von Rechtsanwalt **Jan Lennart Müller**

FAQ zur Datenschutz-Grundverordnung im E-Commerce

Mit Geltung der Datenschutzgrundverordnung (DSGVO) zum 25.05.2018 werden Online-Händler mit einer Reihe von Neuerungen konfrontiert. Bis zu diesem Datum müssen Online-Händler alle Strukturen und Prozesse zur Implementierung des nun EU-weit einheitlich geltenden und harmonisierten Datenschutzes angepasst haben. Wir nehmen uns der Thematik an und beantworten nachfolgend die wichtigsten und gängigsten Fragen im Zusammenhang mit den neuen datenschutzrechtlichen Regelungen:

Muss ich meine Datenschutzerklärung ändern?

Ja! Dieser Schritt ist unumgänglich. Online-Händler müssen ab dem 25.05.2018 komplett neu ausgerichtete Datenschutzerklärungen verwenden.

Die IT-Recht Kanzlei wird ihren Mandanten selbstverständlich rechtzeitig die neuen Datenschutzerklärungen (abgestimmt auf den jeweiligen Verkaufskanal) bereitstellen.

Was leistet die künftige Datenschutzerklärung der IT-Recht Kanzlei?

Die künftige Datenschutzerklärung der IT-Recht Kanzlei nach den Vorgaben der ab 25.5.2018 anzuwendenden Datenschutz-Grundverordnung gibt unseren Mandanten eine Vorlage, wie er seinen Informationspflichten zur rechtmäßigen Verarbeitung von personenbezogenen Daten nachkommen kann. Er kann diese Erklärung nach bewährtem Muster anhand der verschiedenen Optionsbausteine auf seine persönlichen Bedürfnisse individuell konfigurieren.

Diese Erklärung leistet unter anderem Folgendes:

- Sie definiert den sogenannten Datenverantwortlichen. Das ist entweder der Online-Händler selbst oder sein Unternehmen als juristische Person.
- Sie benennt für die verschiedenen Optionsbausteine die künftig notwendige Rechtsgrundlage zur Bearbeitung von personenbezogenen Daten des Kunden und die Weitergabe von solchen personenbezogenen Daten an Dienstleister oder Werbepartner. Sie regelt, wie mit der Erhebung von personenbezogenen Daten z.B. über Kontaktformulare oder Newsletter umzugehen ist.
- Sie benennt die Fälle, in denen eine Einwilligung des Nutzers erforderlich ist.
- Sie stellt klar, in welchen Fällen die Weitergabe von personenbezogenen Daten an Unternehmen in Drittstaaten zulässig ist.

- Sie stellt insbesondere klar, wann die Weitergabe von solchen Daten an die großen Werbepartner mit Sitz in den USA wie z.B. Facebook, Google zulässig ist.
- Sie ist mit diversen Handlungsanweisungen versehen , die den Mandanten das Verständnis und die Verwendung dieser Erklärung erleichtern wird.

Vor allem wird die neue Datenschutzerklärung alle Auskunftsrechte und Interventionsrechte des Nutzers (z.B. Recht auf Berichtigung, Löschung, etc.) aufführen.

Eine vollständige Belehrung des Nutzers über seine Rechte ist gerade in Hinsicht auf mögliche Abmahnungen besonders wichtig.

Mit dieser Datenschutzerklärung hat der Online-Händler zudem bereits einen wichtigen Teil der Angaben zum Verarbeitungsverzeichnis nachgewiesen. Wie unten dargestellt, muss auch der kleine Online-Händler ein solches Verzeichnis führen.

Weitere Informationen zur künftigen Datenschutzerklärung finden Sie hier.

Welche Vorgaben der Datenschutz-Grundverordnung sind zusätzlich zur Datenschutzerklärung zu erfüllen?

Die folgende Auflistung der wichtigsten zusätzlichen Pflichten richtet sich in erster Linie an kleinere und mittlere Online-Händler

Der Online-Händler muss ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten führen, in dem auch diverse Pflichtmaßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung aufgeführt sind.

Die Benennung eines sogenannten Datenschutzbeauftragten sowie die Durchführung einer Datenschutz-Folgenabschätzung betreffen in der Regel den kleineren und mittelgroßen Online-Händler nicht, wenn er weniger als 10 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt und werden daher hier nicht aufgeführt, lesen Sie hierzu diesen Beitrag der IT-Recht Kanzlei.

Der Online-Händler kann diese Aufgaben an einen externen Dienstleister delegieren. Das ist aber wegen der Kosten gerade für den kleinen und mittleren Online-Händler finanziell kaum machbar.

Wichtig: Die nachfolgenden Vorgaben sind meist intern gegenüber den Aufsichtsbehörden zu erfüllen. Die Erfüllung der genannten Vorgaben ist öffentlich kaum nachvollziehbar - daher sind in dem Zusammenhang Abmahnungen seitens Wettbewerber eher nicht zu erwarten. Allerdings sieht die Datenschutz-Grundverordnung erhebliche Bußgelder bei Nichtbeachtung dieser Vorgaben vor.

Im Folgenden sollen die genannten Vorgaben vorgestellt und dem Online-Händler Empfehlungen an die Hand gegeben werden, wie er künftig den Vorgaben für ein Verzeichnis von Verarbeitungsverzeichnis entsprechen soll.

Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten soll nachweisen, dass der Online-Händler sich entsprechend den Vorgaben der Datenschutz-Grundverordnung verhält. Das Verzeichnis ist den Aufsichtsbehörden auf Antrag vorzulegen.

Auch kleine Online-Onlinehändler müssen ein solches Verzeichnis führen, im Einzelnen s. hierzu diesen Beitrag der IT-Recht Kanzlei.

Das Bayerische Landesamt für Datenschutz hat der IT-Recht Kanzlei den Entwurf einer Mustervorlage für ein derartiges Verzeichnis übermittelt . Die IT-Recht Kanzlei wird diesen Entwurf bei der Formulierung einer Mustervorlage berücksichtigen, die insbesondere auf die spezifischen Belange von kleineren Online-Händlern eingehen soll.

Das Verzeichnis von Verarbeitungstätigkeiten muss auch die getroffenen Maßnahmen zur Gewährleistung der Datensicherheit und datenschutzfreundlicher Voreinstellungen enthalten.

Die Datenschutzgrundverordnung (Art. 25, Art. 32) bleibt zu der Frage ziemlich vage, was denn nun Maßnahmen der Datensicherheit und der datenschutzfreundlichen Voreinstellungen genau bedeuten. Nach Auskunft des bayerischen Landesamtes für Datenschutzaufsicht für soll hier von den Kriterien in der Anlage I des bisherigen § 9 Bundesdatenschutzgesetz ausgegangen werden. Diese können in einer Art Checkliste für den Online-Händler wie folgt zusammengefasst werden:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden

können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.
Weitere Hilfestellung ist möglich. Die IT-Recht Kanzlei wird sich um die Formulierung von vereinfachten Muster bemühen, die die besonderen Bedürfnisse von kleineren und mittelgroßen berücksichtigen.

Gerade kleineren Online-Händler soll nach der Intention der Datenschutzgrundverordnung über vereinfachte Standardmuster geholfen werden, die genannten Vorgaben einzuhalten. Ganz wichtig: Der Online-Händler soll nach der Intention der Datenschutzgrundverordnung die von ihm getroffenen Maßnahmen einer sogenannten Zertifizierungsstelle zur Genehmigung vorlegen können (Zertifizierung, Siegel, Prüfzeichen).

Allerdings ist hier bisher noch wenig geschehen. Nach einer Mitteilung des bayerischen Landesamtes für Datenschutzaufsicht werden auch nach dem 25.5.2018 keine bayerischen Zertifizierungsstellen zugelassen sein, ganz zu schweigen von der Entwicklung von standardisierten Zertifizierungsverfahren. Unsere Kritik hierbei: Die Aufsichtsbehörden haben gerade zur Unterstützung von kleineren Online-Händlern eine Obhutspflicht. Sie können nicht von Online-Händlern ab 25.5.2018 die Erfüllung der genannten Maßnahmen verlangen und andererseits den Online-Händlern solche Zertifizierungsverfahren vorenthalten.

Die IT-Recht Kanzlei wird zur weiteren Entwicklung von solchen Zertifizierungsverfahren berichten und darstellen, wie hier gerade kleineren Online-Händlern geholfen werden kann.

Können Kontaktformulare künftig weiter genutzt werden?

Ja, es können weiterhin Kontaktformulare verwendet werden. Sie benötigen auch hier einen Hinweis in Ihrer Datenschutzerklärung. Mandanten der IT-Recht Kanzlei werden selbstverständlich auf eine Datenschutzerklärung zurückgreifen können, die den Wunsch nach Nutzung von Kontaktformularen berücksichtigen.

Ferner müssen Kontaktformulare verschlüsselt werden, um den Vorgaben aus dem Grundsatz der Integrität und Vertraulichkeit (Art. 5 lit.f DSGVO) gerecht zu werden.

Sie möchten mehr erfahren, gerne hier.

Können in Zukunft weiterhin Cookies eingesetzt werden?

Ja, aber unter Vorbehalt. Es kommt auf den Einzelfall an. Zukünftig werden nämlich Cookies als personenbezogene Daten behandelt werden. Daher benötigt ein Online-Händler eine Rechtfertigung für den Einsatz von Cookies. Der Einsatz wird sich maßgeblich an Art. 6 Abs. 1 Satz 1 lit. f DSGVO ausrichten - hierbei ist ein „berechtigtes Interesse“ für den Einsatz von Cookies notwendig.

Erforderlich ist eine sorgfältig durchgeführte Interessenabwägung für die Beurteilung eines berechtigten Interesses. Wenn Sie die Datenschutzerklärung der IT-Recht Kanzlei beziehen, dann erhalten Sie in Bezug auf Cookies ausschließlich Datenschutzklauseln, die eine positive

Interessenabwägung durchlaufen haben.

In einzelnen Ausnahmefällen wird die Einholung einer Einwilligung notwendig werden, aber auch hier gilt: Die Datenschutzerklärungen der IT-Recht Kanzlei werden so konzipiert sein, dass genau mitgeteilt wird, wann und wie die Einwilligung eingeholt werden muss.

Weiterführende Informationen zu Cookies können hier abgerufen werden.

Können Social-Plugins in Zukunft weiterverwendet werden?

Lieber nicht. Die Ära von Social Plugins wird durch die DSGVO zwar nicht beendet. Da das Datenschutzrecht jedoch ab dem 25. Mai 2018 noch näher in den Fokus der Datenschützer gerückt wird, sollten Shop-Betreiber aktiv werden und entweder ganz auf Plugins verzichten oder auf die Shariff-Lösung zurückgreifen.

Weitere Informationen zu Social-Plugins in Bezug auf die Datenschutz-Grundverordnung können Sie hier nachlesen.

Was ist zu beachten, wenn Sie Einwilligungen (z.B. für den Newsletterversand) einholen möchten?

Einwilligungen nach der DSGVO unterliegen strengen Vorgaben. Folgende Voraussetzungen werden Einwilligungen nach der DSGVO zu erfüllen haben:

- **Informiertheit:** Es wird z.B. zu beachten sein, dass in Zusammenhang mit Einwilligungen über die Identität des Datenverarbeiters (in der Regel der Online-Händler), die Zwecke der Datenverarbeitung und ein jederzeitiges, freies Widerrufsrecht zu informieren ist.
- Beachtung des sog. **Kopplungsverbots:** Unter Umständen können vertragliche Einigungsklauseln unwirksam sein, wenn diese sich auf Daten erstrecken, die für die Erfüllung des Vertrages **nicht erforderlich** sind. Es bleibt abzuwarten, wie die Gerichte dieses Kopplungsverbot beurteilen werden.
- „Klares Ungleichgewicht“:* Zudem sollen Einwilligungserklärungen in Zukunft unwirksam sein bei einem sogenannten „klaren Ungleichgewicht“ zwischen dem Verantwortlichen (= Online-Händler) und dem Betroffenen. Es bleibt auch hier abzuwarten, wann die Gerichte ein „klares Ungleichgewicht“ erblicken werden.
- **Widerrufsmöglichkeit:** Einwilligungserklärungen sind jederzeit mit Wirkung für die Zukunft frei widerruflich.
- **Form:** Die Einwilligung kann durch eindeutige, bestätigende Handlung in Form einer schriftlichen, elektronischen oder mündlichen Erklärung erfolgen (es genügt hierzu auch ein Mausklick).
- **Minderjährige:** Minderjährige unter 16 Jahren können keine wirksamen Einwilligungserklärungen abgeben (es kommt dann auf die Einwilligung der Erziehungsberechtigten an).

Nähere Informationen sind hier abrufbar.

Bleiben alte Einwilligungen wirksam?

Wohl ja. Nach dem Beschluss des Düsseldorfer Kreises (= Zusammenschluss der unabhängigen Datenschutzbehörden des Bundes und der Länder) sollen bisher rechtswirksame eingeholte Einwilligungen fortgelten. Jedoch soll besonders die Voraussetzung der Freiwilligkeit („Kopplungsverbot", Art. 7 Abs. 4 i.V.m. Erwägungsgrund (43) DSGVO) und die Altersgrenze von 16 Jahren (Art. 8 Abs. 1 i.V.m. Erwägungsgrund (38) DSGVO) Beachtung finden.

Können Daten in Drittländer (= außerhalb der EU) übermittelt werden?

An den Grundstrukturen zur Übermittlung von personenbezogenen Daten in Drittländer ändert sich durch die maßgeblichen Art. 44ff. DSGVO nicht viel. Wie bisher kommt es auch in Zukunft darauf an, ob im Drittland ein „angemessenes Datenschutzniveau" existiert. Sollte dies nicht der Fall sein, ist zu prüfen ob eine Ausnahme greift, um die Datenübertragung trotz Fehlens eines angemessenen Datenschutzniveaus zu rechtfertigen (zum Beispiel Datentransfer auf Grundlage von Standardvertragsklauseln, auf Grundlage von „Binding Corporate Rules", etc.). Allerdings ist für den praxisrelevanten Fall der Weitergabe von personenbezogenen Daten an Werbepartner in den USA das sog. EU- US „Privacy-Shield Abkommen" zu beachten. Danach ist die Weitergabe von Daten an US-Unternehmen nur zulässig, wenn diese Unternehmen in einem Anhang zu diesem Abkommen gelistet sind. Unsere Datenschutzerklärung berücksichtigt dieses Abkommen bei den einzelnen Optionsbausteinen.

Brauchen Online-Händler einen Datenschutzbeauftragten?

Bei kleineren Online-Händlern im Regelfall nein.

Ein Datenschutzbeauftragter ist nur erforderlich, wenn entweder

- mindestens 10 Personen ständig personenbezogene Daten **automatisiert** verarbeiten oder
- wenn Datenverarbeitungen vorgenommen werden, die eine Datenschutz-Folgenabschätzung unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt-oder Meinungsforschung verarbeitet werden - unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen. Diese zweite Alternative wird bei Online-Händlern im Regelfall nicht vorliegen.

Weitere Informationen zum Datenschutzbeauftragen nach der DSGVO finden Sie hier.

Was versteht man unter den sog. "Betroffenenrechten“?

Den betroffenen Personen (deren Daten erhoben werden), also nicht nur den Kunden, sondern auch den Nutzern der Webseite des Online-Händlers, stehen umfangreiche Rechte zu, die der Online-Händler zu beachten hat:

- Auskunftsrecht
- Recht auf Vergessenwerden (Löschungsrecht)
- Berichtigungsrecht
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht auf Einschränkung der Verarbeitung

Darum ist die oben dargestellte Datenschutzerklärung der IT-Recht Kanzlei, die diese Betroffenenrechte im Einzelnen auflistet, so wichtig.

Weitere Informationen finden Sie hier.

Können künftig Bonitätsprüfungen durchgeführt werden?

Ja. Wenn die Entscheidung über den Abschluss eines Vertrags von der Bonitätsprüfung abhängt (wie z.B. beim Rechnungskauf im Online-Shop), kann eine Bonitätsprüfung durchgeführt werden. Eine solche Bonitätsprüfung durch den Online-Händler oder einen von ihm beauftragten Zahlungsdienstleister ist ausdrücklich zulässig.

Was gilt im Falle einer Zuwiderhandlung gegen die datenschutzrechtlichen Vorschriften der DSGVO?

Verstoßen Online-Händler gegen die Vorgaben zur Auftragsverarbeitung, drohen Bußgelder bis zu 10 Millionen Euro oder von bis zu 2 % des gesamten weltweiten Jahresumsatzes - je nachdem, welcher Betrag der höhere ist. Bei schweren Verstößen gegen die Pflichten des Verantwortlichen (Art. 83 nennt hier Verstöße gegen Artikel 8, 11, 25 bis 39, 42, 43) sollen Geldbußen bis zu 20 Millionen Euro oder von bis zu 4% des gesamten weltweit erzielten unternehmerischen Jahresumsatzes verhängt werden können. Zudem drohen auch wettbewerbsrechtliche Abmahnungen.

Autor:
RA Jan Lennart Müller
Rechtsanwalt