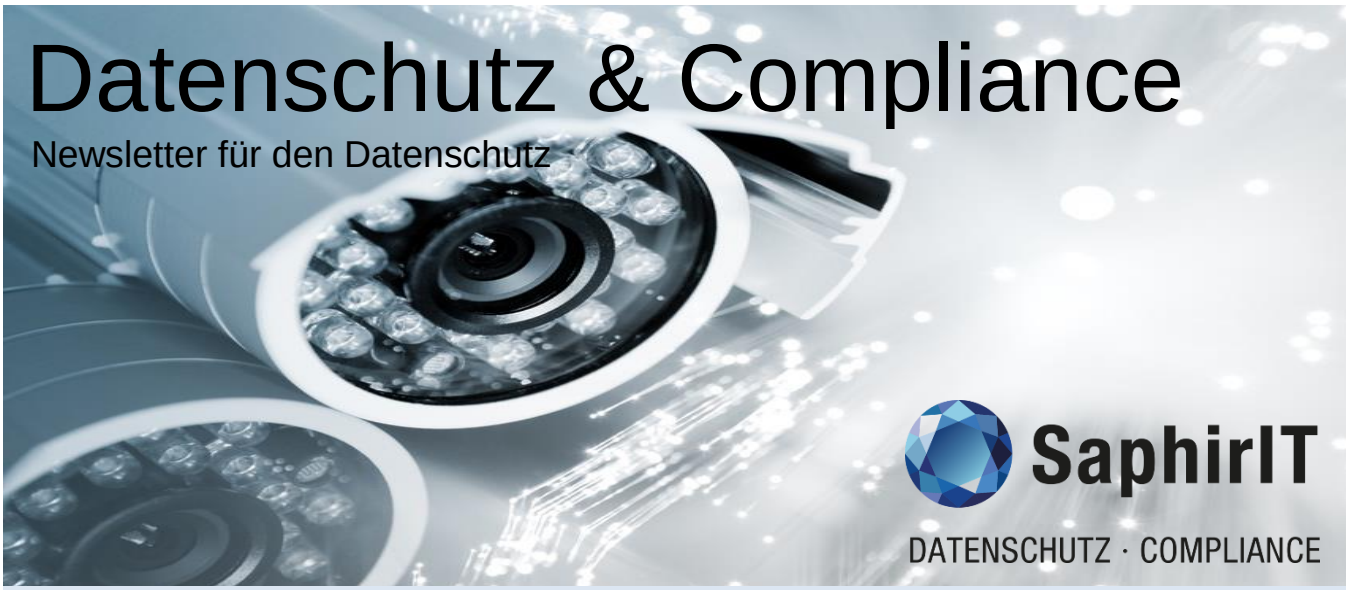

Ausgabe April 2017 | Seite 1-5

INHALT

Sehr geehrte Damen und Herren,

wir freuen uns Ihnen mit dieser Ausgabe unseren Newsletter in einem neuen Layout übersenden zu dürfen. Geben Sie uns gerne Feedback.

Ferner dürfen wir Ihnen mitteilen, dass Frau Isabelle Stroot unser Datenschutzteam zukünftig unterstützt. Frau Stroot studiert Rechtswissenschaften und hat sich bereits zur Datenschutzbeauftragten (TÜV) zertifizieren lassen. Frau Stroot wird zukünftig für unsere Rundbriefe redaktionell zuständig sein. Gerne können Sie Frau Stroot hinsichtlich eventueller Anregungen auch telefonisch unter Tel. 0541/60079296 kontaktieren.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH


Isabelle Stroot

Datenverschlüsselung via https

- Wann Sie Ihre Website verschlüsseln müssen -

In § 9 Bundesdatenschutzgesetz (BDSG) ist geregelt, dass auch Formularseiten, in denen persönliche Daten eingegeben werden (z.B. Kontaktformulare, Anmeldeformulare, Kommentarfunktionen) nach dem „aktuellen Stand der Technik“ zu schützen sind. Die Datenschutzbehörden, sowie Gerichte gehen davon aus, dass nach dem aktuellen Stand der Technik Formulardaten verschlüsselt übermittelt werden müssen. Insbesondere, da sich heutzutage auf fast jeder Website ein Formular befindet, ist für die allermeisten Webseiten-Betreiber ein SSL-Zertifikat unumgänglich. Aber wie sollten Sie

vorgehen, um diesbezüglich im wahrsten Sinne des Wortes auf der sicheren Seite zu sein?

Grundsätzlich ist erst einmal zu sagen, dass nicht die Website selbst verschlüsselt wird, sondern die Kommunikation zwischen den Besuchern der Seite und Ihrem Webserver. Eine sichere Verbindung erkennen Sie in der Browserzeile an einem „http**s**“, anstelle nur eines „http“. In manchen Fällen wird bei der sicheren Verbindung die Geltung des „https“ noch durch ein Schloss-Symbol in der Browserleiste verstärkt.

Im Hintergrund einer solchen sicheren Verbindung passiert nicht allzu viel. Der Server Administrator muss eine Software wie beispielsweise „OpenSSL“ installieren, wodurch eine abgesicherte Kommunikation über das TLS-Protokoll (Transport-Layer-Security) ermöglicht wird. Vielen dürfte noch die Vorgängerversion, nämlich das SSL-Protokoll (Secure-Socket-Layer) ein Begriff sein.

Dann müssen noch einige weitere Einstellungen vorgenommen werden und ein Zertifikat, quasi der digitale Ausweis der Website, hinterlegt werden.

Das Zertifikat (entsprechende sind auf den meisten Computern bereits vorinstalliert) enthält neben einigen Daten auch ein oder mehrere Identifikationsdaten, ein Gültigkeitsdatum, einen öffentlichen Schlüssel und eine Signatur. Letztere bekommt das Zertifikat von einer Zertifizierungsstelle (CA, Certificate Authority). Der Computer kann dann die Richtigkeit des vom Webserver empfangenen Zertifikats anhand der mitgelieferten Signatur prüfen.

Ruft dann der Webseitenbesucher Ihre Website via „http“ auf, erhält er ein Zertifikat vom Server, passt dieses dann zum Server wird dem Besucher das kleine Schloss-Symbol in der Browserleiste angezeigt. Von dem ganzen Prozess bemerkt der Webseitenbesucher nichts. Dies spielt sich alles im Hintergrund ab.

- Sind auf Ihrer Website Inhalte von anderen Webservern vorhanden, beispielsweise Werbebanner, etc. kann dies für den Fall, dass diese nicht mit „https“, sondern nur mit „http“ aufrufbar sind zu einem sog. „Mixed Content“ führen. Da dann eine unterschiedliche Sicherung der Kommunikation vorliegt, kann es zu Fehlermeldungen oder auch einer komplett ungesicherten Verbindung kommen.

Auch wenn „https“ wie alles keine 100%ige Sicherheit bietet, trägt sie nicht nur dazu bei die Sicherheit erheblich zu steigern, um digitale Einbrüche bei CAs oder technische Schwachstellen zu verhindern. Eine mit https gesicherte Website wirkt sich zudem positiv auf das Google-Ranking aus und schützt zumindest in dieser Hinsicht vor teuren Abmahnungen und Bußgeldern.

Seit dem 01.02.2017:
Neue Informationspflicht für das Impressum

Seit dem 01.02.2017 ist die zweite Stufe der Regelungen über außergerichtliche Streitbeilegung in Kraft getreten, die die ein oder andere neue Informationspflicht mit sich bringt.

Durch die gesetzlichen Änderungen möchte der Gesetzgeber vor allem Sicherheit und Vertrauen der Verbraucher in den elektronischen Handel innerhalb der EU steigern und zudem die Gerichte entlasten. Unternehmen sollen sich im Idealfall mit ihren Kunden kostengünstig einigen, bevor der Weg zu Gericht die letzte Option ist.

Genau aus diesem Grund wurden die VO 524/2013 “Verordnung über die Online-Beilegung verbraucherrechtlicher Streitigkeiten“ (ODR-VO), sowie die RL 2013/11/EU „Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten“ (ADR-RL) erlassen.

Die Umsetzung der ADR-RL hat der deutsche Gesetzgeber bereits mit dem Verbraucherstreitbeilegungsgesetz (VSBG) zum 01.04.2016 vorgenommen.

Anders als EU-Verordnungen, müssen EU-Richtlinien nämlich durch den Gesetzgeber in Landesrecht umgesetzt werden.

Die außergerichtliche Streitbeilegung ist grundsätzlich freiwillig. Es kann auch der reguläre Gerichtsweg vorgezogen werden. Verpflichtet sind Unternehmen aber zumindest darauf hinzuweisen, ob sie an einem solchen Schlichtungsverfahren teilnehmen oder nicht. Verpflichtet werden kann ein Unternehmen dazu aber nur im Einzelfall.

Sollten Sie diesbezüglich weitergehende Fragen haben, stehen wir Ihnen jederzeit und gerne zur Verfügung.

Warum eine Informationspflicht zur Streitbeilegung nicht bereits 2016 eingeführt wurde liegt daran, dass diese in zwei Stufen in Kraft getreten sind. Da eine EU-Verordnung auch ohne das Zutun des deutschen Gesetzgebers ihre Wirkung entfaltet, traten die in der ODR-VO geltenden Informationspflichten bereits Anfang 2016 in Kraft. Dieser Verordnung zufolge müssen alle Unternehmen die online Verträge mit Verbrauchern abschließen, auf die Streitbeilegungsplattform der EU-Kommission hinweisen: *http://ec.europa.eu/consumers/odr/*.

Die ADR-RL dagegen wurde erst durch den deutschen Gesetzgeber mit dem VSBG umgesetzt. Dieser beschloss, dass die darin enthaltenen Informationspflichten ab Februar 2017 gelten.

Da sowohl die Pflichten aus der ODR-VO, als auch aus dem VSBG beachtet werden

müssen, ergeben sich folgende Informationspflichten:

- **Hinweis auf die Online Streitbeilegungsplattform** – Dieser Hinweis muss immer erfolgen, wenn Sie einen Vertragsschluss mit Verbrauchern über Waren oder Dienstleistungen online anbieten (Art. 14 ODR-VO).

- **Allgemeine VSBG Informationspflicht** Diese Informationspflicht besteht immer unabhängig von Kundenkontakt und Streitigkeiten, zumindest wenn Sie mehr als 10 Mitarbeiter im Vorjahr hatten (§ 36 VSBG).

- **VSBG-Informationspflicht bei Streitigkeiten** – Diese Informationspflicht besteht, wenn es zum Streit mit dem Kunden kommt und dieser nicht beigelegt werden kann (§ 37 VSBG).

Platziert werden müssen diese Informationen im Impressum der Website und sofern vorhanden in den Allgemeinen Geschäftsbedingungen (AGB).

Inhaltlich setzen sich die Informationen aus folgenden Punkten zusammen:

- Hinweis und Link zur OS-Plattform (wenn Verbraucher mit Ihnen Verträge online schließen können).

- Hinweis, ob Sie an Streitbeilegungsverfahren teilnehmen (entweder freiwillig oder verpflichtend).

- Falls Sie am Streitbeilegungsverfahren teilnehmen, die Post- und die Webadresse der zuständigen Schlichtungsstelle.

Gesetzliche Vorgaben für die E-Mail-Archivierung

- Archivierung und Backup von E-Mails -

Häufig stellt sich die Frage, ob alle E-Mails in einem Unternehmen archiviert werden müssen, und wenn ja, wie lange. Zudem gestaltet sich die Unterscheidung zwischen einer Archivierung und einem Backup von E-Mails teils als schwierig.
Grundsätze für die Archivierung von E-Mails ergeben sich aus den GoBD (Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form, sowie zum Datenzugriff). In dieser Vorschrift sind die formellen Anforderungen an die Buchführung und die Aufbewahrung von steuerrechtlich relevanten elektronischen Daten

unter Bezug auf die Grundsätze ordnungsgemäßer Buchführung geregelt.

Von einem Daten-Backup spricht man in der Regel, wenn Daten kurz- bis mittelfristig zusätzlich gespeichert werden. Genutzt werden Backups insbesondere zur Wiederherstellung verloren gegangener Daten.

- Wichtig ist, dass ein Unternehmen in der Lage ist, jederzeit seine Daten aus dem Backup wiederherzustellen.

Eine Archivierung dagegen liegt bei einer langfristigen Speicherung von Daten auf einem separaten Datenträger vor. Im Vordergrund der Archivierung steht nicht die Wiederherstellung von Daten, sondern die Dokumentation.

Wie lange genau aufbewahrungspflichtige Daten auf einem separaten Datenträger gespeichert werden müssen, hängt ganz von der Art der Daten ab.

Aufbewahrungspflichtig sind nur solche E-Mails, die die Funktion eines Handels- bzw. Geschäftsbriefes oder eines Buchungsbeleges haben. Dient eine E-Mail jedoch als reines Transportmittel, beispielsweise, um einen Anhang zu übersenden, genügt eine Aufbewahrung des Anhangs (wobei das bloße Ausdrucken nicht ausreicht) und nicht der E-Mail selbst. Sobald sich aus der E-Mail zusätzliche Informationen ergeben, muss diese auch archiviert werden.

Zusätzlich müssen steuerrechtlich relevante von nicht steuerrechtlich relevanten E-Mails getrennt werden.

- Besonders bei der Archivierung ist zu beachten, dass die E-Mails unverändert archiviert werden. Insbesondere die Nutzung eines Dokumentenmanagement- oder Archivierungssystems, womit diese Unveränderbarkeit gewährleitet werden kann, und zudem protokolliert wann und inwieweit ein Dokument geändert wurde, sollte hier zum Einsatz kommen.

In der Praxis hängt es häufig vom Einzelfall abhängt, wie lange welche E-Mails und deren Inhalt gespeichert werden müssen. Sprechen Sie uns daher gerne an, wenn Sie sich unsicher sind, oder andere Fragen diesbezüglich haben.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de