von Rechtsanwalt **Jan Lennart Müller**

Achtung - Forderung von Schadensersatz bei DSGVO-Verstoß: SSL-Verschlüsselung des Online-Shops ist angeraten

Nachdem die Datenschutz-Grundverordnung am 25.05.2018 in Kraft getreten ist, kursieren bereits die ersten Abmahnungen zu diesem Thema. Besonders bemerkenswert sind allerdings die Forderungsschreiben nach Zahlung eines Schadensersatzes im Falle der Nicht-Verschlüsselung von Kontaktformularen. Was es hiermit auf sich hat, lesen Sie in unserem heutigen Beitrag.

Hintergrund

Bislang ist noch umstritten, ob Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) im Rahmen wettbewerbsrechtlicher Abmahnungen verfolgt werden können. Es bleibt abzuwarten, ob die Rechtsprechung einen Verstoß gegen Normen der DSGVO als Wettbewerbsverstoß qualifizieren wird.

Neben den bekannten Abmahnungen führte das Fordern von Schadensersatz bei Verstößen bislang ein Schattendasein. Nunmehr existieren die ersten Forderungsschreiben, welche im Falle von datenschutzrechtlichen Verstößen einen Schadensersatz geltend machen. Hierbei stützen sich die Schreiben auf die Vorschrift des Art. 82 Abs. 1 DSGVO, dieser lautet wie folgt:

> *"Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter."*

Schadensersatz bei Datenschutzverstößen?

Die geforderten Schadensersatzsummen belaufen sich auf hohe vierstellige bis hin zu fünfstelligen Summen! Hierbei bleibt abzuwarten, ob diese Forderung zum einen gerichtlich geltend gemacht werden und zum anderen wie die Gerichte mit diesen Forderungen umgehen werden. Die IT-Recht Kanzlei betrachtet die Forderungen derart hoher Schadensersatzforderungen als äußerst kritisch.

Zwar ermöglicht die DSGVO im Falle von Verstößen auch die Verhängung von Bußgeldern durch die entsprechenden Datenschutzaufsichtsbehören. Derartige Bußgelder verfolgen allerdings die Intention den Verstoßenden zu disziplinieren und eingetretene Nachteile zu bestrafen.

Schadensersatz wird hingegen nicht Datenschutzaufsichtsbehörden geltend gemacht, sondern von einer natürlichen Person. Notwendig ist hierbei zumindest ein sog. immaterieller Schaden. Ein solcher liegt dann vor, wenn eine Beeinträchtigung des Persönlichkeitsrechts, etwa in Form von psychischen Auswirkungen, der betroffenen Person durch den Datenschutzverstoß, vorliegt. Nach der bisherigen Rechtsprechung genügt für einen immateriellen Schaden allerdings nicht irgendein Eingriff in das Persönlichkeitsrecht des Betroffenen.

Vielmehr ist ein **schwerwiegender Eingriff** Voraussetzung für einen immateriellen Schaden. Darüber hinaus ist notwendig, dass die Beeinträchtigung nicht in anderer Weise befriedigend ausgeglichen werden kann. Hierbei spielen die **persönlichen Befindlichkeiten keine Rolle**, vielmehr bemisst sich die schwere einer Persönlichkeitsverletzung an **objektiven Kriterien**, wie die Bedeutung und Tragweite des Eingriffs, ferner der Anlass und Beweggrund des Verstoßenden sowie der Grad seines Verschuldens.

Es bleibt abzuwarten, ob bzw. in welchen Fällen die Gerichte Schadensersatzansprüche im Falle gewisser Datenschutzverstöße bejahen werden.

Vermeidung von datenschutzrechtlichen Risiken

Die uns vorliegenden Schadensersatzforderungen betreffen Fälle des Bereitstellens von Kontaktformularen ohne SSL-Verschlüsselung. Was aber ist die SSL-Verschlüsselung, wann und wie sollte diese eingesetzt werden?

Was ist eine SSL-Verschlüsselung?

Das SSL (kurz für: "Secure Sockets Layer") ist ein hybrides Verschlüsselungsprotokoll, mittels dessen personenbezogene Daten durch die Einbindung von Zertifikaten in Domains kodifiziert und so vor Drittzugriffen bei der Eingabe und im Transferprozess geschützt werden. Die Technologie ist in den letzten Jahren zum weltweiten Verschlüsselungsstandard aufgestiegen und zeichnet sich vor allem dadurch aus, dass sie eine wenig zeit- und kostenintensive Einbettung ermöglicht und die eingegeben Daten mit einem Verfahren verschlüsselt, das - theoretisch - einzig den bestimmungsgemäßen Empfänger zur Dekodierung befähigt.

Der Einsatz der SSL-Verschlüsselung ist für den Nutzer dadurch erkennbar, dass beim Aufrufen der jeweiligen URL das normale Übertragungsprotokoll "http" um ein "s" (für das englische "secure" = sicher) erweitert ist. Auf dem Markt kursieren derzeit verschiedene Zertifikate der SSL-Technologie, deren Vorzugswürdigkeit sich vor allem nach der Struktur der jeweiligen Internetpräsenz bemisst.

Verschlüsselung bereits nach alter Rechtslage gefordert

Das Bayerische Landesamt für Datenschutzaufsicht (LDA Bayern) war bereits unter Geltung des ehemaligen BDSG der Ansicht, dass Webseitenbetreiber die Übertragung sensibler Kundendaten mittels Kontaktformularen verschlüsseln müssten. Zudem forderte die LDA Bayern Webseitenbetreiber zu einer entsprechenden Umstellung der Kontaktformulare auf.

Das LDA Bayern stützte seine Auffassung zur alten Rechtslage auf § 9 BDSG, wonach öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen haben, um diese Daten zu schützen. Erforderlich sind solche Maßnahmen allerdings nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

In der Anlage zu § 9 BDSG war normiert, welche Ziele die Maßnahmen verfolgen müssen. Sie gewährleisteten, dass personenbezogene Daten bei der elektronischen Übertragung, während des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierfür sind Verschlüsselungsverfahren nach dem Stand der Technik zu verwenden.

Welche Verschlüsselungsverfahren dabei tatsächlich eingefordert werden dürfen, hänge nach der Ansicht der LDA Bayern davon ob, wie der Stand der Technik zu bewerten ist. Die Verwendung einer Verschlüsselung mit "https" sei inzwischen weit verbreitet und entspreche hierbei den rechtlichen Forderungen des LDA Bayerns.

Verschlüsselung auch nach DSGVO gefordert

Auch unter Geltung der DSGVO sollte eine Verschlüsselung insbesondere bei Kontaktformularen (und des Check-Out-Prozesses) durchgeführt werden:

Art. 5 lit f. DSGVO schreibt bei der Verarbeitung von Daten den sogenannten Grundsatz der **Integrität und Vertraulichkeit** vor. Danach müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Der Grundsatz der Integrität und Vertraulichkeit wird durch Art. 32 Abs. 1 Satz 1 Hs. 2 lit. a und lit. b konkretisiert, der einen **Maßnahmenkatalog** mit dem Ziel enthält, Gefahren für Daten durch Dritte abzuwehren. Dieser regelt:

> *"Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."*

Zudem nennt Art. 32 Abs. 1 Satz 1 Hs. 2 DSGVO konkrete Maßnahmen, die die Datensicherheit sicherstellen sollen. Dazu gehören

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Hieraus folgt: Das Gesetz erachtet die Verschlüsselung als geeignete technische und organisatorische Maßnahme, um die Datensicherheit sicherzustellen. Dementsprechend müssen Formulare im Online-Shop verschlüsselt sein, damit dort eingegebene Daten nicht abgegriffen werden können.

Wann sollte eine Verschlüsselung stattfinden?

Wie oben bereits herausgestellt, sollte dort, wo personenbezogene Daten verarbeitet werden, eine Verschlüsselung stattfinden. Hierbei sollte also zumindest beim Kontaktformular und im Rahmen des Bestellvorgangs (Check-Out) eine Verschlüsselung der Daten vorgenommen werden.

Grundsätzlich wäre es wohl zielführend, wenn die gesamte Internetseite verschlüsselt wird, da ein Mehraufwand hiefür kaum gegeben ist. Zudem ist auch aus Sicht der Platzierung der eigenen Internetseite in Suchmaschinen zu berücksichtigen, dass Google (wohl) Seiten mit Verschlüsselung besser rankt, als Seiten ohne Verschlüsselung (so zumindest ein Statement von Google aus dem Jahre 2014). Zudem hatte Google bereits anklingen lassen, dass das Internet "safe by defaul" sein sollte, also "standardmäßig sicher". Es gibt daher gleich eine doppelte Motivation für Internetseiten-Betreiber, die eigene Seite zu verschlüsseln.

Fazit

Bereits unter Geltung des BDSG war das LDA Bayern der Auffassung, dass zumindest bei einem Online-Kontaktformular eine SSL-Verschlüsselung vorliegen müsse. Unter Geltung der DSGVO hat sich hieran nichts geändert, gemäß Art. 5 lit f. i.V.m. Art. 32 Abs. 1 Satz 1 Hs. 2 DSGVO wird die **Integrität und Vertraulichkeit** der Datenverarbeitung gefordert. Diese Vorgabe wird durch die Forderung präzisiert, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird.

Die DSGVO erachtet die SSL-Verschlüsselung als geeignete technische und organisatorische Maßnahme, um die Datensicherheit sicherzustellen. Hiernach sollten Online-Händler im bestmöglichen Fall ihre komplette Internetseite SSL-verschlüsseln, zumindest aber die Bereiche, in denen personenbezogene Daten der Kunden verarbeitet werden, wie das Kontaktformular und der Bestellprozess, sollten SSL-verschlüsselt werden.

Autor:
RA Jan Lennart Müller
Rechtsanwalt