Update

Juni 2017

E-Commerce – Datenschutz

VON BOETTICHER
RECHTSANWÄLTE

ZUSAMMENFASSUNG

1. **Datenschutz-Grundverordnung: Das Accountability-Prinzip**
   - Ab dem 25. Mai 2018 löst die Datenschutz-Grundverordnung das nationale Recht ab. Das neue Accountability-Prinzip (Rechenschaftsplicht) bringt strenge Nachweispflichten für alle Unternehmen.
2. **Aufsichtsbehörden prüfen DSGVO-Umsetzung und Datenexporte**
   - LDA Bayern stellt Fragebogen bereit.
3. **Ein einzelner Spam-Empfänger kann gesamte Adress-Datenbank entwerten**
   - BGH bestätigt: Unterlassungsanspruch nicht auf einzelne E-Mail-Adresse beschränkt. Hohe Anforderungen an Einwilligung.
4. **Neuer Mindeststandard des BSI zur Nutzung externer Cloud-Dienste**
   - Vertragliche Regelungen von großer Bedeutung.

1. Datenschutz-Grundverordnung: Das Accountability-Prinzip

Ab dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) anwendbar. Ein Ziel: das derzeit bestehende Umsetzungsdefizit des Datenschutzrechts abzubauen. Eine der Neuerungen ist die Pflicht, die datenschutzrechtlichen Vorgaben nicht nur einzuhalten, sondern deren Einhaltung auch nachweisen zu können.

Erleichterte Überwachung

Hintergedanke der neuen Rechenschaftspflicht („Principle of Accountability“) ist wohl das Bestreben, den Aufsichtsbehörden ein effektives Mittel an die Hand zu geben, die Einhaltung datenschutzrechtlicher Vorgaben ohne großen Aufwand überprüfen zu können. Kann ein Unternehmen die im Rahmen seiner Rechenschaftspflicht erforderliche Dokumentation nicht oder nur lückenhaft vorweisen, steht der Verstoß gegen die DSGVO fest, selbst wenn den datenschutzrechtlichen Anforderungen im Übrigen entsprochen wurde. Umgekehrt entbindet natürlich selbst eine lückenlose Dokumentation nicht von der Einhaltung der (sonstigen) datenschutzrechtlichen Pflichten. Allerdings dürfte es in der Praxis kaum vorkommen, dass die Aufsichtsbehörde nach Vorlage einer einwandfreien Dokumentation nicht zufriedengestellt ist – es sei denn, es ergeben sich anderweitige Hinweise auf datenschutzrechtliche Versäumnisse.

Beweislastumkehr

Eine ähnliche Funktion wird der Rechenschaftspflicht wohl auch an anderer Stelle zukommen. Die DSGVO sieht eine Beweislastumkehr zugunsten der betroffenen Personen vor. Liegt ein Verstoß gegen Datenschutzrecht vor, muss das Unternehmen künftig nachweisen, dass es für einen entstandenen Schaden in keinerlei Hinsicht verantwortlich ist. Gelingt dies nicht, wird automatisch unterstellt, dass es für den Verstoß verantwortlich ist. Als Konsequenz hat das Unternehmen dem Betroffenen den materiellen – und neu auch den immateriellen – Schaden zu ersetzen. Dabei ist zu berücksichtigen, dass der immaterielle Schadensersatz („Schmerzensgeld“) eine „wirklich abschreckende Wirkung“ haben und Verstöße unattraktiv machen soll. Immaterieller Schadensersatz, etwa wenn die Patientenakte eines Unfallopfers abhandenkommt, könnte damit deutlich höher ausfallen als das Schmerzensgeld für die Körperverletzung durch den Unfall an sich.

Die Rechenschaftspflicht – so ihr denn entsprochen wurde – kann für das Unternehmen bei Schadensersatzklagen eine entscheidende Hilfestellung sein. Denn nur die Dokumentation ermöglicht es, nachzuweisen, dass und wie das Unternehmen seinen datenschutzrechtlichen Pflichten nachgekommen ist.

Diesen Nachweis muss das Unternehmen auch im Bußgeldverfahren führen. Die DSGVO sieht bekanntermaßen Geldbußen bis zu 20.000.000 Euro oder vier Prozent des weltweiten Konzernvorjahresumsatzes vor.

Umsetzung

Die Rechenschaftspflicht kann dem Unternehmen somit durchaus zugute kommen. Dies ändert aber nichts daran, dass sie eine erhebliche zusätzliche Belastung darstellt – denn künftig muss genau dokumentiert werden, wer auf welche Weise mit personenbezogenen Daten umgehen kann, welche Sicherheitsmaßnahmen ergriffen wurden und wann die Daten gelöscht werden.

Wurde bereits den bestehenden datenschutzrechtlichen Anforderungen Genüge geleistet, lässt sich darauf sicherlich gut aufbauen. Selbst dann gilt jedoch: Ein Jahr ist nicht viel Zeit. Ist der Datenschutz bisher eher stiefmütterlich behandelt worden, sollte das Thema schnellstmöglich angegangen werden, weil auch die Vorarbeiten viel Zeit kosten. Gerade wenn bisher das Datenschutzrecht wenig Beachtung gefunden hat, ist es wahrscheinlich, dass Geschäftsprozesse angepasst werden müssen – etwas, das auch wegen der hohen Geldbußen ernst zu nehmen ist.

Selbst Unternehmen, die ihre Datenverarbeitung ausgelagert haben, können sich nicht in Sicherheit wiegen, denn sie bleiben zur Rechenschaft verpflichtet. Erleichterungen für kleinere Unternehmen – wie etwa beim Verfahrensverzeichnis – sind bei der Rechenschaftspflicht nicht vorgesehen. Kleine Unternehmen werden sich folglich ebenfalls wappnen müssen, wobei natürlich der Umfang ihrer Pflichten abhängig von den datenschutzrechtlichen Risiken ihres Geschäftsbetriebs ist.

Allein die Bestellung eines Datenschutzbeauftragten und die Zuweisung von Aufgaben an diesen sind ganz klar nicht ausreichend – der Datenschutzbeauftragte ist vielmehr dafür da, die Geschäftsführung zu kontrollieren. Unternehmen benötigen deshalb eine Datenschutz-Organisation. Es muss beispielsweise jederzeit möglich sein, eine systematische Zusammenstellung der für den Datenschutz erforderlichen technischen und organisatorischen Maßnahmen vorzuweisen.

... jetzt beginnen!

Auch wenn der 25. Mai 2018 noch weit entfernt scheint – die Pflichten sind umfangreich, so dass jedes Unternehmen spätestens jetzt mit der Vorbereitung beginnen sollte. Wer erst 2018 mit der Umsetzung beginnt, sollte sich des Risikos bewusst sein, dass alle kompetenten Berater dann schon ausgebucht sind.

Weiterführende Informationen:

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

https://www.boetticher.com/17060a

Update E-Commerce – Datenschutz Januar 2017

https://www.boetticher.com/17010

2. Aufsichtsbehörden prüfen DSGVO-Umsetzung und Datenexporte

Zur Halbzeit der Umsetzungsfrist für die Neuregelungen der DSGVO hat das Bayerische Landesamt für Datenschutzaufsicht ca. 150 bayerischen Unternehmen einen Prüffragebogen auf Basis des künftigen Rechts zugeschickt, damit diese Unternehmen feststellen können, wie weit sie mit der Vorbereitung auf das neue Recht schon gekommen sind.

Der Fragebogen zeigt den Paradigmenwechsel, den das Accountability-Prinzip mit sich bringt: Nicht mehr die Behörde muss aufwendig einen Verstoß suchen, sondern das Unternehmen muss seine Compliance nachweisen.

Zuvor hatten das LDA Bayern und andere Datenschutz-Aufsichtsbehörden in einer konzertierten Aktion bereits Übermittlungen personenbezogener Daten in das Nicht-EU-Ausland genauer geprüft. Gefragt wurde zum Beispiel nach der Inanspruchnahme externer Leistungen und Produkte in Bereichen wie Fernwartung, Support, Ticket-Bearbeitung, aber auch Customer Relationship Management oder Bewerbermanagement. Zeigte sich die Nutzung von Nicht-EU-Anbietern, wollten die Aufsichtsbehörden auch die Rechtsgrundlagen erläutert haben.

Weiterführende Informationen:

LDA Bayern, Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018

https://www.boetticher.com/17060b

3. Ein einzelner Spam-Empfänger kann gesamte Adress-Datenbank entwerten

Wie wichtig es ist, für jede einzelne E-Mail-Adresse, an die ein Unternehmen Werbung schickt, die Erlaubnis zu dokumentieren, zeigt ein aktuelles Urteil des BGH. Denn der Unterlassungsanspruch des Empfängers ist nicht auf einzelne E-Mail-Adressen beschränkt. Wer sich also nicht sicher sein kann, ob auch noch eine andere E-Mail-Adresse des Spam-Empfängers in der Datenbank steht, darf die gesamte Datenbank nicht mehr zum E-Mail-Versand nutzen.

Teilweise hatten Gerichte die Ansicht vertreten, der Unterlassungsanspruch sei auf die konkrete E-Mail-Adresse beschränkt. Der BGH entschied anders – in Übereinstimmung mit der ständigen Rechtsprechung, dass nicht nur exakt derselbe Verstoß gerichtlich verboten wird, sondern auch kerngleiche Verstöße.

Im Übrigen verweist der BGH auf seine bekannte Rechtsprechung, dass Werbe-Einwilligungen präzise sein müssen und Generaleinwilligungen unwirksam sind. Dass die (nachträgliche oder künftige) Einholung wirksamer Einwilligungen einen großen Aufwand bedeutet, ist nach der – auch insoweit nicht neuen – Rechtsprechung des BGH ohne Bedeutung.

Eine Besonderheit weist der Fall nur insoweit auf, als dass der Kläger sich verbeten hatte, dass seine für den Spam-Versand genutzte E-Mail-Adresse an den für den E-Mail-Versand genutzten Dienstleister weitergegeben wird. Der BGH entschied, dass in diesem Verbot möglicherweise ein Rechtsmissbrauch liegen könne, wenn das Unternehmen keine andere Möglichkeit habe, weiteren Werbeversand an den Kläger zu verhindern.

Diese Ausführungen mögen prozessualen Besonderheiten geschuldet sein, denn eigentlich ist es ganz einfach, den Unterlassungspflichten nachzukommen: keine Werbe-E-Mails mehr an die Adressen schicken, bei denen die Einwilligung unwirksam ist. Dass möglicherweise genau dieses faktische generelle Verbot Ziel des Weitergabeverbots des Klägers war, wird man wohl kaum als Rechtsmissbrauch ansehen können, wenn das werbende Unternehmen offensichtlich nicht die datenschutzrechtlich regelmäßig erforderliche Gestaltung als Auftragsdatenverarbeitung gewählt hat, sondern eine Lösung, bei der der technische Dienstleister die Daten in eigener Verantwortung verarbeitet.

Wer E-Mail und andere elektronische Direktkommunikation zur Werbung nutzt, muss deshalb auf die Formulierung der Einwilligungserklärung ganz besondere Sorgfalt verwenden. Gleiches gilt für die Dokumentation der Einwilligung.

Weiterführende Informationen:

BGH, Urteil vom 14.3.2017, Az. VI ZR 721/15

https://www.boetticher.com/17060c

4. Neuer Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Mindeststandard zur Nutzung externer Cloud-Dienste veröffentlicht. Das Dokument hält fest, was in der Beschaffungs-, der Einsatz- und der Beendigungsphase unbedingt zu beachten ist. Der Mindeststandard bezieht sich zwar explizit auf Cloud-Services, kann aber auch für viele weitere Auslagerungen von Datenverarbeitungen genutzt werden.

Einen Schwerpunkt des Mindeststandards stellen naturgemäß die erforderlichen vertraglichen Regelungen dar. Insgesamt enthält das Papier allerdings nichts Neues, sondern beschreibt letztlich im Wesentlichen nur, welche Ansprüche an eine gesetzeskonforme Auftragsdatenverarbeitung zu stellen sind. Nur wenige Anforderungen gehen darüber hinaus. Einzelne datenschutzrechtliche Pflichten bei Auftragsdatenverarbeitungen sind allerdings nicht aufgeführt.

Weiterführende Informationen:

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 24.4.2017

https://www.boetticher.com/17060d

Ansprechpartner:

Wenn Sie Fragen haben oder weitere Informationen zu einem der Themen wünschen, wenden Sie sich bitte an:

Matthias Bergt
E-Mail: mbergt@boetticher.com
Tel. +49 / 30 / 61 68 94 03

Dr. Anselm Brandi-Dohrn, maître en droit
E-Mail: abrandi-dohrn@boetticher.com
Tel. +49 / 30 / 61 68 94 03

oder Ihren üblichen Ansprechpartner bei VON BOETTICHER.

VON BOETTICHER Rechtsanwälte
Oranienstraße 164
10969 Berlin

VON BOETTICHER Rechtsanwälte
Widenmayerstraße 6
80538 München