

DATENSCHUTZ: NEUES RECHT FÜR EUROPA – DER FALL FACEBOOK ALS WARNUNG

Mehr Transparenz für Verbraucher

VON MELANIE REINSCH

Die Zeit drängt. Denn in wenigen Monaten gilt laut Beschluss des EU-Parlaments die neue, einheitliche europäische Datenschutzgrundverordnung (EU-DSGVO). Alte Datenschutzerklärungen („Privacy Policy“), in denen Organisationen die Kunden über den Umgang mit Privatsphäre aufklären, müssen daher schon bald an die neuen Regelungen angepasst werden. Im Kern geht es darum, die Rechte der Nutzer zu stärken und Transparenz zu schaffen. Im Gegenzug bedeutet dies, dass auf die Unternehmen höhere Anforderungen zukommen werden. Eine Umfrage von Bitkom im November ergab, dass sich 48 Prozent der Unternehmen für die Umsetzung externe Experten zur Hilfe geholt haben. Jedes vierte Unternehmen hat dazu zusätzliches Personal eingestellt.

Von der umfassenden Datenschutz-Reform sind Unternehmen betroffen, die in der EU ansässig sind und die mit personenbezogenen Daten arbeiten – online wie offline. Das können Mitarbeiter-, Nutzer- oder Kundendaten sein, zum Beispiel Name, E-Mail-Adresse, Kfz-Zeichen, Geburtstag oder aber Cookies. Auch die analoge Papierakte in der Schublade gehört dazu. Zudem sind Firmen, die im Ausland sitzen und deren Angebote sich aber an EU-Bürger wenden, von der Verordnung betroffen – zum Beispiel Facebook, Google und Co. Es dürfte daher kaum Unternehmen geben, die von der Reform ausgeschlossen sind. Auch IP-Adressen – also die Adresse eines Computers oder Servers – zählen zu personenbezogenen Daten. Damit ist auch jeder Seitenanbieter von der DSGVO betroffen.

Am 25. Mai 2018 ist Stichtag. Ab hier endet die zweijährige Übergangsfrist. Dann sind Verstöße durch die EU-Datenschutz-aufsichtsbehörden und Gerichte überprüfbar. Wer sich nicht kümmert, dem können danach empfindliche Geldstrafen drohen: bis zu 20 Millionen Euro. Oder: Bußgelder bis zu vier Prozent des weltweiten Unternehmensumsatzes. Das könnte für einige Unternehmen für Überraschungen sorgen.

Trotzdem ist keine Panik angesagt – wer sich auch schon vorher mit entsprechendem Datenschutz beschäftigt hat, fängt nicht von vorne an. Viele Datenschutzrichtlinien sind bisher in Deutschland im Bundesdatenschutzgesetz (BDSG) und Telemediengesetz (TMG) geregelt gewesen. Sich mit der Reform beschäftigen und den Datenschutz überprüfen, ist jedoch unumgänglich, denn die neuen Regelungen gehen weit über die alten hinaus.

Informationspflichten: Schon vorher war es so, dass Unternehmen über Datenverarbeitungsvorgänge informieren mussten. Neu ist nun, dass dort nicht nur der Zweck, sondern auch die Rechtsgrundlage für die Verarbeitung der Daten angegeben werden muss. Es gilt der Grundsatz „Verbot mit Erlaubnisvorbehalt“, das bedeutet: Die Verarbeitung personenbezogener Daten ist eigentlich verboten und nur in Ausnahmefällen erlaubt – wenn es das Gesetz gestat-

tet, jemand die Einwilligung dazu gegeben hat oder es rechtliche Verpflichtungen gibt. Letzteres ist zum Beispiel der Fall, wenn jemand in einem Onlineshop ein Produkt kauft und der Seitenbetreiber für den Warenversand die Adresse des Käufers speichern muss. Zudem gibt es die sogenannten berechtigten Interessen. Dazu kann laut DSGVO auch Direktwerbung zählen. Unternehmen sollten also bei der Erhebung personenbezogener Daten stets die entsprechende Rechtsgrundlage im Hinterkopf haben. Zudem muss der Verantwortliche die Dauer der Speicherung der Daten offenlegen. Kann er das nicht, muss der Betreiber zumindest über die Kriterien für die Speicherfrist informieren. Ein Nutzer muss auch darüber aufgeklärt werden, wenn ein Unternehmen die Daten von Dritten bekommen hat. Das ist zum Beispiel bei einem Abschluss von Finanzierungsverträgen im Bankwesen der Fall, wenn die Kreditwürdigkeit überprüft wird, oder zum Beispiel bei der Schufa.

Privacy by design und privacy by default: Neu ist auch die Pflicht, elektronische Geräte und Software von vornherein datenschutzfreundlich zu entwickeln und die Grundeinstellungen dementsprechend einzustellen. Das gilt auch für Onlinedienste. Der Nutzer soll selbst bestimmen können, ob er die Einstellungen ändern möchte.

Recht auf Löschen: Die Verordnung gibt den Verbrauchern ein „Recht auf Vergessen“. Das heißt, jeder kann vom Seitenbetreiber verlangen, dass seine persönlichen Daten gelöscht werden sollen: Wenn die Daten zum Beispiel nicht mehr benötigt werden, wenn sie unrechtmäßig verarbeitet wurden oder man seine Einwilligung für die Verarbeitung zurückzieht. Hinzukommt auch ein Recht auf Berichtigung. Betroffene können

verlangen, dass falsche Daten korrigiert werden müssen.

Datenschutz-Folgenabschätzung: Ebenfalls neu eingeführt wird die Pflicht zur Datenschutz-Folgenabschätzung, wenn ein hohes Risiko für die Rechte und Pflichten der Nutzer besteht. Das kann zum Beispiel passieren, wenn neue Technologien eingesetzt werden, bei denen automatisiert Daten verarbeitet werden. Der Verantwortliche muss in Absprache mit dem Datenschutzbeauftragten prüfen, ob die Sicherheitsvorkehrungen ausreichend sind und die Verordnung eingehalten wird.

Recht auf Datenübertragbarkeit: Neu ist zum Beispiel auch, dass Nutzer ihre Daten

zu einem anderen Anbieter mitnehmen dürfen – zum Beispiel, wenn sie den Anbieter wechseln: die Bank, das soziale Netzwerk, den Arbeitgeber. Es soll also möglich sein, ein Unternehmen anzuweisen, die Daten auf einem maschinenlesbaren Format ohne Verlust zu übermitteln. Das betrifft aber nur Daten, die der Nutzer auch selbst zur Verfügung gestellt hat.

Datenschutzbeauftragter: Ein Datenschutzbeauftragter muss ernannt werden, wenn ein Unternehmen aus datenschutzrechtlicher Sicht einer Tätigkeit nachgeht, die einer Kontrolle bedarf. Dazu gehören Behörden oder öffentliche Stellen. Jedes Unternehmen kann aber auch freiwillig einen Datenschutzbeauftragten benennen. Ab Mai müssen Sei-

tenbetreiber zwingend die Kontaktdaten des Datenschutzbeauftragten bereitstellen.

Datenpannen: Passiert einem Unternehmen eine Datenpanne, von der persönliche Daten betroffen sind, muss das der Aufsichtsbehörde gemeldet werden – innerhalb von 72 Stunden. Dazu muss in etwa angegeben werden, wie viele Datensätze betroffen sind, welche Folgen die Panne haben könnte und wie Abhilfe geschaffen werden kann.

Sprache: Eine Herausforderung wird es sein, dass die Kunden nicht nur vollumfänglich aufgeklärt werden müssen, sondern das auch noch leicht verständlich, in einer klaren Sprache, übersichtlich und leicht zugänglich passieren muss.



FOTO: 123RF