Gretchenfrage

Die für Datenschützer nicht unerwartete Außerkraftsetzung des Privacy Shields durch den EuGH hat im vergangenen Sommer eine Welle von Vertragsneugestaltungen und viel Unsicherheit ausgelöst. Darf man personenbezogene Daten noch von US-Unternehmen verarbeiten lassen? Und wenn ja: wie? Nicht nur die zahlreichen kleineren Anbieter und Dienste vor allem im Web-Tracking-Umfeld, sondern auch große wie Amazons Web Services, Google Analytics oder Microsoft 365 tun sich schwer damit, hinreichende und ggf. zusätzliche Garantien zum Schutz der Daten vor einem Zugriff der amerikanischen Sicherheitsbehörden zu bieten – schließlich gilt für sie der US-CLOUD Act. Mit allerlei vertraglichen Klimmzügen versuchen sie, dem Dilemma der Unvereinbarkeit des nationalen amerikanischen mit dem europäischen Datenschutzrecht zu entkommen.

Dabei gerät mehr und mehr die entscheidende Frage aus dem Blick. Denn worum geht es im Kern? Unternehmen möchten einem fremden Dritten Daten ihrer Kunden oder ihrer Mitarbeiter anvertrauen, für die sie verantwortlich sind – und es, Vertrag hin oder her, auch bleiben. Die von der DSGVO geforderten vertraglichen Vereinbarungen, technisch-organisatorischen Zusicherungen und anderen Transfer-Instrumente, die mit dem Verarbeiter abgestimmt werden müssen, sind dabei nicht mehr (und auch nicht weniger) als ein Mittel, um die Vertrauenswürdigkeit dieses Dritten zu untermauern. Sie sollten – eigentlich – selbstverständlich sein.

Denn jedes Vertrauen braucht Fundierung. Es erwächst aus langjähriger Zusammenarbeit, eigenen Inspektionen (Audits), offiziellen Anerkennungen, Prüfungen durch anerkannte Institutionen (Zertifikate), klaren Vereinbarungen und rechtlichen Absicherungen. Und selbst dann: Ein wenig verbleibende Skepsis ist kein Fehler. Und das gilt nicht nur für die Verarbeitung personenbezogener Daten durch Dritte: Auch beim Einsatz von Software oder Hardware im eigenen Unternehmen stellen sich diese Fragen, denn niemand kann jede Soft- und Hardware vor dem Einsatz auf die Abwesenheit von Hintertüren und sicherheitskritischen Schwachstellen untersuchen.

Doch vertrauensbildende Maßnahmen erfordern eine etwas genauere Beschäftigung mit Dienst und Dienstleister – keine guten Überlebensbedingungen in einer schnelllebigen Zeit. Sie entfallen daher zumeist und reduzieren sich auf die formale Prüfung und den Abschluss eines Vertrags. Und so mutiert unser immer blinderes Vertrauen in Dienste und Dienstleister Zug um Zug zu reiner Vertrauensseligkeit. Wer nicht ganz geschichtsvergessen ist, weiß, dass das den perfekten „Nährboden" für Täuschung und Betrug abgibt – man denke an den Bauunternehmer Schneider, an Balsam, FlowTex, Enron oder jüngst Wirecard.

Während einerseits nicht nur unsere Abhängigkeit von der IT, sondern auch die von kaum noch austauschbaren Cloud-Diensten Dritter wächst, schrumpft andererseits zugleich das Fundament, auf dem Zusammenarbeit immer gründen sollte: solides Vertrauen.

Wer seine Risiken beherrschen will, sollte sich daher häufiger die Frage stellen: Vertraue ich diesem Dienst oder jenem Dienstleister (ja, und auch: dieser Software) wirklich? Und wenn die Antwort kein klares „Ja" ist, sollte man sich vielleicht besser ein wenig genauer damit beschäftigen. Oder aber wenigstens nicht verwundert die Augen aufreißen, wenn der Blindflug eines Tages schief geht.

Mit herzlichen Grüßen, Ihr