

von Rechtsanwalt **Max-Lion Keller**, LL.M. (IT-Recht)

## Wie können sich Online-Händler auf die künftige Datenschutz-Grundverordnung vorbereiten?

Die Datenschutz-Grundverordnung kommt und ist ab 25.5.2018 für Online-Händler verpflichtend. Die Verordnung bringt eine verwirrende Fülle von neuen Pflichten, die Online-Händler beachten müssen. Zu Recht wird kritisiert, dass diese Verordnung zwar gut gemeint ist aber gerade den kleineren und mittleren Online-Händler unverhältnismäßig belastet.

Die IT-Recht Kanzlei will insbesondere den kleineren und mittleren Online-Händlern bei der Vorbereitung auf die neuen Vorgaben der Datenschutz-Grundverordnung helfen. In der aktuellen Übersicht, die keine Vollständigkeit anstrebt, sollen die für den Online-Händler wichtigsten Vorgaben der Datenschutz-Grundverordnung und die Empfehlungen der IT-Recht Kanzlei zur Umsetzung vorgestellt werden. Viele Vorgaben werden bereits durch die künftige Datenschutzerklärung der IT-Recht Kanzlei abgedeckt, die sie ihren Mandanten in den kommenden Wochen zur Verfügung stellen wird.

### I. Was leistet die künftige Datenschutzerklärung der IT-Recht Kanzlei?

Die IT-Recht wird [ihren Mandanten](#) in den nächsten Wochen eine Datenschutzerklärung auf der Grundlage der Datenschutz-Grundverordnung zur Verfügung stellen. Diese künftige Datenschutzerklärung ist für den Online-Händler von **erheblicher Bedeutung** und regelt unter anderem Folgendes:

- Die künftige Datenschutz-Erklärung der IT-Recht Kanzlei definiert den sogenannten Datenverantwortlichen. Das ist entweder der Online-Händler selbst oder sein Unternehmen als juristische Person.
- Die künftige Datenschutzerklärung benennt für die verschiedenen Optionsbausteine die künftig notwendige Rechtsgrundlage zur Bearbeitung von personenbezogenen Daten des Kunden zur Weitergabe von solchen personenbezogenen Daten an Dienstleister oder Werbepartner. Die IT-Recht Kanzlei wird ihren Mandanten nach bewährtem Muster Optionsbausteine anbieten, die sie nach ihren Bedürfnissen individuell konfigurieren können.
- Die künftige Datenschutzerklärung regelt, wie mit der Erhebung von personenbezogenen Daten z.B. über Kontaktformulare umzugehen ist.
- Die künftige Datenschutzerklärung benennt die Fälle, in den eine Einwilligung des Nutzers erforderlich ist.
- Die künftige Datenschutzerklärung wird klarstellen, bei welchen der größeren Werbepartner mit Sitz in den USA die Weitergabe von personenbezogenen Daten zulässig ist.

- 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 von Wettbewerbern besonders wichtig.
- Die künftige Datenschutzerklärung wird mit diversen Handlungsanweisungen versehen sein, die den Mandanten das Verständnis und die Verwendung dieser Erklärung erleichtern wird.

## II. Welche Vorgaben der Datenschutz-Grundverordnung muss der Online-Händler zusätzlich zur Datenschutzerklärung 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.
- Der Online-Händler muss diverse Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung und datenschutzfreundlicher Voreinstellungen vornehmen.

Die Benennung eines sogenannten Datenschutzbeauftragten sowie die Durchführung einer Datenschutz-Folgenabschätzung betreffen in der Regel den kleineren und mittleren Online-Händler nicht 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.

Im Folgenden sollen die genannten Vorgaben vorgestellt und dem Online-Händler Empfehlungen an die Hand gegeben werden, wie er künftig diesen Vorgaben entsprechen soll.

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.

## 1. 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 Onlinehändler müssen ein solches Verzeichnis führen, im Einzelnen s. hierzu diesen [Beitrag der IT-Recht Kanzlei](#).

Nach einer Mitteilung des Bayerischen Landesamt für Datenschutz soll noch im Januar 2018 eine entsprechende Mustervorlage für ein derartiges Verzeichnis veröffentlicht werden. Die IT-Recht Kanzlei wird hierzu berichten und prüfen, ob diese Mustervorlage auf die spezifischen Belange von kleineren Online-Händlern eingeht.

## 2. Maßnahmen zur Gewährleistung der Datensicherheit und datenschutzfreundlicher Voreinstellungen

Die Datenschutzgrundverordnung (Art. 25, Art. 32) bleibt zu der Frage ziemlich vage, was denn nun Maßnahmen der Datensicherheit und der datenschutzfreundlichen Voreinstellungen genau bedeuten. §§ 64, 71 Bundesdatenschutzgesetz neu (Geltung ab 25.5.2018) geben hier wesentlich detailliertere Kriterien vor. Diese Vorschriften gelten zwar eigentlich für öffentliche Stellen und nicht für Privatpersonen oder private Unternehmen. Mangels anderer Durchführungsvorschriften sind sie aber auch für Online-Händler sehr hilfreich. Diese Anforderungen können in einer Art Checkliste für den Online-Händler wie folgt zusammengefasst werden:

- Verwehrung des Zugangs Dritter zu IT-Systemen des Online-Händlers,
- Verhinderung des unbefugten Lesens, Kopierens und der Veränderung von Datenträgern,
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten,
- Verhinderung der Nutzung automatisierter Verarbeitungssysteme durch Unbefugte,
- Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt werden,
- Gewährleistung, dass nachträglich überprüft werden kann, welche personenbezogenen Daten eingegeben oder verändert worden sind,
- Gewährleistung, dass bei der Übermittlung von Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden können,
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden,
- Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können,
- Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,
- Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind,

- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können,
- Gewährleistung, dass mit Hilfe der Pseudonymisierung und Verschlüsselung personenbezogener Daten ein angemessenes Schutzniveau hinsichtlich personenbezogener Daten sichergestellt ist,
- Gewährleistung, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme sichergestellt ist,
- Gewährleistung, dass personenbezogene Daten bei einem Zwischenfall rasch wiederhergestellt werden können,
- Gewährleistung, dass Daten nach den Grundsätzen der Datensparsamkeit verarbeitet werden,
- Über Voreinstellungen sicherstellen, dass nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist,
- Über Voreinstellungen sicherstellen, dass Daten nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

Eine solche Checkliste ist einstweilen eine wertvolle Orientierungshilfe für den kleineren Online-Händler.

Weitere Hilfestellung ist möglich. Gerade kleineren Online-Händlern 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.

Autor:

**RA Max-Lion Keller, LL.M. (IT-Recht)**

Rechtsanwalt