PÜHN

Rechtsanwälte

Mandantenrundschreiben
03/2021

Datenschutzrecht
Datenschutz in der Praxis

Datenspeicherung in einer „Cloud“, also einer „Wolke“, vermittelt den Eindruck, dass eine dauerhafte Speicherung gegeben ist und Daten „immer und irgendwie“ zu jedem beliebigen Zeitpunkt abgerufen werden können. Ebenso wird der Eindruck vermittelt, dass nicht mehr befürchtet werden muss, dass mit dem „crash“ oder dem Diebstahl des mobilen Endgeräts dort gespeicherte Daten endgültig verloren sind.

Praktisch werden die Daten natürlich nicht in einer imaginären Wolke aufbewahrt, sondern in real existierenden Rechenzentren, auch „server farms“ genannt. Durch Sicherheitsdienste und Elektrozäune geschützt, mit Klimaanlagen und Notstromaggregaten versehen, wird von den Diensteanbietern vermittelt, dass diese Rechenzentren ein höheres Maß an Sicherheit bieten, als dies jeder übliche Nutzer durch eigene Leistungen selbst verwirklichen könnte.

Allerdings sind auch solche Rechenzentren nicht gegen innere und äußere Einwirkungen absolut geschützt – dies ist auch schlichtweg nicht möglich. Zu einem verheerenden Brand kam es Mitte März bei einem der größten Cloud-Anbieter Europas OVHCloud aus Frankreich. In einem Rechenzentrum in Straßburg brannte ein Server-Gebäude mit ca. 12.000 Servern vollkommen nieder, ein weiterer Bau wurde großteils zerstört. OVHCloud sah sich gezwungen, das gesamte Rechenzentrum herunterzufahren. Mehrere Millionen Websites gingen zunächst offline, darunter staatliche Portale, Banken, Newskanäle und die Regierungsseite data.gouv.fr.

Nun könnte dies als spektakulärer Unfall angesehen werden, der keine größeren, insbesondere dauerhafte Probleme nach sich zieht, wenn die Daten tatsächlich - wie es die Cloud-Rhetorik sowie die Vorstellungen von der „Cloud“ nahelegen –, anderswo gespeichert und über andere Rechenzentren weiterhin abrufbar wären.

Im Fall von OVHCloud ist es allerdings nach Presseberichten wohl so gewesen, dass einige Kunden – weil die Datenspiegelung in einem anderen Rechenzentrum u.U. kostenpflichtig ist – auf eine solche Spiegelung verzichtet hatten bzw. die gespiegelten Daten nicht in einem örtlich anderen Rechenzentrum gespiegelt wurden, sondern in dem gleichen Rechenzentrum in Straßburg, wenn auch in anderen Gebäuden. Einige Kunden, die einen irreversiblen Totalverlust anzeigten, waren nach Presseberichten die französische Großkanzlei Leroi&Associés und der englische Computerspiel-Anbieter Facepunch mit seinem Survival-Spiel „Rust“.

Ob die Brandursachen jemals geklärt werden können, ist offen. Die Datenverluste stehen hingegen fest. Sowohl die Kanzlei als auch der Spieleanbieter haben zwangsläufig auch personenbezogene Daten ihrer Kunden im Sinn der DSGVO – also z.B. Namen, Anschriften und Geburtsdaten – gespeichert. Nach Art. 5 Abs. 1 f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet, einschließlich dem Schutz vor unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung. Die Intention für den Erlass der DSGVO lag primär darin, dass die Erhebung personenbezogener Daten sowie deren Verarbeitung/Weitergabe reglementiert werden sollten. Der Schutz vor Verlust/Zerstörung der Daten war nur ein untergeordneter Aspekt, da dieser Schutz

für den Nutzer der Daten essenziell ist. Im Erwägungsgrund 39 zur DSGVO findet sich deshalb hierzu auch keine Vorgabe/Erläuterung. Eine Datensicherung, die dann eingreift, wenn das eigentliche Medium zerstört wird und deshalb von diesem ersten Speichermedium sowohl elektronisch als auch physisch/örtlich getrennt ist, entspricht allerdings dem Stand der Technik und ist technisch auch unproblematisch umsetzbar. Nur eine solche Datensicherung entspricht damit auch einer geeigneten technischen und organisatorischen Maßnahme zum Schutz vor Verlust/Zerstörung von Daten.

Sollten die von dem Brand betroffenen Firmen also personenbezogene Daten ihrer Kunden ausschließlich in der – vermeintlich sicheren – „Cloud“ gespeichert haben, läge nicht nur ein (gegebenenfalls dramatischer) betriebswirtschaftlicher Verlust vor, sondern der zuständige Datenschutzbeauftragte könnte auch noch empfindliche Bußgelder – nach Art. 83 Abs. 5 DSGVO bis zu 20.000.000,00 € oder 4 % des weltweit erzielten Jahresumsatzes – verhängen.

Fazit:

Die Sicherung von Daten zeigt insbesondere an vorstehendem Beispiel, dass eine einmalige Speicherung allein in der „Cloud“ nicht für die Erfüllung der Anforderungen der DSGVO ausreichend ist. Vielmehr müssen auch dort gespeicherte Daten noch einmal an einem getrennten Ort gesichert werden.

Wir beraten in datenschutzrechtlichen Fragen und unterstützen unsere Mandanten, Geschäftsprozesse auch unter dem Gesichtspunkt des Schutzes personenbezogener Daten effektiv und in Übereinstimmung mit datenschutzrechtlichen Vorgaben abzuwickeln.

Dietsch
Rechtsanwalt
Fachanwalt für Bau- und Architektenrecht