„Black Cloud“ über einem Rechenzentrum in Deutschland Hat das Auswirkungen nach der DSGVO?

Die FAZ titelt am 13.3.2021: „Am Rhein brennt Europas Datenschutz“ … ein Rechenzentraum der OVH in Deutschland brannte seit 10.3.2021, 00:47 Uhr.

Nach Medienberichten ging in Deutschland **Europas größtes Rechenzentrum in Flammen auf** und damit sind auch **personenbezogene Daten** in einer „**schwarzen Wolke**“ verloren gegangen. Ein **schwarzer Tag für die „Cloud“** bzw. die Unternehmen, die dort ihre Daten „sicher“ abgelegt haben.

Beim **Cloud-Anbieter OVH** sind **12.000 Server** auf fünf Stockwerken (Bericht in der FAZ, 13.3.2021) abgebrannt und **3.6 Millionen Websiten** sind nach dem Brand **offline** (Bericht auf Golem.de). Auf der Website: OVH Tasks veröffentlicht OVH selbst **Informationen zum Stand der Arbeiten** nach dem Brand, und auch auf dem **Corporate-Blog** findet man Informationen: News von OVH Deutschland > Brand an unserem Standort in Straßburg.

Die „Cloud“ auch nur ein physisches Rechenzentrum

Bei der Speicherung in der „Cloud“ deckt man an dezentrale Speicherung, bei der niemand (und schon gar nicht der Verantwortliche iSd DSGVO) weiß, wo konkret die Daten gespeichert werden. Letztlich ist es jedoch dennoch so, dass die Daten in einem **konkreten Rechenzentrum vom „Cloud-Dienste-Anbieter“** gespeichert werden, und wenn dieses **physisch zerstört** wird, dann kann der Verantwortliche nur hoffen oder sicher wissen, weil er dies vertraglich so festgelegt hat, dass seine **Daten**

redundant in einem anderen Rechenzentrum abgesichert weiterhin verfügbar oder vorhanden sind.

Wenn dies nicht der Fall ist, und ein **unwiederbringlicher Datenverlust** oder auch nur eine **Beeinträchtigung der Verfügbarkeit** gegeben ist, dann besteht aus datenschutzrechtlicher Sicht **akuter Handlungsbedarf**.

Datenschutzverletzung melden.

Wenn ein **Verantwortlicher „Daten verliert**“, und zwar entweder weil er diese lokal zB auf einem USB-Stick oder einem mobilen Gerät gespeichert hat, oder wenn er diese „in der Cloud“ abgelegt hat, dann ist er verpflichtet, dies **unverzüglich**, jedoch **längstens binnen 72 Stunden der Aufsichtsbehörde zu melden**, wenn davon **personenbezogene Daten natürlicher Personen** betroffen sind, und aus dem Datenverlust ein **Risiko** für die betroffenen Personen **nicht auszuschließen** ist. (Art 33 DSGVO)

Wenn das **Risiko** für die Rechte und Interessen der betroffenen Personen „**hoch**“ ist, dann sind auch die **betroffenen Personen zu verständigen**. (Art 34 DSGVO)

Wenn sich aus dem Datenverlust eine Situation ergibt, die **kein Risiko für die betroffenen Personen** darstellt, dann ist die Datenschutzverletzung gem. Art 33 Abs 5 DSGVO durch den Verantwortlichen zu **dokumentieren**.

Verlust der Verfügbarkeit als Data Breach?

Schon der **Verlust der Verfügbarkeit**, auch wenn es kein dauerhafter Datenverlust ist, kann zu einer Situation führen, die für die betroffenen Personen, deren Daten verarbeitet werden, ein **Risiko** darstellt, und kann **meldepflichtig** sein. Dies kann zB der Fall sein, wenn eine Website oder ein Online-Service einer Bank, das in der (abgebrannten) Cloud gehostet ist/war, für Kunden nicht erreichbar ist.

Näheres zur Frage der Meldepflicht bei Datenschutzverletzungen erfahren Sie auch in einem unserer Blogbeiträge vom 3.12.2018 zum Thema: Was ist als Datenschutzverletzung zu melden.