kann eine Untersagungsverfügung in der Praxis eine Unternehmensschließung bedeuten. Wenn die Datenschutzverstöße grundlegende Dinge betreffen, vielleicht gar kein Datenschutzbeauftragter bestellt ist, wird regelmäßig die Geschäftsleitung ihren Aufgaben nicht nachgekommen sein. Die Mitglieder der Geschäftsleitung sind dem Unternehmen dann voll schadensersatzpflichtig.

Weiterführende Informationen:

Bergt, Schutz personenbezogener Daten bei der E-Mail-Bestätigung von Online-Bestellungen, NJW 2011, 3752
verfügbar über <http://beck-online.beck.de>

2. Aufsichtsbehörden geben Orientierungshilfe zu Cloud Computing

Wie genau der Begriff der Cloud-Services zu verstehen ist, bleibt umstritten. Wann allerdings Unternehmen Cloud-Services für personenbezogene Daten nutzen dürfen, ist seit kurzem deutlich klarer: Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Ende November die „Orientierungshilfe – Cloud Computing“ ihrer Arbeitskreise Technik und Medien „zustimmend zur Kenntnis“ genommen. Kritisch sind nach einer versteckten Fußnote aber Verträge mit US-Unternehmen oder ihren Töchtern.

Die Datenschutzbeauftragten gehen – zu Recht – davon aus, dass die Nutzung von Cloud-Services regelmäßig eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG darstellen dürfte. Die Nutzung von Cloud-Services, die im Europäischen Wirtschaftsraum (EWR) betrieben werden, ist so ohne Einwilligung des Betroffenen oder gesetzliche Erlaubnis zulässig, wenn die Anforderungen des § 11 BDSG eingehalten werden.

Dies bedeutet zunächst, dass Verträge für Cloud-Services zwingend schriftlich – Fax oder E-Mail reichen nicht – geschlossen werden müssen. Die Verträge müssen unter anderem Regelungen über technische und organisatorische Maßnahmen zur Datensicherheit beim Anbieter enthalten. Zudem ist der Auftraggeber verpflichtet, sich vor Beginn des Auftrags und sodann regelmäßig davon zu „überzeugen“, dass diese Maßnahmen auch tatsächlich umgesetzt werden. Wer die so genannte Erstkontrolle unterlässt oder den Vertrag nicht schriftlich oder mit unvollständigen Regelungen abschließt, kann mit einem Bußgeld von 50.000 Euro bestraft werden. Die Datenschutzbeauftragten akzeptieren dabei im Grundsatz, dass die Kontrolle in weiten Bereichen durch Zertifizierungen von Drittanbietern ersetzt werden kann.

Eine in der Praxis äußerst heikle „Kleinigkeit“ haben die Datenschutzbeauftragten allerdings in Endnote 18 ihrer Orientierungshilfe versteckt: Über eine Garantie, dass die Cloud nur im EWR arbeitet, hinaus „ist auch eine Bindung an EU-Recht zwingend“. Im Klartext bedeutet diese – wohl aus politischer Rücksicht so zurückhaltend formulierte – Anforderung, dass als Auftragnehmer für jegliche Art von Auftragsdatenverarbeitung beispielsweise sämtliche US- oder US-amerikanisch beherrschten Unternehmen ausscheiden. Denn diese können von den dortigen Behörden etwa nach dem „Patriot Act“ gezwungen werden, Daten ihrer Kunden herauszugeben – auch wenn dies nach europäischem Recht unzulässig ist. Dass dieses Risiko sich in der Praxis durchaus realisiert, legen Stellungnahmen von Microsoft und Google gegenüber Medien nahe.

Nach der Ansicht der Datenschutzbeauftragten kommt bei EDV-Verträgen mit US- (oder US-amerikanisch beherrschten) Unternehmen eine (rechtlich privilegierte) Auftragsdatenverarbeitung schlicht nicht in Betracht. Statt dessen müssen die Anforderungen an eine „Quasi-Auftragsdatenverarbeitung“ in Drittstaaten eingehalten werden, muss also insbesondere – neben besonderen vertraglichen Regelungen oder einer Safe-Harbor-Erklärung des Unternehmens – auch eine Rechtfertigung (Einwilligung oder Interessensabwägung nach § 28 Abs. 1 Nr. 2 BDSG) vorliegen. Werden dabei auch Regelungen entsprechend § 11 Abs. 2 BDSG getroffen, könnte die Interessensabwägung zu einer Zulässigkeit der „Quasi-Auftragsdatenverarbeitung“ führen.

Die Einschätzung der Datenschutzbeauftragten ist rechtlich nachvollziehbar: Wenn ein Auftraggeber damit rechnen muss, dass sich ein Auftragnehmer über § 11 Abs. 3 S. 1 BDSG hinwegsetzt und Daten entgegen EU-Recht an US-Behörden weitergibt, muss er Zweifel an der Zuverlässigkeit des Auftragnehmers haben. Ob dies allerdings zwingend zu einer Unzulässigkeit der Auftragsdatenverarbeitung führen muss, ist eine andere

Frage: Wenn nur Daten verarbeitet werden, die im Rahmen einer „Quasi-Auftragsdatenverarbeitung“ an diesen Auftragnehmer ins Ausland übermittelt werden dürften – wo sie dem Zugriff der dortigen Behörden ebenfalls unterliegen –, ist schwer nachvollziehbar, warum dieser Auftragnehmer die Daten nicht im Rahmen einer Auftragsdatenverarbeitung erhalten darf. Diese hätte für den Betroffenen sogar den Vorteil, dass der Auftraggeber für jede illegale Weitergabe der Daten durch den Auftragnehmer verantwortlich bliebe. Hier könnte man allenfalls das Argument der Klarheit für den Betroffenen anbringen, da nur eine geplante Datenübermittlung in Drittstaaten (etwa als „Quasi-Auftragsdatenverarbeitung“) ins Verfahrensverzeichnis aufzunehmen wäre (§ 4e S. 1 Nr. 8 BDSG).

Nicht ausreichen dürfte im Übrigen, schlicht das Recht eines EU-Mitgliedsstaates für die Auftragsdatenverarbeitung zu vereinbaren, denn die Zuverlässigkeit des Auftragnehmers wird ja gerade durch die Zugriffsmöglichkeit unter Verstoß gegen EU-Recht beeinträchtigt. Zudem dürften die (öffentlich-rechtlichen) Zugriffsmöglichkeiten ausländischer Behörden auf solche Daten unabhängig vom gewählten Recht bestehen.

Im Ergebnis sollte die restriktive Haltung der Datenschutzbehörden allerdings meist folgenlos bleiben, weil die Übermittlung an den „Quasi-Auftragsdatenverarbeiter“ nach § 28 Abs. 1 Nr. 2 BDSG erlaubt ist – nur der Weg ist anders. In der Praxis ausgeschlossen bleibt aber jede „Quasi-Auftragsdatenverarbeitung“, wenn es um sensible Daten nach § 3 Abs. 9 BDSG geht, also etwa politische Ansichten oder Gesundheit. Das sollten die Aufsichtsbehörden dann auch klar so sagen.

Weiterführende Informationen:

Orientierungshilfe – Cloud Computing

http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Bergt, Datenschutzrechtliche Erstkontrolle durch vertrauenswürdige Dritte, zur Veröffentlichung vorgesehen in ITRB 2012, Heft 4

zu bestellen unter <http://www.itrb.de>

3. Google Analytics kann jetzt „beanstandungsfrei“ gestaltet werden

Der Einsatz von Google Analytics war nach bisheriger Ansicht der Datenschutz-Aufsichtsbehörden schlicht illegal (siehe dazu unseren Client Letter Update E-Commerce – Datenschutz April 2011). In Verhandlungen mit Google hat der Hamburgische Datenschutzbe-

auftragte nun ein Verfahren vereinbart, das einen „beanstandungsfreien“ Einsatz von Analytics ermöglicht. Auch wenn diese Hinweise formal nur für Unternehmen mit Sitz in Hamburg gelten, dürften sie aufgrund von Abstimmungen mit den anderen Aufsichtsbehörden bundesweit zur Anwendung kommen.

Analytics-Nutzer müssen dazu einen schriftlichen Vertrag über Auftragsdatenverarbeitung mit Google schließen, ihre WWW-Seiten-Besucher über den Einsatz von Google Analytics informieren, eine Widerspruchsmöglichkeit einräumen (was über Googles Browser-Plugins realisiert wird) und ihre Analytics-Einstellungen so ändern, dass IP-Adressen nur gekürzt gespeichert werden. Außerdem müssen sie sich von der Einhaltung der erforderlichen Datensicherheitsmaßnahmen bei Google überzeugen, was ihnen allerdings nur durch Einsichtnahme in ein Wirtschaftsprüfer-Gutachten möglich ist, diese Kontrolle dokumentieren und die bestehenden Datenbestände löschen – was allerdings nur durch Schließen des Accounts möglich ist.

Bedeutsam ist die Mitteilung auch in anderer Hinsicht: Der Hamburgische Datenschutzbeauftragte erkennt darin die Möglichkeit an, dass sich Auftraggeber einer datenschutzrechtlichen Auftragsdatenverarbeitung für ihre Kontrollen jedenfalls in Massenverfahren ausschließlich auf Zertifikate von vertrauenswürdigen Dritten verlassen, die der Auftragnehmer eingeholt hat.

Weiterführende Informationen:

Datenschutz does not like Facebook's „Like“-Button, Google Analytics & Co., Client Letter Update E-Commerce – Datenschutz April 2011

http://www.boetticher.de/fileadmin/user_upload/downloads/CL_E-Commerce2011-04.pdf

Hinweise des Hamburgischen Datenschutzbeauftragten für Webseitenbetreiber, die Google Analytics einsetzen

http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf

Bergt, Datenschutzrechtliche Erstkontrolle durch vertrauenswürdige Dritte, zur Veröffentlichung vorgesehen in ITRB 2012, Heft 4

zu bestellen unter <http://www.itrb.de>

4. Zahlungsfunktion bei Online-Portal nur mit BaFin-Genehmigung

Wer über ein Online-Portal nicht nur Bestellungen an Lieferanten vermittelt, sondern auch Zahlungen entge-

gennimmt und an die Lieferanten weiterleitet, benötigt eine Genehmigung durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Das hat das Landgericht Köln in einem Rechtsstreit zwischen zwei Online-Essensliefer-Portalen entschieden.

Das Weiterleiten des Geldes mache das Portal zu einem Zahlungsinstitut gemäß § 1 Abs. 1 Nr. 5 Zahlungsdienste-Aufsichtsgesetz (ZAG), so dass es eine Erlaubnis nach § 8 Abs. 1 ZAG benötige. Dass die Zahlungsmöglichkeit nur eine Nebenleistung zur Vermittlung der Bestellungen darstellt, sei unbedeutend, wenn nur die Zahlungsdienste gewerblich erbracht werden und kein gesetzlicher Ausnahmefall vorliegt. Diese Ausnahmefälle lägen hier nicht vor. Insbesondere handle es sich nicht um eine Handelsvertreter-Tätigkeit, Inkasso oder Nachnahme-Zahlungen.

Wer für Dritte Zahlungsdienstleistungen erbringt, sollte sein Geschäftsmodell dringend rechtlich prüfen lassen, ob eine Erlaubnispflicht nach dem ZAG oder dem Kreditwesengesetz (KWG) vorliegt. Möglicherweise lässt sich das Geschäftsmodell auch erlaubnisfrei umgestalten.

Diese Empfehlung gilt nicht nur im Hinblick auf wettbewerbsrechtliche Abmahnungen durch Konkurrenten – wie im entschiedenen Fall –, sondern auch im Hinblick auf das eigene Vorstrafenregister: So ist beispielsweise das gewerbliche Erbringen von Zahlungsdiensten ohne Erlaubnis nach § 8 Abs. 1 ZAG eine Straftat, und zwar sogar dann, wenn nur Fahrlässigkeit vorliegt.

Weiterführende Informationen:

LG Köln, Urteil vom 29.9.2011, Az. 81 O 91/11

http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2011/81_O_91_11_Urteil_20110929.html

5. Über Nichtbestehen eines Widerrufsrechts muss informiert werden

Über das Bestehen eines gesetzlichen Widerrufs- oder Rückgaberechts informieren Unternehmer bereits aus eigenem Interesse, um die Widerrufsfrist in Gang zu setzen. Aber auch über das Nichtbestehen muss nach § 312c Abs. 1 BGB i. V. m. Art. 246 § 1 Abs. 1 Nr. 10 EGBGB informiert werden.

Dies gilt auch für Bestellkarten für Zeitschriften-Abonnements, wie sich der Axel-Springer-Verlag vom Bundesgerichtshof sagen lassen musste. Über das Nichtbestehen eines Widerrufsrechts muss nur dann nicht informiert werden, wenn das Fernabsatzrecht insgesamt keine Anwendung findet, etwa bei Gemüse-Abos, die regelmäßig nach Hause geliefert werden.

Weiterführende Informationen:

BGH, Urteil vom 9.6.2011, Az. I ZR 17/10

<http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=58437>

Ansprechpartner:

Wenn Sie Fragen haben oder weitere Informationen zu einem der Themen wünschen, wenden Sie sich bitte an:

Matthias Bergt
E-Mail: mbergt@boetticher.com
Tel. +49 / 30 / 61 68 94 03

Dr. Anselm Brandi-Dohrn, maître en droit
E-Mail: abrandi-dohrn@boetticher.com
Tel. +49 / 30 / 61 68 94 03

oder Ihren üblichen Ansprechpartner bei v. Boetticher Hasse Lohmann.

Dieses Update stellt lediglich eine Auswahl von aktuellen Entscheidungen und Entwicklungen zu den besprochenen Themen dar, dient der allgemeinen Information und ersetzt keinesfalls eine spezifische Beratung im Einzelfall. Wenn Sie Fragen zu den hier angesprochenen Rechtsproblemen – oder zu anderen Rechtsgebieten – haben, wenden Sie sich bitte an Ihren Ansprechpartner bei v. Boetticher Hasse Lohmann oder an die oben unter „Ansprechpartner“ angegebene Person.

Wenn Sie keine weiteren Informationen von v. Boetticher Hasse Lohmann über aktuelle Rechtsentwicklungen erhalten möchten, senden Sie bitte eine E-Mail an eine der oben als Ansprechpartner genannten Personen.

v. Boetticher Hasse Lohmann
Oranienstraße 164
10969 Berlin

v. Boetticher Hasse Lohmann
Freiherr-vom-Stein-Straße 11
60323 Frankfurt am Main

v. Boetticher Hasse Lohmann
Widenmayerstraße 6
80538 München

© 2012 v. Boetticher Hasse Lohmann – Partnerschaft von Rechtsanwälten. Alle Rechte vorbehalten.

v. Boetticher Hasse Lohmann – Partnerschaft von Rechtsanwälten ist eine eingetragene Partnerschaftsgesellschaft (AG München PR 516). Sitz: Widenmayerstr. 6, 80538 München. Impressum und weitere Informationen unter <http://www.boetticher.de/impressum.html>.