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

Pflichten von Online-Händlern als Datenverantwortliche nach der künftigen Datenschutzgrundverordnung

Den Datenverantwortlichen trifft ab dem 25.5.2018 nach der künftigen unmittelbar geltenden EU-Datenschutzgrundverordnung die umfassende Verantwortung und Haftung für die Verarbeitung von personenbezogenen Daten. Bei Zuwiderhandeln können ihn drakonisch hohe Bußgelder treffen. Der Online-Händler sieht sich so ab dem 25.5.2018 mit einer Unzahl von schwierigen Fragen konfrontiert. Wer genau ist der Verantwortliche? Welche Pflichten kommen auf ihn zu? Können seine Pflichten an Dritte delegiert werden? Welcher Haftungsmaßstab gilt?

Der folgende Beitrag will zu diesen Fragen im Frage & Antwort Modus detailliert Stellung nehmen. Artikel der Datenschutzgrundverordnung werden im Folgenden ohne Verweis zitiert.

Zu beachten ist, dass die Datenschutz-Grundverordnung in Deutschland durch das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (Anpassungsgesetz) ergänzt und konkretisiert wird, das ebenfalls ab dem 25.05.2018 gelten wird. Auf dieses Gesetz wird noch im Einzelnen zurückzukommen sein.

I. Begriff des Datenverantwortlichen

Frage: Wer ist der Verantwortliche?

Nach der Legaldefinition des Art. 4 Nr. 7 ist ein Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Datenverantwortlicher kann demnach das Unternehmen des Online-Händlers je nach rechtlicher Person (z.B. GmbH oder GBR), der Online-Händler als Einzelperson oder als Inhaber eines Unternehmens oder der Geschäftsführer des Unternehmens sein.

Praxistipp: Für Online- Unternehmen, die als juristische Person wie z.B. eine GmbH gegründet worden sind, ist es aus Haftungsgründen empfehlenswert, diese juristische Person selbst und nicht eine natürliche Person wie zum Beispiel den Geschäftsführer als Verantwortlichen auszuweisen. Denn nur der Verantwortliche haftet (s. dazu Kapitel 5). Es wäre daher möglicherweise schädlich, den Gesellschafter einer GmbH oder den Geschäftsführer selbst einer solchen Haftung auszusetzen.

Frage: Ist ein Mitarbeiter des Online-Unternehmens, der unternehmensintern mit der Datenverarbeitung beauftragt ist, Datenverantwortlicher?

Verantwortlicher kann nur die Stelle (natürliche oder juristische Person) sein, der **wesentliche Entscheidungsbefugnis** für die Verarbeitung von personenbezogenen Daten zukommt. Dies trifft für den Mitarbeiter eines Online-Unternehmens nicht zu, der intern mit der Datenverarbeitung beauftragt ist. Verantwortlicher bleibt die benannte Stelle, also der Inhaber, der Geschäftsführer oder das Unternehmen in seiner jeweiligen rechtlichen Form.

Frage: Auf welche Weise wird der Verantwortliche benannt?

Es gibt keine Pflicht, den Verantwortlichen gegenüber einer öffentlichen Stellen zu benennen. Aber der Verantwortliche muss allgemein die Nutzer seiner Webseite über seine Kontaktdaten informieren (Art. 13) und muss zusätzlich im Verzeichnis der Verarbeitungstätigkeiten seine Kontaktdaten aufführen (Art. 30).

Frage: Sind Kleinunternehmen von einer solchen Informations- und Verzeichnispflicht ausgenommen?

Im Ergebnis nein.

Auch Kleinunternehmen müssen Ihre Kunden bei Erhebung von personenbezogenen Daten über die Kontaktdaten des Verantwortlichen informieren und im Pflichtverzeichnis der Verarbeitungstätigkeit den Verantwortlichen ausweisen.

Art. 30 Absatz 3 sieht zwar vor, dass Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, von der Verzeichnispflicht ausgenommen sind. Diese Ausnahme wird allerdings leider für Online-Händler nicht relevant, da sie nur bei gelegentlicher Datenverarbeitung greift. Die Erhebung und Verarbeitung von Kundendaten gehört jedoch zum Kerngeschäft von Online-Händlern.

Frage: Sind Verantwortliche auch Datenschutzbeauftragte?

Nein

Die Begrifflichkeit der Datenschutz-Grundverordnung unterscheidet klar zwischen

- einem Verantwortlichen und
- einem Datenschutzbeauftragten.

Ein Datenschutzbeauftragter ist durch den **Verantwortlichen zusätzlich** zu benennen, wenn die **Kerntätigkeit** von Online-Händlern in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Absatz 1, lit b) oder in der Verarbeitung von besonders sensitiven Daten (Art. 37 Absatz 1 lit c) besteht.

§ 38 Anpassungsgesetz konkretisiert die Kriterien für die Pflichtbenennung eines Datenschutzbeauftragten. Demnach ist bei der Fallgestaltung des Art. Absatz 1, lit b (umfangreiche und systematische Überwachung von betroffenen Personen) ein Datenschutzbeauftragter zu benennen, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung beschäftig sind.

Dies trifft auf Online-Händler im Regelfall nicht zu.

II. Pflichten des Verantwortlichen

Art 24 ist die Generalnorm für die umfassende Verantwortung des Datenverantwortlichen. Er hat geeignete technische und organisatorische Maßnahmen umzusetzen, um die Einhaltung einer rechtmäßigen Datenverarbeitung sicherzustellen und den Nachweis dafür zu erbringen. Die einzelnen Pflichten des Datenverantwortlichen gemäß Art 24, die in vielen Einzelvorschriften der Datenschutz-Grundverordnung konkretisiert werden, sollen im Folgenden vorgestellt werden:

- 1. Vornahme technisch-organisatorischer Maßnahmen, um die Zulässigkeit der Datenverarbeitung sicherzustellen (Art 24)
- 2. Vornahme von technisch-organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung, Art 32
- 3. Pflicht des Verantwortlichen, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung zu gewährleisten (Art 25)
- 4. Führen eines Verzeichnisses von Verarbeitungstätigkeiten, Art 30
- 5. Pflicht zur Information des Kunden bei Erhebung und Verarbeitung seiner personenbezogenen Daten (Art.12 ff)
- 6. Pflicht zur Übertragung von personenbezogenen Daten (Art. 20)
- 7. Durchführung einer Datenschutz-Folgenabschätzung
- 8. Meldung der Verletzung des Schutzes personenbezogener Daten (Art. 33, 34)

Im Einzelnen:

1. Vornahme technisch-organisatorischer Maßnahmen, um die Zulässigkeit der Datenverarbeitung sicherzustellen (Art 24)

Frage: An welche technisch-organisatorischen Maßnahmen ist hier zu denken?

Art 24 erläutert den Begriff technisch-organisatorische Maßnahmen nicht. Es ist hilfreich, auf den in § 9 Bundesdatenschutzgesetz (GDSG) benutzten Begriff der technisch-organisatorischen Maßnahmen zur Gewährleistung der notwendigen Sicherheits- und Schutzanforderungen zurückzugreifen. Dieser Begriff wird in der Anlage zu § 9 BDSG näher erläutert.

Demnach sind technische Maßnahmen, z.B.

- Umzäunung des Geländes
- Sicherung von Türen und Fenstern
- bauliche Maßnahmen allgemein
- Alarmanlagen jeglicher Art
- oder Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa Benutzerkonto, Passworterzwingung, Logging (Protokolldateien), biometrische Benutzeridentifikation

Demnach sind organisatorische Maßnahmen, z. B.

- Besucheranmeldung
- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Vier-Augen-Prinzip
- Festgelegte Intervalle zur Stichprobenprüfungen

2. Vornahme von technisch-organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung, Art 32

Art. 32 ist die einschlägige Vorschrift zur Sicherheit der Datenverarbeitung.

Frage: Welche Maßnahmen zur Gewährleistung der Datenverarbeitung werden in Art 32 aufgeführt?

Es müssen alle Maßnahmen zum organisatorischen und technischen Schutz der personenbezogenen Daten nach dem jeweiligen Stand der Technik ergriffen werden.

Beispielhaft werden in Art. 32 aufgeführt:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- Sicherstellung der Fähigkeiten von System und Diensten
- Wiederherstellung der Verfügbarkeit und des Zugangs zu Daten
- Verfahren zur Überprüfung der Gewährleistung der Sicherheit der Verarbeitung

Frage: Hat der Verantwortliche die Pflicht, getroffene organisatorisch-technische Maßnahmen zu überprüfen und zu aktualisieren?

Ja

Der Verantwortliche muss die getroffenen Maßnahmen und bei Anpassungsbedarf aktualisieren (Art. 24)

Frage: Kann durch die Einhaltung von Verhaltenskodizes und Zertifizierungsverfahren der Nachweis erbracht werden, dass den Pflichten des Verantwortlichen entsprochen ist?

Nach dem Wortlaut des Art. 24 darf die Einhaltung von Verhaltenskodizes und Zertifizierungsverfahren nur ein Indiz sein, dass den Pflichten des Verantwortlichen entsprochen wird (s. dazu auch Kapitel 5). Es obliegt den zuständigen Aufsichtsbehörden diesen entsprechend in eigener Verantwortung zu prüfen (s. Kommentar Ehmann/Selmayer, Art. 24 Rdr. 11). In der Praxis werden aber nach Ansicht der IT-Recht Kanzlei gerade bei der Routineüberprüfung von Online-Händlern solche Verhaltenskodizes und Zertifizierungsverfahren eine große Rolle spielen.

3. Pflicht des Verantwortlichen, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung zu gewährleisten (Art 25)

Frage: Was ist mit dieser Gestaltungspflicht gemeint?

Damit sind anerkannte Methoden und Modelle zum sog. "Privacy Design" und Privacy by Default" (datenschutzfreundliche Voreinstellungen) gemeint. Technische Prozesse sollen im Vorhinein mit dem Datenschutz in Einklang gebracht werden. Der Verantwortliche soll bereits bei der Planung eines Datenverarbeitungssystems den Gesichtspunkt des Datenschutzes berücksichtigen. Beispielhaft wären zu nennen Verschlüsselung, Datenschutzhinweise durch entsprechende Banner auf einer Webseite, Schulungsmaßnahmen der Mitarbeiter. Der Verantwortliche sollte ein schlüssiges Datenschutzkonzept vorweisen können.

Frage: Kann der Nachweis dieser Gestaltungspflicht durch die Einhaltung genehmigter Zertifizierungsverfahren erleichtert werden?

Ja, Art. 25 Abs. 3

4. Führen eines Verzeichnisses von Verarbeitungstätigkeiten, Art 30

Frage: Welche Angaben muss das Verzeichnis von Verarbeitungstätigkeiten gem. Art 30 und § 70 Anpassungsgesetz enthalten?

In Art. 30 wird ein detaillierter Katalog von Pflichtangaben aufgelistet. Wie bereits oben ausgeführt, gilt diese Verzeichnispflicht **auch für Kleinunternehmen**:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine 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 Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- Angaben über die Rechtsgrundlage der Verarbeitung
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

5. Pflicht zur Information des Kunden bei Erhebung und Verarbeitung seiner personenbezogenen Daten (Art.12 ff)

Frage: Welche Art von Informationspflichten treffen den Verantwortlichen?

Der Verantwortliche ist zu geeigneten Maßnahmen für eine transparente Informationspolitik verpflichtet und soll dem Betroffenen die Ausübung seiner Rechte erleichtern. Hierbei ist zu unterscheiden zwischen der Information zur Erhebung und Verarbeitung von personenbezogenen Daten die immer zu erfolgen hat und der Information, die nur auf Antrag des Betroffenen erfolgt.

Frage: Über welche Inhalte muss gem. Art. 13 antragslos informiert werden?

Der Verantwortliche hat zum Zeitpunkt der Erhebung personenbezogener Daten über folgende Inhalte zu informieren:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- Wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
-

das Bestehen eines Rechts, eine Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (zum Profiling, s.unten Ziffer 8) .

Tipp für die Praxis: Diese sehr umfangreichen Auskunftspflichten betreffen jeden Online-Händler. Ihnen kann in der Praxis nur in Form einer Datenschutzerklärung sachgerecht entsprochen werden, die auf der Webseite des Online-Händlers hinterlegt ist. Die IT-Recht Kanzlei stellt Ihren Mandanten künftig Texte für **Datenschutzerklärungen zur Verfügung, die diesen Informationsvorgaben der Datenschutzgrundverordnung vollumfänglich entsprechen**.

Frage: Über welche Inhalte muss der Verantwortliche den Betroffenen auf Anfrage in Form einer Einzelinformation unterrichten (Art. 15)?

Die antragslose Pflichtinformation (Art. 13) und die Pflichtinformation auf Antrag (Art 15) sind in ihren Inhalten weitgehend deckungsgleich. Es kann daher hier auf die antraglose Pflichtinformation verwiesen werden. Wichtig ist aber das Recht einer betroffenen Person, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden (Negativauskunft).

Frage: Können Einzelinformationen auf Antrag abgewiesen werden oder nur gegen Entgelt gegeben werden?

Einzelinformationen an Betroffene auf Antrag haben grundsätzlich unentgeltlich, in schriftlicher oder elektronischer Form und spätestens 1 Monat nach Antragstellung zu erfolgen (Art. 12). Der Verantwortliche kann sich bei offenkundig unbegründeten oder exzessiven Anträgen weigern, tätig zu werden oder ein angemessenes Entgelt. verlangen. Der Verantwortliche trägt die Beweislast, ob ein Antrag offensichtlich unbegründet oder exzessiv ist. Die Verweigerung einer Information oder die Koppelung mit einer Entgeltforderung sollte daher gut überlegt sein. Eine gewisse Beweislasterleichterung ist nach Erwägungsgrund 63 gegeben. Demnach sind Antragsbegehren exzessiv, wenn sie in unangemessen kurzen Abständen geltend gemacht werden. Beantragt der Antragsteller mehrere Kopien der Einzelinformation, so kann ein angemessenes Entgelt verlangt werden.

Frage: Welche weiteren Informationspflichten hat der Verantwortliche gegenüber dem Betroffenen zu erfüllen?

- Verpflichtung auf Antrag des Betroffen, unvollständige personelle Daten - auch mittels ergänzender Erklärung - zu vervollständigen (Art. 16).
- Verpflichtung, den Betroffen, der eine Einschränkung der Verarbeitung seiner Daten erwirkt hat, von einer Aufhebung der Einschränkung zu unterrichten (Art.18)
- Unterrichtung des Betroffenen über die Verletzung des Schutzes seiner Daten (Art. 34), hierzu im Einzelnen Ausführungen unter Ziffer 9.

6. Pflicht zur Übertragung von personenbezogenen Daten (Art. 20)

Frage: Was bedeutet die Pflicht zur Übertragung von personenbezogenen Daten?

Der Verantwortliche hat die Pflicht, dem Betroffenen auf Antrag die ihn betreffenden personenbezogenen Daten, die er dem Verantwortlichen bereitgestellt hat, in einer gängigen maschinenlesbaren Form herauszugeben und an einem anderen Verantwortlichen nach Wahl des Betroffenen zu übermitteln. Es ist also zwischen Herausgabe von Daten und Übermittlung von Daten zu unterscheiden. Der Betroffene kann seine personenbezogenen Daten auch selber an einen Verantwortlichen seiner Wahl übermitteln. Diese Pflicht betrifft jeden Online-Händler, der eine Webseite unterhält.

7. Durchführung einer Datenschutz-Folgenabschätzung

Frage: In welchen Fällen muss eine Datenschutz-Folgenabschätzung vor Datenverarbeitung durchgeführt werden, Art. 35?

Die **Pflicht zur Datenschutz-Folgenabschätzung trifft in der Regel den Online-Händler nicht**. Sie ist nur dann gegeben, wenn mit der Verarbeitung von Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen verbunden ist. Nach Erwägungsgrund 85 der Datenschutz-Grundverordnung ist damit z.B. das Risiko eines physischen, materiellen oder immateriellen Schadens, Identitätsdiebstahl, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, etc. gemeint. **Ausdrücklich ausgenommen** ist die bei Vorleistung des Online-Händlers übliche, automatisierte Bonitätsprüfung des Kunden durch Bezahldienste. Eine solche Bonitätsprüfung ist nach Art 22 Abs. 2 zulässig, da sie für den Abschluss eines Vertrages erforderlich ist. Die bloße Verweigerung eines Vertragsabschlusses ist keine Rechtsverletzung im Sinne des Art 35. Andernfalls würde der Grundsatz der Vertragsfreiheit faktisch ausgehebelt (s. auch Kommentar Gola, Art. 22 Rndr. 25).

Als Regelbeispiele einer erforderlichen Datenschutz-Folgenabschätzung nennt Art. 35 Abs. 3

- Es liegt eine eingriffsintensive und umfangreiche Verarbeitung von personenbezogenen, insbesondere von sensiblen Daten vor
- Es liegt eine systematische und umfangreiche Bewertung persönlicher Aspekte, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet. Hier gemeint ist z.B. ein Profiling im Rahmen von Arbeitsverhältnissen, aber nicht wie ausgeführt im Rahmen einer Bonitätsprüfung bei Onlineverträgen.

Frage: Was hat der Verantwortliche bei Erforderlichkeit einer Datenschutz-Folgenabschätzung zu tun?

a. Er hat die Aufsichtsbehörde zu konsultieren (Art. 36)

b. Die Folgenabschätzung enthält zumindest folgende Angaben, Art. 35

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

8. Meldung der Verletzung des Schutzes personenbezogener Daten (Art. 33, 34)

Frage: In welchen Fällen besteht gegenüber der zuständigen Aufsichtsbehörde eine Meldepflicht zur Verletzung personenbezogener Daten?

Eine Meldepflicht bei Verletzung des Schutzes von personenbezogenen Daten besteht in der Regel, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Das heißt aber, den Verantwortlichen trifft hier die Beweislast. Bei Unterlassen einer solchen Meldung hat er nachzuweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem solchen Risiko führt (Erwägungsgrund 85).

Tipp für die Praxis: Der Online-Händler ist daher im Zweifel gut beraten, mögliche Verletzungen des Schutzes personenbezogener Daten dem Bundesbeauftragten zu melden.

Frage: Wann sind solche Verletzungen des Datenschutzes der zuständigen Aufsischtsbehörde zu melden?

Unverzüglich und möglichst binnen 72 Stunden nach Kenntnisnahme (Art. 33)

Frage: Welche Informationen hat die Meldung an die Aufsichtsbehörde zu enthalten (Art. 33 Abs. 3)?

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Frage: Ist auch der durch die Datenschutzverletzung Betroffene zu benachrichtigen (Art. 34)?

Führt die Verletzung des Datenschutzes voraussichtlich zu einem hohen Risiko für den Betroffenen, so ist er unverzüglich zu unterrichten. Einer Benachrichtigung bedarf es nicht, wenn

- der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat,
- sichergestellt wurde, dass das hohe Risiko für die Rechte der betroffenen Person aller Wahrscheinlichkeit nicht mehr besteht,
- mit der Benachrichtigung der betroffenen Person ein unverhältnismäßiger Aufwand verbunden wäre.

III. Erleichterung des Nachweises der Pflichteneinhaltung des Verantwortlichen über genehmigte Verhaltensregeln und Zertifizierungsverfahren (Art. 42 ff)

Frage: Welche Zielsetzung haben Verhaltensregeln und Zertifizierungsverfahren?

Wie oben ausgeführt, werden auch kleinere Onlineunternehmen, die regelmäßig personenbezogene Daten verarbeiten, nicht von den Vorgaben der der Datenschutz-Grundverordnung entlastet. Die rechtliche Unbestimmtheit vieler Pflichten ist für Online-Händler wegen erheblicher Sanktionsdrohungen problematisch. Der Verordnungsgeber hat das Problem, dass gerade mittlere und Kleinunternehmen mit den Anforderungen der Datenschutzgrundverordnung überlastet werden, gesehen. Abhilfe sollen Verbände und Vereinigungen schaffen, die über genehmigte Verhaltensregeln und Zertifizierungsverfahren die Pflichten des Verantwortlichen präzisieren und seine Nachweispflicht erleichtern. Die Nachweispflicht gilt mit der Einhaltung von Verhaltensregeln und eines Zertifizierungsverfahrens (mit Datenschutzsiegel und -prüfzeichen) zwar nicht als erfüllt (s. dazu auch unten Kapitel 5), aber sie ist doch ein wichtiges Indiz, dass der Verantwortliche seine Pflichten erfüllt hat,

Frage: Wie ist das Verfahren für die Genehmigung von Verhaltensregeln und deren Überwachung ausgestaltet?

Als Antragsteller kommen Verbände in Betracht, die Onlinehändler vertreten. Sie sollen Verhaltensregeln ausarbeiten, die die branchenspezifischen Besonderheiten des Onlinehandels insbesondere die Bedürfnisse von kleineren und mittleren Onlineunternehmen berücksichtigen. Verhaltensregeln müssen ein förmliches Genehmigungsverfahren bei der zuständigen Aufsichtsbehörde des jeweiligen Bundeslandes durchlaufen. Die Überwachung, ob genehmigte Verhaltensregeln eingehalten werden, muss durch den Verband erfolgen. Der Verband kann die Überwachung aber auch an eine Überwachungsstelle delegieren, die einer Akkreditierung durch die zuständige Aufsichtsbehörde bedarf.

Frage: Wie ist das Zertifizierungsverfahren ausgestaltet?

Eine zugelassene Zertifizierungsstelle darf Zertifizierungen durchführen. Die zuständige Aufsichtsbehörde kann aber entscheiden, dass sie selber Zertifizierungen anbietet. Damit ist ein Interessenkonflikt nicht zu vermeiden. Ob dies auch der Intention des deutschen Anpassungsgesetzes entspricht, ist unklar. Das Zertifizierungsverfahren muss den besonderen Bedürfnissen der Kleinstunternehmen und Klein- und Mittelunternehmen entsprechen. Gem. § 39 Anpassungsgesetz soll die Akkreditierung durch die deutsche Akkreditierungsstelle (DAkks) im Einvernehmen mit der zuständigen Aufsichtsbehörde erfolgen.

Frage: Gibt es schon genehmigte Zertifizierungsverfahren und akkreditierte Zertifizierungsstellen?

Nach Kenntnis der IT-Recht Kanzlei ist hierzu aktuell nichts bekannt.

Frage: Gibt es schon genehmigte Verhaltensregeln von Verbänden der Online-Wirtschaft?

Nach Kenntnis der IT-Recht Kanzlei liegen derartige Verhaltensregeln bisher nicht vor.

Frage: Was ist mit den bisherigen Zertifikaten?

Es gibt bundesweit eine Vielzahl von Zertifizierungsverfahren zur Auftragsdatenverarbeitung. Eine Übersicht findet sich auf **der Webseite der Stiftung Datenschutz**.

Es ist unklar, welche Bedeutung diese alten Zertifikate im Kontext der künftigen Datenschutz-Grundverordnung haben werden. Jedenfalls genießen sie nicht die Nachweiserleichterung, dass der Verantwortliche seine o.g. Pflichten nach Datenschutz-Grundverordnung erfüllt hat und sind somit für die Onlinehändler im Kontext der Datenschutz-Grundverordnung faktisch wertlos.

Kommentar der IT-Recht Kanzlei: Genehmigte Verfahrens- und Zertifizierungsverfahren wären vor allem für kleinere Online-Unternehmen eine beträchtliche Erleichterung, die ohne solche Verfahren Angesicht des oben dargestellten umfangreichen Pflichtenkatalogs überfordert sind, zumal eine Nichtbeachtung der dargestellten Pflichten mit hohen Bußgeldern geahndet werden kann. Es ist daher verwunderlich, dass ein gutes halbes Jahr vor Geltung der neuen Vorschriften der Datenschutz-Grundverordnung noch nichts zu solchen Verfahren in Deutschland bekannt ist. Die gutgemeinten Empfehlungen in der Datenschutz-Grundverordnung zur Förderung gerade von kleineren und mittleren Unternehmen klingen da etwas hohl.

Hoffentlich werden solche Verfahren nun alsbald auf den Weg gebracht. Die IT-Recht Kanzlei wird hierzu berichten.

IV. Verarbeitung von personenbezogenen Daten im Auftrag des Verantwortlichen (Art. 28)

Die Beauftragung eines spezialisierten Dienstleisters mit der Einhaltung der Vorgaben der Datenschutz-Grundverordnung ist gerade für kleinere und mittlere Online-Unternehmen, die in der Regel nicht über die notwendige Sachkenntnis des Datenschutzrechts verfügen, äußerst praxisrelevant. Die Datenschutz-Grundverordnung hat dem Rechnung getragen und die Beauftragung eines sogenannten Auftragsverarbeiters durch den Verantwortlichen in Art. 28 geregelt. Art. 28 will vor allem datenschutzrechtliche Standards bei der Auswahl und der Beauftragung des Auftragsverarbeiters regeln.

Frage: Welche Kriterien muss der Verantwortliche bei der Auswahl des Auftragsverarbeiters beachten?

Der Verantwortliche darf nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichende Garantien zur Durchführung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten bieten.

Praxistipp: Da für Online-Händler die Einschätzung schwierig ist, ob ein Auftragsverarbeiter diese Garantien bieten kann, sollten sie von der Möglichkeit des Art. 28 Abs. 5 Gebrauch machen. Online-Händler sollten nur Dienstleister als Auftragsverarbeiter einsetzen, die die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahren gewährleisten können. Es sollte im Interesse solcher Dienstleister sein, auf baldige deutsche Regeln für Verhaltensregeln und für ein Zertifizierungsverfahren zu drängen.

Frage: Welche Inhalte muss ein Vertrag des Verantwortlichen mit dem Auftragsverarbeiter haben?

Art. 28 nennt einen umfänglichen Katalog von Pflichtangaben zu Gegenstand, Dauer des Vertrages. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Person und den Rechten und Pflichten des Datenverantwortlichen. Der Vertrag muss schriftlich abgeschlossen sein.

Praxistipp: Auch hier gilt die Empfehlung, von der Möglichkeit der Anwendung von Standardverträgen Gebrauch zu machen. Um sicherzustellen, dass solche Standardverträge die geforderten Regelungsinhalte nach Art. 28 enthalten, sollten diese Standardverträge zertifiziert sein (zu entsprechenden Musterverträgen, s. z.B. Bitcom https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/EU-DSGVO/Datenschutzkonforme-Datenverarbeitung.html).

V. Haftung des Verantwortlichen (Art. 82)

Frage: In welchen Fällen haftet der Verantwortliche?

Der Verantwortliche haftet für Schäden, die einer Person aufgrund einer Datenverarbeitung entstehen, die mit der Datengrundschutz-Verordnung oder dem deutschen Anpassungsgesetz nicht in Einklang stehen (Erwägungsgrund 146). Anspruchsberechtigt ist daher nicht nur der Kunde, sondern z.B. auch der Besucher der Webseite des Onlineshops, der keine Ware bestellt aber auf Grund seines Besuches personenbezogene Daten hinterlässt.

Frage: Muss die betroffene Person die Rechtswidrigkeit der Datenverarbeitung und das Verschulden der Verantwortlichen nachweisen?

Nein

Hier ist die Nachweispflicht zu Lasten des Verantwortlichen erheblich erleichtert oder die Beweislast umgekehrt.

Die einen Schaden geltend machende Person muss nur insoweit die Rechtswidrigkeit der Datenverarbeitung darlegen, wie ihm dies ohne Einblick in die internen Datenverarbeitungsprozesse möglich ist. Er muss also nur Anhaltspunkte für einen Datenschutzverstoß benennen (s. Kommentar Gola, Art. 82, Rdnr, 15). Gemäß Art. 82 Abs. 3 muss der Verantwortliche (und nicht der Geschädigte) nachweisen, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Frage: Wer muss den Schaden nachweisen?

Der Geschädigte muss nachweisen, dass ihm durch die rechtswidrige Verarbeitung von Daten durch den Verantwortlichen ein Schaden entstanden ist. Dabei reicht es aus zu beweisen, dass die Datenverarbeitung grundsätzlich geeignet war, den Schaden auszulösen.

Den Betroffenen trifft allerdings die volle Beweislast, dass ein Schaden entstanden ist und in welcher Höhe (s. Kommentar Bucher/Kühling, Art. 82 Rdnr. 20, 48).

Frage: Welche Art von Schäden sind zu erstatten

Grundsätzlich sind Vermögensschäden erstattungspflichtig. Typische Schäden, die im Rahmen der Tätigkeit von Onlineshops auftreten könnten sind Schäden wegen Vertragsverweigerung auf Basis falscher Bonitätswerte, Mehrkosten wegen eines negativen Schufa-Scores, der wegen Vertragsverweigerung auf Grund falscher Bonitätswerte entstanden sind (s. Kommentar Bucher/Kühling a.a.O.).

Zu erstatten sind auch Schäden, die mittelbar entstehen wie die Kosten der Rechtsverfolgung, Anwaltskosten bei Beschwerden gegenüber der Beschwerdebehörde (s. Kommentar Bucher/Kühling, Art. 82, Rdnr. 19).

Frage: Können auch immaterielle Schäden gelten gemacht werden?

Nach bisheriger deutscher Rechtsprechung, die auch dem bisherigen § 8 Abs. 2 Bundesdatenschutzgesetz entspricht, konnten immaterielle Schäden nur bei schwerwiegenden Persönlichkeitsverletzungen geltend gemacht werden. § 8 Bundesdatenschutzgesetz wird mit Geltung der Datenschutz-Grundverordnung aufgehoben. Art. 82 Abs. 1 verpflichtet ausdrücklich auch zu einem Ersatz eines immateriellen Schadens. Die bisherige Einschränkung auf schwerwiegende Persönlichkeitsverletzungen wird dann wohl nicht mehr gelten.

Es bleibt abzuwarten, wie die künftige Rechtsprechung den Art 82 Abs. 1 auslegen wird und ob künftig bei Datenschutzverletzungen signifikante Schmerzensgelder zugesprochen werden.

Frage: Haftet der Verantwortliche für das Handeln seiner Mitarbeiter?

Ja

Er muss sich deren Tätigkeit zurechnen lassen, ohne sich entlasten zu können.

Frage: Gibt es einen Haftungsausschluss für den Verantwortlichen?

Ja, aber der Nachweis ist schwierig, da zu Lasten des Verantwortlichen eine Beweislastumkehr gilt.

Wie oben bereits ausgeführt hat der Verantwortliche nachzuweisen, dass "er in keinerlei Weise für den Umstand, den für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art 82 Abs. 3).

Frage: Gilt ein Haftungsausschluss bei Anwendung von genehmigten Verhaltensregeln und Zertifizierungsverfahren?

Die Anwendung solcher Regeln und Verfahren schließt eine Haftung nicht aus. Allerdings wird dem Verantwortlichen die Nachweispflicht erheblich erleichtert, dass er nicht für den eingetretenen Schaden verantwortlich ist (s. bereits oben Kapitel 3).

Frage: Kann der Verantwortliche seine Haftung an den Auftragsverarbeiter delegieren?

Nein

Verantwortlicher und Auftragsverarbeiter haften gemeinsam (Art. 82 Abs. 1). Vertragliche Absprachen mit dem Auftragsverarbeiter, die eine Haftung des Verantwortlichen ausschließen, sind nicht zulässig. Sind Verantwortlicher und Auftragsverarbeiter an derselben Datenverarbeitung beteiligt, so haften sie regelmäßig als Gesamtschuldner. Der Geschädigte kann sich an beide wenden (s. Gola, Art. 82, Rdnr. 6. Soweit der Schaden dem Auftragsverarbeiter zuzurechnen ist, hat der Verantwortliche, der vollen Schadensersatz geleistet hat, einen Rückgriffsanspruch gegen den Auftragsverarbeiter.

Anmerkung der IT-Recht Kanzlei: In der Praxis werden kleinere Online-Händler bei Regressstreitigkeiten mangels Sachkenntnis der Vorgaben der Datenschutz-Grundverordnung Schwierigkeiten haben, einen Rückgriffsanspruch gegen einen hoch spezialisierten Dienstleister als Auftragsverarbeiter durchzusetzen (s. Kommentar Ehmann/Selmayr, Art. 82, Rdnr. 24). Umso wichtiger ist die sorgfältige Auswahl des Auftragsverarbeiters und die Anwendung von Zertifizierungsverfahren, s. Kapitel 3).

Frage: Gilt das Haftungsprivileg für Provider auch weiterhin?

Ja

Erwägungsgrund 21 stellt klar, dass das Providerprivileg der Artikel 12-15 E-Commerce Richtlinie (§§ 7 ff Telemediengesetz) unverändert fort gilt. Hosting-Provider sind damit weiterhin von der Haftung für Inhalte Dritter auf ihrer Plattform freigestellt, wenn sie keine Kenntnisse von der Rechtswidrigkeit dieser Inhalte haben, die Rechtswidrigkeit nicht offensichtlich ist und sie solche Inhalte unverzüglich nach Kenntnis löschen oder sperren.

> *"(21) Die vorliegende Verordnung berührt nicht die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates (2) und insbesondere die der Vorschriften der Artikel 12 bis 15 jener Richtlinie zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste. Die genannte Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt."*

VI. Verwaltungsrechtliche und strafrechtliche Sanktionen gegen den Verantwortlichen

Die künftige Datenschutz-Grundverordnung führt gegenüber der bisherigen Rechtslage europaweit zu einer drastischen Verschärfung der Sanktionen bei Datenschutzverstößen, die den Verantwortlichen ungleich härter treffen können als Schadensersatzansprüche von betroffenen Personen (s. dazu Kapitel V). Auch die Interventionsmöglichkeiten der Aufsichtsbehörden wurden wesentlich verschärft.

Frage: Welche Interventionsmöglichkeiten haben die Aufsichtsbehörden?

Die Aufsichtsbehörde haben sehr weitgehende Interventionsmöglichkeiten, die Online-Händler empfindlich treffen können (Art.58). § 40 Anpassungsgesetz hat die Interventionsmöglichkeiten der Aufsichtsbehörde ergänzend konkretisiert.

Die Aufsichtsbehörde verfügt gem. Art. 58 Abs. 1 über folgende Untersuchungsbefugnisse, die es ihr gestatten,

- den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
- Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
- eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,
- den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
- von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten, Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen
und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

Die Aufsichtsbehörde verfügt gem. Art. 58 Abs. 2 über folgende Abhilfebefugnisse, die es ihr gestatten,

- einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
- einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen, den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
- den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten offengelegt wurden, über solche Maßnahmen anzuordnen,
- eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
- die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

Frage: Welche Bemessungskriterien bestehen bei Verhängung von Geldbußen?

Art. 83 nennt eine Vielzahl von Bemessungskriterien, in welcher Weise Geldbußen neben den dargestellten Interventionsmöglichkeiten der Aufsichtsbehörden verhängt werden sollen. Es soll laut Art. 83 Abs. 1 sichergestellt werden, dass die Verhängung von Geldbußen wirksam, verhältnismäßig und abschreckend ist. Die rechtswidrige Bearbeitung von Daten durch Online-Händler kann daher ernste Folgen haben.

Frage: In welcher Höhe können Geldbußen verhängt werden?

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 im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes verhängt werden.

Das sind in der Tat drakonische Sanktionen, die eine Abschreckungswirkung nicht verfehlen werden.

Frage: Können auch Geldstrafen und Freiheitsstrafen verhängt werden?

Ja, bei Vorsatz und in schweren Fällen

Gem. § 42 Abs. 1 Anpassungsgesetz wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, einem Dritten übermittelt und hierbei gewerbsmäßig handelt.

Gem. § 42 Abs. 2 Anpassungsgesetz wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, ohne hierzu berechtigt zu sein, verarbeitet oder durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Empfehlung der IT-Recht Kanzlei: Onlinehändler sollten angesichts der drakonischen Sanktionsmöglichkeiten die Vorgaben zur Datenverarbeitung nach der Datenschutz-Grundverordnung sehr ernst nehmen. Da die meisten Online-Händler angesichts der komplexen datenschutzrechtlichen Materie damit überfordert sind, die Datenverarbeitung im Einklang mit der Datenschutz-Grundverordnung zu organisieren, werden sie sich an externe Dienstleister wenden müssen. Dabei ist auf die Seriosität dieser Dienstleister zu achten. Es sollten keine Aufträge an Dienstleister vergeben werden, die nicht die Einhaltung genehmigter Verhaltensregeln und Zertifizierungsverfahren gewährleisten können. Es ist zu hoffen, dass die Aufsichtsbehörden, die ja gerade auch kleine und mittlere Unternehmen in Fragen des Datenschutzes unterstützen sollen, ihrer Betreuungsfunktion gerecht werden.

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