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

Das Verarbeitungsverzeichnis: müssen Online-Händler nach künftiger Datenschutz-Grundverordnung vorweisen können

Auch kleinere Online-Händler müssen ab Geltung der Datenschutz-Grundverordnung (25. Mai 2018) ein Verzeichnis der Verarbeitungstätigkeiten führen, um die Einhaltung der Vorgaben der Datenschutz-Grundverordnung nachzuweisen. Eine Nichtbeachtung dieser Pflicht kann mit hohen Bußgeldern geahndet werden. Wie sollen insbesondere kleinere Online-Händler, die mit den komplizierten Vorgaben der Datenschutz-Grundverordnung nicht vertraut sind, dieser Pflicht genügen? Wenn Sie mehr dazu wissen wollen, dann lesen Sie den folgenden Beitrag.

(Die Datenschutz-Grundverordnung wird im Folgenden nur mit dem jeweiligen Artikel oder Erwägungsgrund zitiert.)

1. Pflicht zum Führen eines Verarbeitungsverzeichnis (Art. 30)

Online-Händler sind nach der ab 25. Mai 2018 geltenden Datenschutz-Grundverordnung als sogenannte Verantwortliche verpflichtet, unter anderem ein Verarbeitungsverzeichnis zu führen, Art. 30 (zu den Pflichten des Verantwortlichen siehe hier). Diese Pflicht **trifft ohne Ausnahme auch kleinere Online-Händler**, die mit den komplizierten Vorgaben der Datenschutz-Grundverordnung nicht vertraut sind. Es gibt keine Privilegierung mehr für Kleinunternehmen. Bisher mussten Kleinunternehmen ein solches Verzeichnis nicht führen. Dieses Verzeichnis muss den zuständigen Aufsichtsbehörden allerdings nur auf Anfrage vorgemeldet werden (Art. 30 Abs.4). Es entfallen künftig die bisherigen Meldepflichten an die Aufsichtsbehörde (§ 4 Bundesdatenschutzgesetz, geltende Fassung bis Mai 2018)

Das Verarbeitungsverzeichnis soll so praktisch die Erfüllung aller Pflichten der Online-Händler als Verantwortliche dokumentieren, um den Aufsichtsbehörden die Überprüfung zu erleichtern. Es ist schriftlich und in deutscher Sprache zu führen. Wenn Eintragungsänderungen erfolgen, sollte dies dokumentiert werden.

Fit für die Datenschutz-Grundverordnung 2018

Die IT-Recht Kanzlei stellt ihren Mandanten selbstverständlich ab April 2018 Folgendes zur Verfügung:

1. Professionelle Datenschutzerklärung, welche den umfangreichen Anforderungen der Datenschutz-Grundverordnung vollumfänglich entspricht.

2. Ein Muster (inklusive detaillierter Handlungsanleitung) für das obligatorische Verzeichnis für Verarbeitungstätigkeiten.

3. Checkliste und ein Muster für die Datenschutzfolgenabschätzung

4. Muster für die Dokumentation im Falle einer Datenpanne

5. Eine Handlungsanleitung, die sich mit folgenden Themen auseinandersetzt:

- der richtige Umgang mit Newslettern und die sichere Einholung von Einwilligungen
- der rechtskonforme Einsatz von Google-Analytics
- wie bindet man Videos richtig ein
- Verwendung von Bannern und Pop-Ups zur Information über Cookies
- wann und wie können Telefonnummern an Paketdienstleister zu Ankündigungszecken weitergeleitet werden
- unter welchen Voraussetzungen können Kundenfeedback-Anfragen versendet werden
- und vieles mehr!

Weitere Informationen hierzu finden Sie in unserem aktuellen Beitrag: Die Datenschutz-Grundverordnung kommt – mit den Schutzpaketen der IT-Recht Kanzlei sind Sie bestens vorbereitet!

2. Vorgeschriebener Inhalt eines Verarbeitungsverzeichnis (Art. 30 Abs. 1)

- Namen und Kontaktdaten des Verantwortlichen;
- Zweck der personenbezogenen Verarbeitung;
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländer (vor allem USA);
- Angaben zur Übermittlung von personenbezogenen Daten an ein Drittland (hier sind vor allem die USA gemeint);
- Wenn möglich Fristen für die Löschung der verschiedenen Datenkategorien;
- Beschreibung der technischen und organisatorischen Maßnahmen, wie personenbezogene Daten geschützt werden sollen.

Diese Dokumentationspflichten, denen Online-Händler hier unterworfen sind, sind umfassend und überfordern kleinere Online-Händler, die mit den Vorgaben der Datenschutzgrund-Grundverordnung nicht vertraut sind.

Im Einzelnen

Namen und Kontaktdaten des Verantwortlichen

Dies ist relativ einfach darzulegen. Der Online-Händler muss sich entscheiden, wer nun Verantwortlicher ist. Wie im o.g. Beitrag erläutert wurde, ist es zweckmäßig, hier das Unternehmen des Online-Händlers als Verantwortlichen anzugeben. Es muss die vollständige postalische Adresse einschließlich Telefonnummer und E-Mail-Adresse genannt werden.

Zweck der Verarbeitung

Für Online-Händler liegt in der Regel der Zweck der Verarbeitung von personenbezogenen Daten im Online-Verkauf von Produkten. Zu nennen sind hier aber auch Nutzung von personenbezogenen Daten zu Werbezwecken.

Kategorien der betroffenen Personen und Kategorien der personenbezogenen Daten

Hier sind als betroffene Personen die Kunden des Online-Händlers und die Bestelldaten zu nennen. Sensitive Daten wie Gesundheitsdaten sind hervorzuheben.

Kategorien von Empfänger

Hier ist sind alle Stellen oder Personen anzugeben, an die Daten weitergegeben werden (Transportdienstleister, Bezahldienstleister mit und ohne Bonitätsprüfung, Versand-Apotheken, wenn es um Patientendaten geht und Dienstleister, die von Online-Händlern mit den Aufgaben der Datenschutz-Grundverordnung betrauet sind („Auftragsverarbeiter“), aber auch Dritte, die diese Daten für Werbezwecke nutzen (Tracking, Profiling, Analysedienste, etc.). Wichtig ist in diesem Zusammenhang die Weitergabe von Daten an Stellen im Drittland (vor allem in den USA).

Übermittlung von personenbezogenen Daten an ein Drittland

Bei Weitergabe von personenbezogenen Daten an Dritte, die in einem Drittland wohnen, muss jeweils gesondert das Drittland genannt werden, in das Daten übermittelt werden. Eine Übermittlung in Drittländer erfolgt auch, wenn sich dort der Server befindet oder der E-Mail-Verkehr hierüber abgewickelt wird. Dies ist besonders relevant für die USA. Hier ist das EU-USA Privacy Shield Abkommen zu beachten.

Fristen für die Löschung der verschiedenen Datenkategorien

Nach Art. 17 Abs. 1 lit. a müssen personenbezogene Daten unverzüglich gelöscht werden, wenn sie für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr erforderlich sind. Normalerweise entfällt die Notwendigkeit einer Speicherung mit der Abwicklung des Kaufs, es sei denn es liegen gesetzliche Aufbewahrungsfristen (Steuerrecht, Handelsrecht) vor oder der Betroffene hat in die weitere Speicherung eingewilligt. Es gibt als keine starren Löschungsfristen. Dies macht es schwierig, Löschungsfristen im Verarbeitungsverzeichnis aufzunehmen.

Beschreibung der technischen und organisatorischen Maßnahme, wie personenbezogene Daten geschützt werden

Dies ist mit eine der schwierigsten Vorgaben der Datenschutz-Grundverordnung, da die durch den Online-Händler zu treffenden technischen und organisatorischen Maßnahmen zur Datensicherheit außerordentlich umfangreich und komplex sind und ohne externen Sachverstand kaum zu erfüllen sind . Es ist zu hoffen, dass Online-Händlern hier bald durch abgestimmte Verfahrensregeln und Zertifizierungsverfahren geholfen werden kann. Die IT-Recht Kanzlei wird hierzu berichten.

3. Wie kann Online-Händlern beim Führen eines Verarbeitungsverzeichnisses geholfen werden?

Die IT-Recht Kanzlei wird ihren Mandanten (wohl Anfang April) einen Verarbeitungsverzeichnis-Generator zur Verfügung stellen, über den ein gesetzeskonformes Verarbeitungsverzeichnis in wenigen Schritten realisiert werden kann. Selbstverständlich fallen dadurch keine weitere Kosten an.

Autor:
RA Max-Lion Keller, LL.M. (IT-Recht)
Rechtsanwalt