

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Dr. Alexander Golland, Adrian Schneider, Philipp Quiel, Tilman Herbrich

Datenschutz im Fokus

Zwischen Datenschutz- und Bankenaufsichtsrecht

Verantwortliche zwischen Datenschutz- und Bankenaufsichtsrecht – wie können Vorgaben beider Rechtsgebiete gleichzeitig beachtet werden?

Seite 150

Ein Jahr DSGVO in der Unternehmenspraxis: War die Angst berechtigt?

Ein Überblick zu dem, was bisher geschah

Seite 153

Die Melde- und Benachrichtigungspflichten nach Art. 33, Art. 34 DSGVO in der betrieblichen Praxis (Teil 1)

Ein Überblick zu den Melde- und Benachrichtigungspflichten nach Art. 33, Art. 34 DSGVO

Seite 156

Behördenkommunikation- und verfahren: Eine Orientierungshilfe

Ablauf des Behördenverfahrens und Ratschläge zur Kommunikation

Seite 160

Fragen aus der Praxis

Mammutaufgabe: Erfüllung der Informationspflichten

Seite 163

Aktuelles aus den Aufsichtsbehörden

„Datenübermittlungen bei Online-Überweisungen“

Seite 165

Die Verarbeitung zum Zwecke der Vertragserfüllung – Leitlinien des Europäischen Datenschutzausschusses

Seite 167

Rechtsprechung

Anspruch gegen eine Versicherung auf Übermittlung einer Gutachtenkopie

Seite 169

Keine Sperrwirkung der DSGVO bei Verstößen gegen das Wettbewerbsrecht wegen Telefonwerbung

Seite 171

Stichwort

Ratloser Betriebsrat – Betriebsrat als eigener Verantwortlicher

Seite 173

▪ Nachrichten Seite 146 ▪ Service Seite 174

Tilman Herbrich/Rosa Buchartowski

Mammutaufgabe: Erfüllung der Informationspflichten

Frage

Die Erfüllung der datenschutzrechtlichen Informationspflichten ist alles andere als trivial. Dies zeigt eindrucksvoll der Prüfbericht des BayLDA im Rahmen des Safer Internet Day vom 05.02.2019, wonach 75% der insgesamt 40 geprüften Websites keine ausreichenden Informationen zu eingesetzten Tracking-Diensten bereitgestellt haben. Umsetzungsdefizite in der Praxis sind jedoch auch an anderer Stelle zu beobachten. Wie verhält es sich eigentlich mit der Zurverfügungstellung von Informationen über Verarbeitungen in der analogen Welt? Reicht es aus, wenn man lediglich eine Datenschutzerklärung auf der Website bereithält und sollte man sich nicht sicherheitshalber den Erhalt von Datenschutzinformationen bestätigen lassen?



Antwort

Das Pflichtenprogramm für die Erfüllung der wesentlichen Informationspflichten folgt aus Art. 12-14 DSGVO. Dabei richtet sich der Umfang der notwendigen Informationen nach der Art der Datenerhebung. Werden personenbezogenen Daten direkt beim Betroffenen erhoben, gilt Art. 13 DSGVO. Wie auch im Falle einer indirekten Erhebung nach Art. 14 DSGVO (z. B. Bereitstellen von Adressbüchern durch Nutzer in Apps oder Veröffentlichung von Bewertungen auf Online-Plattformen) wird zudem zwischen Pflichtangaben und zusätzlichen Informationen differenziert, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Was den Umfang der Informationspflichten anbelangt, kann man auf diverse Stellungnahmen, Kurzpapiere und Muster von Datenschutzbehörden zurückgreifen, idealerweise von der zuständigen Behörde am Sitz des Verantwortlichen.

Nach Art. 12 DSGVO sind Verantwortliche verpflichtet, geeignete Maßnahmen zu treffen, um den von der Datenverarbeitung Betroffenen Informationen zu übermitteln. Diese sollen in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen; die Sprache soll klar und einfach sein. Dabei herrscht grundsätzlich Formfreiheit, jedoch gilt für eine mündliche Informationsübermittlung der strengere Maßstab des Art 12 Abs. 1 S. 3 DSGVO „Falls von der betroffenen Person verlangt [...]“. Relevant wird dies bei Telefonbestellungen. Der vorgegebene Zeitpunkt der Informationspflicht ist die Datenerhebung, weshalb die Informationen dem Betroffenen praktisch vor Verarbeitung zur Verfügung gestellt werden müssen.

Insbesondere in der analogen Welt stehen Verantwortliche vor der Herausforderung, Kunden, Gäste und andere Betroffene rechtzeitig und hinreichend zu informieren. Ganz gleich, ob Kunden bei der EC-Kartenzahlung oder bei der Verwendung elektronischer Kundenkarten im Einzelhandel, der Besuch in Arztpraxen, die Buchung von Reisedienstleistungen, der Besuch im Hotel oder Restaurant oder die Videoüberwachung, überall dort, wo personenbe-

zogene Daten erhoben werden, gilt eine uneingeschränkte Informationspflicht nach Art. 13 DSGVO. Eine Erheblichkeitsschwelle existiert insoweit nicht. Als Vorbild geht etwa die Stadt München voran; sie stellt auf ihrer Website über 100 unterschiedliche Datenschutzinformationen für die unterschiedlichen Verarbeitungen in den verschiedenen Ämtern zur Verfügung.

Für reichlich Aufmerksamkeit haben im letzten Jahr die Modalitäten für die Bereitstellung von Datenschutzinformationen bei Bildaufnahmen von Menschenmengen auf Großveranstaltungen gesorgt. Die Erfüllung der Informationspflichten scheint ohne Einbeziehung der Veranstalter schlichtweg nicht möglich zu sein. Nicht zuletzt deshalb haben sich Aufsichtsbehörden vielfach geäußert und versucht, über die Anwendung von Art. 14 Abs. 5 DSGVO (Unmöglichkeit der Informationserteilung) Ausnahmen für Fotografen zu konstruieren. Werden indes Fotografen im Auftrag des Veranstalters tätig, müssen z. B. an Einlässen Informationen nach Art. 12 ff. DSGVO zur Verfügung gestellt werden. Gleiches gilt bei der Veröffentlichung von gewöhnlichen Bildaufnahmen jenseits des privaten und familiären Lebensbereiches.

Häufig beobachtet man, dass in Apps Datenschutzerklärungen von Websites wortgenau übernommen werden. Jedoch unterscheidet sich eine Datenschutzerklärung für eine Website von einer Datenschutzerklärung für eine App auf mobilen Endgeräten. Das liegt daran, dass die Datenverarbeitungsprozesse je nach App-Betriebssystemen zum Teil anders gelagert sind. Außerdem wird z. B. während des App-Trackings (z. B. Google Analytics) anstelle von Cookies auf „mobile identifier“ (IDFA/GAID) zurückgegriffen. Auch ergeben sich Unterschiede bei der Ausübung des Widerspruchsrechts mittels „automatisierter Verfahren“, wie es Art. 21 Abs. 5 DSGVO fordert.

Immer wieder wird die Frage nach der Zulässigkeit eines Medienbruchs aufgeworfen, sprich, ob man im analogen Bereich nicht Bezug auf die Online-Datenschutzerklärung eines Unternehmens nehmen kann. Wenngleich Aufsichts-

behörden sich dafür aussprechen, werden in der Fachliteratur Medienbrüche z. T. für unzulässig angesehen; das letzte Wort ist also insoweit noch nicht gesprochen.

Und zu guter Letzt, keinesfalls ist es empfehlenswert, sich den Erhalt von Datenschutzbestimmungen vom Betroffenen bestätigen zu lassen – so wie es häufig auf Websites und in Apps geschieht. Eine solche Handhabung macht die Datenschutzerklärung wie die AGB zum Vertragsbestandteil, wenn sie aus dem maßgeblichen Empfängerhorizont nicht als unverbindliche Hinweise, sondern als bindender Vertragsbestandteil verstanden wird. Insbesondere vom gemeinsamen „Abhaken“ der AGB und Datenschutzerklärung ist dringend abzuraten, da eine solche Handhabung die Datenschutzerklärung wie AGB zum Vertragsbestandteil macht, wenn sie aus dem maßgeblichen Empfängerhorizont nicht als unverbindliche Hinweise, sondern als bindender Vertragsbestandteil verstanden werden. Dann unterfällt nach Ansicht des Kammergerichts die Datenschutzerklärung einer AGB-Kontrolle nach § 307 ff. BGB (23 U 196/13).

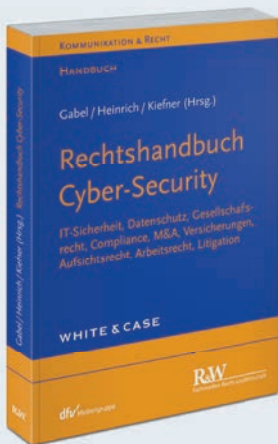
Autoren: Tilman Herbrich (Ass. jur. & CIPP/E) ist Teil der Schriftleitung und Privacy Expert bei Spirit Legal LLP in Leipzig. Als Privacy Expert berät er Unternehmen bei der Einführung und Durchsetzung neuer Werbetechnologien im Einklang mit und Datenschutz- und Wettbewerbsrecht.



Rosa Buchartowski ist Dipl.-Jur. und Wissenschaftlicher Mitarbeiter bei Spirit Legal LLP Rechtsanwälte.



Bestens gewappnet gegen Cyber-Attacken!



- Umfassende Darstellung zu Cyber-Security für das deutsche Recht: gängige Formen, Kosten, vorbeugende Maßnahmen, Verhalten im Ernstfall
- **Erstmals unter Einbezug aller relevanten Rechtsbereiche:** IT-Sicherheit, Datenschutz, Gesellschaftsrecht, Compliance, M&A, Versicherungen, Aufsichtsrecht, Arbeitsrecht, Litigation, Kartellrecht, Vergaberecht, Strafrecht
- Vergleichende Länderberichte zu USA, UK und China
- Praktische rechtsgebietsübergreifende Checklisten
- Geeignet für Wissenschaft und Praxis

Die Herausgeber

Dr. **Detlev Gabel** leitet bei White & Case LLP die europäische Praxisgruppe Data, Privacy & Cyber-Security.

Dr. **Tobias Heinrich** ist im Bereich Mergers & Acquisitions tätig. Er berät Unternehmen und strategische Investoren bei nationalen und grenzüberschreitenden M&A-Transaktionen, Joint Ventures und strategischen Kooperationen.

Dr. **Alexander Kiefner** berät Unternehmen in allen Fragen des Gesellschaftsrechts mit Schwerpunkten im Aktien- und Konzernrecht unter Einschluss der kapitalmarktrechtlichen Bezüge.

Die Herausgeber sind Rechtsanwälte und Partner im Frankfurter Büro von White & Case LLP.

Meine Bestellung

___ Expl. **Rechtshandbuch Cyber-Security**
2019, Kommunikation & Recht, Handbuch,
510 Seiten, Kt., ISBN: 978-3-8005-0012-3,
€ 98,-

Weitere Informationen:



Name | Firma | Kanzlei

E-Mail

Straße | Postfach

PLZ | Ort

Datum | Unterschrift