#dcsdacharticle XXXXX

Datenschutz zwischen Anspruch und Wirklichkeit

In Sachen Datenschutz und Datensicherheit ständig up-to-date und clean zu sein, erfordert umfangreiches Knowhow. Dies gilt umso mehr da Rechenzentrumsbetreiber zahlreiche Besonderheiten beachten müssen. Von Bernd Fuhlert, Director Datatree AG.

Umfassender Datenschutz und Datensicherheit auf höchstem Niveau sind für verantwortungsbewusste Rechenzentrumsbetreiber eine Selbstverständlichkeit. „Zugleich aber müssen sie in der Praxis eine Fülle gesetzlicher Vorschriften und einschlägige Gerichtsurteile beachten, die schnell gravierende Lücken zwischen Anspruch und Wirklichkeit reißen können“, warnt Bernd Fuhlert, Vorstand des Düsseldorfer Compliance Providers DATATREE AG. Dies gelte umso mehr als in Deutschland beim Umgang mit personenbezogenen Daten die weltweit strengsten gesetzlichen Datenschutzvorschriften herrschen. Diese sind nicht nur im Bundesdatenschutzgesetz (BDSG) sondern auch in einer Reihe weiterer Gesetze wie beispielsweise dem Gesetz gegen unlauteren Wettbewerb (UWG), dem Urhebergesetz (UrhG), dem Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG) oder auch der Sozialgesetzgebung (SGB) festgelegt, die gegenüber dem BDSG sogar Vorrang haben. Hinzu kommt eine Fülle ständig neuer Gerichtsurteile, die die rechtskonforme Erhebung, Speicherung, Verarbeitung und Nutzung personenbezogener Daten aktuell bestimmen.

Geschäftsführung haftet bei Verstößen

Die Verantwortung für die gesetzeskonforme Umsetzung des Datenschutzrechtes und die Sorge für ständige Datensicherheit aber trägt allein die Leitung des jeweiligen Rechenzentrums. „Damit haftet die Geschäftsführung als sogenannte `Verantwortliche Stelle´ im Schadensfall“, erklärt Datenschutzexperte Fuhlert. „Um Fehler zu vermeiden und alle datenschutzrechtliche Klippen von vornherein zu umschiffen“, müssten Rechenzentrumsbetreiber eine Reihe von Besonderheiten ihres Gewerbes berücksichtigen. So handelt es sich beim Leistungsspektrum der Rechenzentren in Deutschland zumeist um eine klassische Auftragsdatenverarbeitung (ADV) nach § 11 BDSG, wobei das Rechenzentrum als Auftragnehmer fungiert. Eine Auftragsdatenverarbeitung liegt immer dann vor, wenn der Auftraggeber dem Auftragnehmer jeden einzelnen Arbeitsschritt der Datenverarbeitung vorschreibt und zugleich bei diesem die Einhaltung der sogenannten technisch-organisatorischen Maßnahmen überwacht. Der Auftraggeber muss also jederzeit Herr der Daten sein und ist beim Umgang mit personenbezogenen Daten die verantwortliche Stelle.

Das Rechenzentrum als Auftragnehmer hingegen hat keinerlei vertraglichen Verpflichtungen gegenüber den Kunden, Mitarbeitern oder sonstigen Personen, deren Datensätze übermittelt werden. Es nutzt ausschließlich die bereitgestellten Daten. Ihm ist es untersagt, diese Daten zu bearbeiten oder sonstige inhaltsbezogene Entscheidungen zu treffen. „Die jeweiligen Aufgaben und Pflichten der Auftraggeber und-nehmer sind dann in einem Vertrag zur Auftragsdatenverarbeitung festzulegen, für den es wiederum feste inhaltliche Vorschriften im BDSG gibt.“ erläutert DATATREE Vorstand Bernd Fuhlert.

Rechenzentrumsbetreiben drohen bei Verstößen hohe Straf- und Bußgelder

Wofür haben Rechenzentrumsbetreiber als Auftragnehmer nun aber konkret zu sorgen? Im Vertrag verpflichten sie sich, stets für gesetzeskonformen Datenschutz und ausreichende Datensicherheit zu sorgen. Kommt es trotzdem zu Datenschutzverstößen und Sicherheitslecks, richten sich entsprechende Bußgelder und Abmahnungen zwar an den Auftraggeber jedoch wird er die Strafgelder vom Rechenzentrumsbetreiber zurückfordern, da sich dieser als Auftragnehmer vertraglich auf die Einhaltung gesetzlicher Vorgaben verpflichtet hat. Das kann schnell sehr teuer werden. So sind im BDSG Geldbußen bis zu 500.00 Euro vorgesehen, nach dem Entwurf eines wahrscheinlich ab 2015 einheitlich geltenden neuen europäischen Datenschutzrechtes sogar Straf- und Bußgelder im Millionen Euro-bereich. Darüber hinaus können auch noch im Vertrag zur Auftragsdatenverarbeitung vereinbarte Konventionalstrafen fällig werden.

Im Zuge der Auftragsdatenverarbeitung gehört es zu den gesetzlichen Pflichten der Rechenzentrumsbetreiber, die im Paragraphen § 9 BDSG und Anlage vorgesehenen technisch organisatorischen Maßnahmen zu ergreifen. Dazu zählen sicherheitstechnische Maßnahmen wie eine funktionierende Kontrolle, dass Unbefugte keinen Zutritt zum Rechenzentrum haben sowie Maßnahmen, die eine unbefugte Nutzung der Datenverarbeitungssysteme verhindern Der Rechenzentrumsbetreiber muss gewährleisten, dass ausschließlich Berechtigte Zugriff auf personenbezogene Daten haben und diese nicht unbefugt gelesen, kopiert verändert oder entfernt werden können. Das gilt auch für die elektronische Übertragung oder die Weitergabe auf Datenträger.

Eine Änderung darf auch nicht bei der Dateneingabe erfolgen können. Zudem sind die Daten gegen zufällige Zerstörung oder Verlust zu schützen und ausschließlich nach den Weisungen des Auftraggebers zu verarbeiten. Nicht zuletzt ist zu gewährleisten, dass für unterschiedliche Zwecke erhobene Daten getrennt verarbeitet werden. „Alles in allem kommen auf die Rechenzentrumsbetreiber also jede Menge Anforderungen zu, die nicht immer leicht zu bewältigen sind“, so Experte Fuhlert.

Cloud Computing ist umstritten

Das gilt umso mehr da Cloud-Computing- Angebote zunehmen, die Datenspeicherung in der Internet-Wolke jedoch vor allem unter sicherheitstechnischen Aspekten umstritten ist. So kann nicht immer eindeutig festgestellt werden, wo in der Cloud sich die Daten des Nutzers befinden. Die Haftungsrisiken des Rechenzentrumsbetreibers: Auch beim Cloud Computing sind die Vorgaben zur Auftragsdatenverarbeitung nach §9 und §11 BDSG einzuhalten. Die besondere Problematik: Der Rechenzentrumsbetreiber muss seinem Auftraggeber zu jedem Zeitpunkt nachweisen können, wo sich dessen Daten genau befinden.

Während dies bei einer Hardware-Speicherung vor Ort leicht nachzuvollziehen ist, kann das bei einer Cloudspeicherung problematisch sein. „So sollten sich Rechenzentren nicht einer „diffusen Wolke“ bedienen, die jeweils denjenigen Verarbeiter einbindet, der gerade verfügbar und zudem der preiswerteste ist, ohne das nach außen offenzulegen“, warnt Bernd Fuhlert. Zudem gäbe es nicht gerade wenige weitere Klippen obwohl es für den Umgang mit personenbezogenen Daten Orientierungshilfen von Datenschützern und konkrete Sicherheitsempfehlungen für Cloud Computing Anbieter gibt (siehe Anmerkungen).

So hat das Fraunhofer-Institut für Sichere Informationstechnologie in einer Studie die Sicherheitsanforderungen verschiedener Cloud-Dienstleister getestet und dabei zahlreiche Mängel festgestellt. Beispielsweise wurden beim Datentransport keine Schutzmaßnahmen ergriffen oder nicht dokumentierte Protokolle genutzt. Bisweilen erfolgte zudem keine Datenverschlüsselung seitens der Klienten, oder es wurden zwar die Daten, aber keine Dateinamen verschlüsselt.

Treuhand-Datenbank bietet Innovative Datenspeicherung

Folge: „Rechenzentrumsbetreiber, die nachweisen können, dass sie datenschutz- und sicherheitstechnisch up-to-date und clean sind, haben einen Wettbewerbsvorteil und sollten dies auch nach außen dokumentieren“, empfiehlt Datenschutzexperte Fuhlert. Dazu dienten anerkannte Zertifizierungen, die strenge kontinuierliche Prüfungen garantieren.