Resilienz

Herausforderung im Datenschutzrecht

Der vom lateinischen resilire, „zurückspringen bzw. abprallen", abgeleitete Begriff Resilienz wird in den verschiedenen Wissenschaftsbereichen zur Darstellung und Erklärung der Widerstandsfähigkeit und Belastbarkeit von Menschen, Unternehmungen und Institutionen, Materialien, sowie politischen, wirtschaftlichen, rechtlichen und technischen Systemen verwendet.

Die seit 25.5.2018 innerhalb der gesamten EU für die elektronische Verarbeitung von personenbezogenen Daten geltende DSGVO (Datenschutzgrundverordnung) hat das Thema Belastbarkeit bzw. Resilienz von Systemen auch in das Datenschutzrecht eingeführt. Zentrale Bestimmung hierfür ist Artikel 32 DSGVO. Dieser Artikel fordert von denjenigen, die personenbezogene Daten verarbeiten (Verantwortliche und Auftragsverarbeiter), technische und organisatorische Maßnahmen (TOM) zu ergreifen, die die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT- Systeme sicherstellen sollen. Eine Definition des Schutzzieles „Belastbarkeit" enthält die DSGVO nicht. Es bedarf somit für die Anwender (Verantwortliche und Auftragsverarbeiter) der Auslegung dieses Begriffes. Die meisten Experten setzen Belastbarkeit mit „Robustheit" gleich und verstehen darunter die Fähigkeit von datenverarbeitenden Systemen, erwartbare Störereignisse zu bewältigen. Die Belastbarkeit von IT-Systemen spielt nicht nur bei betriebseigenen IT-Systemen eine Rolle, sondern hat Resilienz eine ganz besondere Bedeutung in den Bereichen connected cars und anderen Verkehrsmitteln mit automatisierter Steuerung, Roboter und IoT.

Eine häufig eingesetzte Maßnahme für das Erreichen von belastbaren und robusten Systemen ist die Redundanz. Angesichts des in der deutschen Fassung der DSGVO verwendeten Begriffes „Belastbarkeit" geben sich die meisten Experten und Autoren damit zufrieden, Schutz vor erwartbaren Störungen von Datensystemen als ausreichend zu erachten. Wenn man aber das in der englischen Fassung der DSGVO (GDPR) verwendete Wort „Resilience" heranzieht, erheben sich Zweifel, ob dieser Schutz vor erwartbaren Störungen von Datensystemen ausreichend ist, um die geforderte Datensicherheit zu gewährleisten. Dieser englische Begriff „Resilience" geht über das deutsche Wort „Belastbarkeit" hinaus und bedeutet Schutz und Maßnahmen, dass ein System auch in unvorhergesehenen Szenarien seine Funktionsfähigkeit aufrechterhalten kann. Thoma (Resilienz by design, 14, 2014) definiert Resilienz „als die Fähigkeit, tatsächlich unter potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. Widrige Ereignisse sind menschlich, technisch sowie natürlich verursachte Katastrophen oder Veränderungsprozesse, die katastrophale Folgen haben". Um das Schutzziel des Artikels 32 DSGVO der Belastbarkeit im Sinne von Resilienz (Widerstandsfähigkeit) zu erreichen, sind aus Sicht des Datenverarbeiters weitergehende Maßnahmen erforderlich. Zu diesen gehören jedenfalls die Einrichtung eines Compliance-Datenschutzsystems, Backup-Systeme, Krisenvorkehrungen für das Krisenmanagement im Schadensfalls,

Gerald Ganzger, Managing Partner Lansky, Ganzger & Partner Rechtsanwälte

Herstellung von Notfallszenarien, klare Vertretungsregelungen im Bereich IT bis hin zu Doppelbesetzungen von IT-Positionen. Eine empfohlene Maßnahme aus technischer Sicht ist auch, die Systeme aus möglichst kleinen Komponenten zusammenzusetzen, damit sie weniger angreifbar sind. Die Diskussion, wie die von Artikel 32 DSGVO geforderte „Belastbarkeit" von IT-Systemen tatsächlich auszulegen ist, wird weiter andauern. Es ist derzeit noch offen, welche Maßnahmen nun tatsächlich zur Erreichung der Belastbarkeit bzw. Resilienz von Datenverarbeitungssystemen zu treffen sind. Die ersten gerichtlichen bzw. behördlichen Entscheidungen zu Schadenersatzforderungen von Betroffenen nach Störfällen werden mehr Klarheit bringen.