UNiSCON Sealed Cloud Technologies
A member of TÜV SÜD

Personaldaten in den Datenraum? Das müssen Vorstände beim Datenschutz beachten

09.07.2019 – München: In deutschen Unternehmen gibt es einen Bereich, in dem Datenverarbeitung immer gleichbedeutend mit der Verarbeitung personenbezogener Daten ist: Human Resources. Denn Personaldaten haben definitionsgemäß stets einen Personenbezug und weisen damit in den meisten Fällen einen erhöhten Schutzbedarf auf.

Personaldaten: DSGVO diktiert die Regeln

Selbstverständlich sind personenbezogene Daten nicht erst seit Inkrafttreten der Datenschutz-Grundverordnung angemessen zu schützen. Bereits das Bundesdatenschutzgesetz (alt) formulierte konkrete Regeln für den Umgang mit personenbezogenen Daten, die auch unter der DSGVO weiter Bestand haben:

- Rechtsgrundlage zur Datenverarbeitung ist erforderlich
- Daten dürfen nicht unbegrenzt gespeichert werden
- Verarbeitung der Daten darf nur für den beabsichtigten Zweck erfolgen
- Datenschutzverletzungen sind meldepflichtig
- Daten sind angemessen zu schützen

Doch darüber hinaus fordert die DSGVO bei Zuwiderhandlungen empfindliche Strafen – vorgesehen sind Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes[1]. Besonders heikel: Pflichtverletzungen im Datenschutzbereich können Geschäftsführer und Vorstände persönlich ersatzpflichtig machen; diese haften dann gegebenenfalls auch mit ihrem Privatvermögen[2]. In Extremfällen können sogar Gefängnisstrafen verhängt werden[3]. Viele Unternehmen setzen daher auf vermeintlich sichere Storage-Angebote wie beispielsweise digitale Datenräume.

Risiko: Privilegierter Zugriff

Doch selbst, wenn die üblichen „technischen und organisatorischen Maßnahmen“ zum Schutz der Daten getroffen werden, bleibt ein nicht zu unterschätzendes Restrisiko. Dieses Risiko besteht selbst dann, wenn die personenbezogenen Daten in einem virtuellen Datenraum oder einer Business Cloud abgelegt sind. Denn gerade organisatorische Maßnahmen wie etwa sorgfältig durchdachte Rechte- und Rollenkonzepte lassen sich mit verhältnismäßig überschaubarem Aufwand umgehen. Darüber hinaus können sich Administratoren in der Regel privilegierten Zugriff zu den Servern verschaffen und vertrauliche Daten einsehen, manipulieren oder entwenden. Das aber bringt die Verantwortlichen in Bedrängnis, denn diese haben die Integrität der Daten sicherzustellen.

Abhilfe durch Technik?

Um personenbezogene Daten wie Personaldaten vor Einsicht, Manipulation oder Verlust zu schützen, braucht es eine technische Lösung, die jeglichen – auch privilegierten – Zugriff zuverlässig unterbindet. Herkömmliche Public-Cloud-Angebote können diese Anforderung in der Regel nicht erfüllen. Sogar viele Business Clouds tun sich schwer, unerwünschte Datenzugriffe wirkungsvoll zu unterbinden – die meisten klassischen Server-Infrastrukturen

[1] https://dsgvo-gesetz.de/art-83-dsgvo/
[2] https://www.rosepartner.de/geschaeftsfuehrerhaftung-datenschutzrecht.html
[3] https://diligent.com/wp-content/uploads/2017/11/WP0032_US_The-GDPR-Checklist-for-Directors.pdf

sehen privilegierte Admin-Zugänge vor, beispielsweise zu Wartungs- oder Monitoring-Zwecken.

Einen besseren Ansatz verfolgen betreibersichere Infrastrukturen[4]: Hier wurden die organisatorischen Schutzmaßnahmen ausnahmslos durch technische Maßnahmen ersetzt, die sich auch mit hohem Aufwand nicht umgehen lassen. Die Server sind hermetisch abgeriegelt, ein privilegierter Admin-Zugriff ist nicht vorgesehen – eine Kenntnisnahme vertraulicher Daten ist ebenso ausgeschlossen wie Diebstahl und Manipulation. Das gilt nicht nur für Administratoren, sondern für alle externen und internen Angreifer.

Unternehmen, die zur Speicherung und Verarbeitung vertraulicher und personenbezogener Daten auf betreibersichere Cloud- und Datenraum-Angebote setzen, sind damit rechtlich auf der sicheren Seite. Stehen die Server noch dazu in einem EU-Land mit besonders hohem Datenschutzniveau wie etwa Deutschland, schafft dies zusätzlich Vertrauen. Die passenden Zertifikate erleichtern den Verantwortlichen überdies die Erfüllung ihrer Rechenschaftspflichten[5].

Betreibersichere Infrastrukturen sind eine noch recht junge Alternative zu herkömmlichen Cloud-Infrastrukturen und werden wegen ihres hohen Datenschutzniveaus seit einigen Jahren zunehmend im geschäftlichen Umfeld eingesetzt. Dazu zählen unter anderem die versiegelte Cloud der Deutschen Telekom und die Sealed Platform der TÜV SÜD-Tochter Uniscon GmbH.

Weiterführende Informationen zu den iDGARD Datenräumen sowie druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de.

Uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die Uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet Uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist Uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

Uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20

[4] https://de.wikipedia.org/wiki/Sealed_Cloud
[5] https://dsgvo-gesetz.de/art-5-dsgvo/

UNiSCON
Sealed Cloud Technologies
A member of TÜV