IWW INSTITUT
INFORMATIONSDIENSTE

DATENSCHUTZGRUNDVERORDNUNG

DSGVO-Vorgaben für Webshop-Betreiber: So gelingt die Umsetzung

von RA Christian Galetzka, LL.M., Würzburg

Auch für Webshop- und alle sonstigen Webseiten-Betreiber wird am 25.5.18 eine neue Zeitrechnung beginnen, wenn die Datenschutzgrundverordnung (DSGVO) in Kraft tritt und in allen EU-Mitgliedsstaaten unmittelbar gilt. Webshop-Betreiber kommen verstärkt mit personenbezogenen Kundendaten in Berührung und verarbeiten diese über ihre IT-Systeme oder lassen diese durch Dritte verarbeiten. Sie werden sich daher intensiv mit den neuen Anforderungen der DSGVO befassen müssen. Die Checkliste dieses Beitrags soll eine erste Hilfestellung für unternehmensinterne Umsetzungsmaßnahmen speziell im Bereich E-Commerce bieten, ist aber genauso im sonstigen IT-Umfeld verwendbar.

CHECKLISTE / Umsetzung DSGVO

1. Überarbeitung der Datenschutzerklärungen auf der Internetseite: Ist die Datenschutzerklärung auf dem aktuellen Stand der DSGVO-Vorgaben?

Art. 13 und 14 DSGVO halten im Vergleich zu § 13 Abs. 1 TMG erweiterte und sehr viel präzisere Informationsanforderungen bereit, die zu einer Anpassung von Datenschutzerklärungen auf Internetseiten veranlassen sollten. U. a. sind Informationen erforderlich

- zum Verantwortlichen für die über die Webseite erfolgenden Datenverarbeitungsvorgänge (Name, Adresse, Kontaktdaten),
- zum Datenschutzbeauftragten (sofern eine Verpflichtung zur Bestellung besteht),
- über Art, Umfang und Zweck der Datenverarbeitung unter Angabe der Rechtsgrundlage,
- zur Löschung von Nutzungs- und Bestandsdaten sowie Cookies (Stichwort: Löschkonzept),
- zur Behandlung von Tracking-Daten,
- über das Beschwerderecht bei einer Aufsichtsbehörde für den Datenschutz,
- bez. der Betroffenenrechte, insbesondere zum neuen Recht auf Datenportabilität (vgl. Art. 20 DSGVO).

2. Verzeichnis von Verarbeitungstätigkeiten (Verfahrensverzeichnis): Ist das Verfahrensverzeichnis/Verzeichnis von Verarbeitungstätigkeiten auf dem aktuellen Stand?

Schon auf Grundlage des noch geltenden BDSG ist jedes Unternehmen, das mit personenbezogenen Daten in Berührung kommt und diese verarbeitet, verpflichtet, ein Verfahrensverzeichnis – bzw. im Wording der DSGVO neu – ein Verzeichnis von Verarbeitungstätigkeiten zu führen und dieses im Bedarfsfall auch der Aufsichtsbehörde für den Datenschutz vorzulegen.

In dem Verfahrensverzeichnis sollten sämtliche Datenverarbeitungsvorgänge nach Art, Umfang und Zweck erfasst sowie aufbereitet werden. Besonders risikogefährdete Datenverarbeitungen wie z. B. Videoüberwachungen, Profiling oder die Verarbeitung von besonderen personenbezogenen Daten (Gesundheitsdaten, Zahlungsdaten, Positionsdaten) sollten speziell geprüft und nach Möglichkeit sollte bereits in das Verfahrensverzeichnis ein Verweis auf eine gesondert durchgeführte Datenschutz-Folgenabschätzung (Art. 35 DSGVO) aufgenommen werden. Auch Verarbeitungen von personenbezogenen Daten durch Dritte oder im Auftrag für Dritte (= Auftragsverarbeitungen) sollten in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden.

3. Vertragsmanagement, insbesondere Auftragsverarbeitungen: Sind die Datenschutzvereinbarungen über die Verarbeitung von personenbezogenen Daten im Auftrag (Auftragsverarbeitungen) auf dem aktuellen Stand?

Webshop-Betreiber sollten ihre Prozesse dahingehend überprüfen, ob sie selbst personenbezogene Daten im Auftrag für Dritte verarbeiten, Dritte personenbezogene Daten in ihrem Auftrag verarbeiten lassen oder technische Dienstleister mit von ihnen verarbeiteten personenbezogenen Daten in Berührung kommen können. In sämtlichen Fällen sollte schon nach geltender Rechtslage bereits ein Vertrag zur Auftragsdatenverarbeitung nach den Vorgaben des § 11 BDSG abgeschlossen worden sein.

Solche bestehenden Vereinbarungen zur Auftragsverarbeitung sollten an die Vorgaben der DSGVO (vgl. Art. 28 DSGVO) entweder angepasst oder neu abgeschlossen werden. In diesem Bereich besteht ein elementarer Umsetzungsbedarf, insbesondere im Hinblick auf die neue Haftungsverteilung zwischen Auftraggeber der Auftragsverarbeitung und dem Auftragsverarbeiter selbst. Beide haften – und das ist neu – gesamtschuldnerisch für Datenschutzverstöße. Gerade im Hinblick auf die Erhöhung des Bußgeldrahmens (vgl. Art. 83 DSGVO) und die Strafbarkeit bei bestimmten Datenschutzverstößen (vgl. § 42 BDSG neu) sollte diesem Umsetzungspunkt besonderes Augenmerk gewidmet werden.

4. Datenschutzbeauftragter: Wurde ein Datenschutzbeauftragter bestellt?

Nach neuer Rechtslage sind Unternehmen verpflichtet, einen Datenschutzbeauftragten zu bestellen, soweit sich i. d. R. mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (Personenzahlkriterium). Unabhängig von der Personenanzahl besteht eine Bestellpflicht, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden oder die Datenverarbeitung besondere Risiken für die Betroffenen zur Folge haben kann (z. B. risikogefährdete Datenverarbeitungsvorgänge, die einer Datenschutz-Folgenabschätzung unterliegen).

Praxishinweis | Unter Umständen ist es sinnvoll, auch unabhängig von den gesetzlichen Voraussetzungen der DSGVO und des BDSG neu einen Datenschutzbeauftragten zu bestellen, der sich um sämtliche betrieblichen Datenschutzanforderungen sowie um Anfragen von Betroffenen kümmert. Der Datenschutzbeauftragte kann eine interne oder externe Person sein. In der anwaltlichen Beratungspraxis lässt sich feststellen, dass die Ausübung von Betroffenenrechten wie Auskunft, Berichtigung, Sperrung und Löschung von personenbezogenen Kundendaten gerade bei Webshop-Betreibern immer mehr an der Tagesordnung ist. Hier empfiehlt sich geradezu die Schaffung einer Datenschutzposition, die idealerweise mit der fachlichen Kompetenz eines Datenschutzbeauftragten versehen sein sollte.

5. Datensicherheit – Umsetzung/Anpassung technischer und organisatorischer Maßnahmen: Wurden die getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit überprüft und an die neuen Anforderungen der DSGVO angepasst?

Bis zum Inkrafttreten der DSGVO ist eine Bestandsaufnahme und ggf. Neustrukturierung bereits getroffener technischer sowie organisatorischer Maßnahmen zur Datensicherheit (Art. 32 DSGVO) empfehlenswert. Zu diesen Maßnahmen gehören u. a.:

- 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
- Die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Beachten Sie | Prinzipiell geht es hier lediglich um alten Wein in neuen Schläuchen, da auch die noch aktuelle Rechtslage in § 9 BDSG i. V. m. der Anlage zu § 9 BDSG für den Verantwortlichen einen ausführlichen Kanon von technischen und organisatorischen Maßnahmen vorsieht. Im Zuge des immer mehr ausgeprägten Datenschutzbewusstseins bei Betroffenen oder auch bei Mitbewerbern sollte auf diesen Punkt ebenfalls besonderes Augenmerk bei der Umsetzung gelegt werden.

6. Anpassung interner Datenschutzorganisation und Verfahrensabläufe an die DSGVO-Standards: Ist die Überprüfung/Anpassung erfolgt?

Auch die internen Verfahrensabläufe sollten im Hinblick auf den Datenschutz anhand der Vorgaben der DSGVO überprüft und an die neue Gesetzeslage angepasst werden, z. B.

- Erstellung von **Datenschutz-Folgenabschätzungen** bei risikobehafteten Datenverarbeitungsvorgängen
- Prüfung der **Datenschutz-Organisationsstruktur**: Anpassung unternehmensinterner Regularien, Richtlinien, Policys, Handbücher
- Prozess für den Umgang mit **Datensicherheitsvorfällen** („Datenpannen")
- Umsetzung der (antragsunabhängigen) Verpflichtung zur Löschung von personenbezogenen Daten (z. B. in Form eines **Löschkonzepts**)
- Gewährleistung der **Betroffenenrechte** (Auskunft, Berichtigung, Sperrung, Löschung, Datenportabilität)
- **Einwilligungsmanagement**
- Ggf. Anpassung stattfindender **Datenverarbeitungen** an geänderte Zulässigkeitsvorgaben der DSGVO