



**Dr. Carlo Piltz**  
Chefredakteur  
Datenschutz-Berater

## Corona – aber nicht nur

Sehr geehrte Leserinnen und Leser,

auch der zurückliegende Mai 2020 stand noch ganz im Zeichen der Corona-Pandemie. Peu à peu kehrt nun aber das öffentliche Leben zurück. Damit einher gehen natürlich auch wichtige Fragen des Datenschutzes. Die Bundesländer haben jeweils spezifische Regelungen für die Unternehmen erlassen, wie diese Kundendaten zu verarbeiten haben, wenn etwa Lokale, der Einzelhandel oder Fitnessstudios wieder öffnen. Hinweise und auch Mustertexte der Aufsichtsbehörden finden Sie auf den jeweiligen Internetseiten der Behörden.

Ganz generell gilt auch in dieser Situation, dass der Datenschutz zu beachten ist, andererseits aber auch keine unüberwindbaren Hürden aufstellt, wenn es etwa um eine angemessene Information von Besuchern oder die ordentliche Vernichtung von Besucherlisten geht. Zudem ist darauf zu achten, dass Zugriff auf solche Gäste- oder Kundenlisten nur berechtigte Mitarbeiter haben. Die Aufsichtsbehörden sehen es als unzulässig an, wenn eine Person die Daten anderer Gäste oder Kunden zur Kenntnis nehmen kann. Eine Möglichkeit ist, dass der Verantwortliche die Daten selbst erfragt und in entsprechende Listen einträgt. Als Rechtsgrundlagen der Erhebung und Speicherung der Besucher- oder Kundendaten kommt ganz überwiegend eine rechtliche Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) aus der jeweiligen Verordnung des Bundeslandes oder auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO in Betracht. Natürlich ist auch in dieser Situation auf den Grundsatz der Zweckbindung zu achten. Das bedeutet: für die Erfüllung entsprechender Pflichten aus einer Landesverordnung erhobene Daten dürfen nicht für andere Zwecke, wie etwa Werbung, genutzt werden. Es sei denn, der Kunde oder Besucher erteilt hierfür seine Einwilligung.

Ein anderes, dennoch nicht minder relevantes Thema, ist die IT-Sicherheit, die uns auch im Datenschutzrecht stän-

dig begleitet. Mit Stand vom 7. Mai 2020 hat das Bundesinnenministerium den neuen Referentenentwurf für das IT-Sicherheitsgesetz 2.0 veröffentlicht. Die (geplanten) Neueregungen enthalten einige thematische Überschneidungen zum Datenschutzrecht. Interessant ist etwa die geplante Anpassung des § 13 TMG durch neue Absätze 7a, 9 und 10. Nach dem vorgeschlagenen § 13 Abs. 9 TMG sollen etwa Diensteanbieter iSd TMG (z. B. App- oder Webseitenbetreiber) verpflichtet werden, den Zugang zu Daten zu sperren, wenn tatsächliche Anhaltspunkte für eine unrechtmäßige Erlangung oder Verbreitung personenbezogener Daten vorliegen. Zudem wird in § 13 Abs. 7a TMG vorgeschlagen, dass das Bundesamt für Sicherheit in der Informationstechnik gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter nach § 13 Abs. 7 S. 1 TMG anordnen kann. Oder anders formuliert: das BSI kann dann die Umsetzung von technischen und organisatorischen Schutzmaßnahmen fordern und anordnen. Hier tritt mithin aus Sicht des Diensteanbieters (der oft auch der Verantwortliche iSd DSGVO sein wird) eine weitere Aufsichtsbehörde auf den Plan.

In unserem aktuellen Heft finden Sie erneut eine interessante Mischung an Beiträgen. So etwa einen Aufsatz zum Datenschutz im vernetzten KfZ, ein Stichwort zu dem neuesten Urteil des BGH in der Sache „Planet49“ und auch eine Einschätzung dazu, ob rückwirkend heilende Einwilligung nach der DSGVO erteilt werden können.

Bei der Lektüre wünschen wir als Redaktion Ihnen erneut viel Freude und manche gedankliche Anregung.

Ihr

**Dr. Carlo Piltz**