verneglobal

THE SMART DATA CENTER SOLUTION

Datenschutz, Datensicherheit und Compliance am Beispiel Islands

Dr. J. Bücking

Inhalts

Prolog

In der internationalen Rechtsprechung mag vieles unterschiedlich bewertet und auf unterschiedlichen Rechtsgrundlagen entschieden werden. So verhält es sich beispielsweise im Verhältnis zwischen dem anglo-amerikanischen „case law“ und dem kontinentaleuropäischen Ansatz des kodifizierten Gesetzesrechts. Auch mögen der US-amerikanischen Ansatz, Daten möglichst anschlagsicher über diverse Rechenzentren national oder auch global verteilt aufzubewahren und deren Ortung dementsprechend zu erschweren, in einem diametralen Gegensatz zueinander stehen zu dem kontinentaleuropäischen Dogma, jederzeit Zutritt, Kenntnis und Kontrolle über die technisch-organisatorischen Maßnahmen einschließlich der jeweiligen Lokationen der Daten zu haben. In einem allerdings besteht Einigkeit: Die „rechtssichere“ Aufbewahrung und Verfügbarhaltung von unternehmenskritischer Information gehört heutzutage zu den rechtlichen Selbstverständlichkeiten, entsprechende Backup- und Archivierungsprozesse sind daher zur Einhaltung der jeweils einschlägigen Compliance-Standards unabdingbar. Hinzu tritt seit den Ereignissen des Jahres 2013 mit der NSA-Abhöraffäre die besondere Bedeutung des Schutzes von Geschäfts- und Personendaten. Das Thema Datensicherheit ist mithin aus dem Geschäftsleben nicht mehr wegzudenken. Welche - auch persönlichen - Haftungsrisiken sich allerdings dahinter verbergen, ist dagegen den wenigsten im Detail bekannt. Eine „Noncompliance“ kann hier fatale Folgen haben. Aus der Rechtsprechung sind Fälle bekannt, die von der Anfechtbarkeit des Beschlusses über die Entlastung des Managements bis zur außerordentlichen Kündigung der Anstellungsverträge und Abberufung aus der Funktion des CEO reichen. Dieses Dokument bietet einen Überblick darüber, welche Haftungsrisiken existieren und wie man diese Risiken durch ein geeignetes IT-Sicherheitsmanagement begrenzen kann. Der Fokus gilt dabei dem Backup und der Archivierung aus Sicht des deutschen Datenschutzrechts im Verhältnis zum „Datenfreihafen“ Island.

Teil 1: Rechtspflichten und Haftungsfallen der IT-Sicherheit

Im Unterschied zu früher, als das Eigentum, Rohstoffe, die Qualifikation der Belegschaft, die Auftragslage etc. über Wohl und Wehe eines Unternehmens entschieden, stellt die Verfügbarkeit und der Schutz von Informationen heute die betriebswichtigste Ressource im unternehmerischen Organismus dar. Studien belegen, dass bereits ein 10-tägiger Ausfall von Schlüsselsystemen der IT ein Unternehmen so nachhaltig schädigt, dass es mit einer Wahrscheinlichkeit von 50% innerhalb von 5 Jahren vom Markt verschwindet[1]. 93% der Unternehmen, die infolge eines Totalausfalls mindestens 10 Tage ohne Rechenzentrum auskommen mussten, meldeten innerhalb eines Jahres Insolvenz an[2]. 70% der Unternehmen, bei denen es zu katastrophalen Datenverlusten kam, mussten innerhalb von 18 Monaten aufgeben[3].

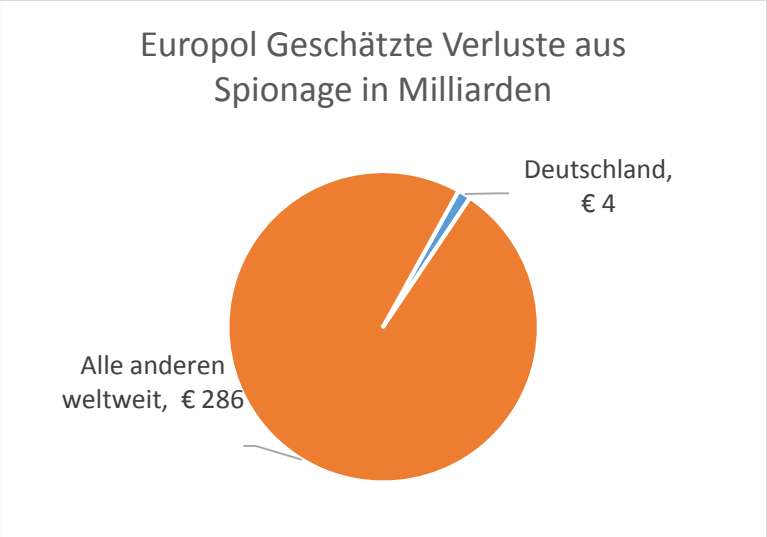
Allgemeine IT-Haftungsrisiken

Aus der allgemeinen Erkenntnis heraus, dass die Verfügbarkeit von Unternehmensdaten ein Do-or-die-Kriterium in Wirtschaft und öffentlicher Verwaltung ist, besteht von Gesetzes wegen die Verpflichtung zu einem effektiven Risiko- und Informationsmanagement einschließlich der dazugehörigen internen Kontrollmechanismen und deren sorgfältiger Dokumentation. Deren Einhaltung ist „Chefsache“ und gehört als Teil der „corporate governance“ zu den unternehmerischen Lenkungs- und Leitungsaufgaben. Insoweit bestehen allerdings auch entsprechende Kontroll- und Hinweispflichten der unternehmerischen Sonderbeauftragten für Compliance, IT-Sicherheit und Datenschutz. Eines der Hauptziele dieses Informationsschutzes ist dabei (neben dem Eigentumsschutz), sich beweisrechtlich für künftige Auseinandersetzungen mit Gegnern, Behörden, Mitarbeitern etc. über Vertragsinhalte, Haftungsansprüche oder eben auch um die Qualität der vertriebenen Produkte selbst oder deren Folgeschäden zu positionieren. Dies kann nur gelingen durch Beweissicherheit, mit der im elektronischen Zeitalter die Informationssicherheit als Vorbedingung untrennbar verbunden ist - wobei die Beweisqualität wiederum maßgeblich bestimmt wird durch die zugrunde liegende IT-Sicherheit: Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit. Ein verantwortungsbewusstes Risikomanagement stellt heutzutage daher einen essentiellen Bestandteil einer hinreichend sicheren Unternehmensstrategie dar. Risikomanagement bedeutet daher nicht zuletzt Unternehmensschutz durch Informations- und Kommunikationsmanagement. Dies gilt insbesondere im Zeitalter von Outsourcing und Cloud-Computing einerseits und der allgegenwärtigen Industriespionage und Kommunikationsüberwachung andererseits:

Wirtschaftsspionage

Besorgnis erregenden Berichten zuverlässiger Quellen wie Europol und dem deutschen Bundeswirtschaftsministerium zufolge werden täglich in Deutschland Daten von 20 Millionen Telefonaten und 10 Millionen Internetverbindungen allein durch den US-Geheimdienst NSA gespeichert. Deutschland ist zudem das wichtigste Spionageziel in der EU. Dabei geht es nicht nur um Terrorschutz sondern auch um Wirtschaftsinteressen. Hiervon ist mutmaßlich die Hälfte aller Unternehmen betroffen. Umfragen beziffern den hierdurch entstandenen Schaden auf 4 Milliarden

[1] META Group Studie, 2003.
[2] National Archives and Records, 2012.
[3] Britisches Wirtschaftsministerium, 2012



Euro, weltweit wird dieser laut Europol auf 290 Milliarden Euro geschätzt. Gerade Mittelständler erleben jeden Tag Spionageangriffe. Jedes fünfte Unternehmen wurde angeblich schon ausspioniert - Tendenz: steigend. Denn mehr als die Hälfte der deutschen Unternehmen schützt sich nur unzureichend gegen Angriffe. Zwar wächst die Sensibilität, dennoch haben laut Studien 25 % der kleinen und mittelständischen Unternehmen überhaupt keine Sicherheitsstrategie. Durchschnittlich geben sie nur 3.300,- EUR im Jahr für die IT-Sicherheit aus, so das Bundeswirtschaftsministerium. Unzählige High Tech-Unternehmen machen Deutschland zu einem der wichtigsten Wissenstandsorte weltweit. Die Angriffe zielen demgemäß auf die Neuentwicklung von Produkten und Produktionsverfahren. Rund um den Globus sind zwar gigantische Rechenzentren entstanden. Jedoch stehen allein fünf der zehn weltgrößten Serverfarmen in den zunehmend in Verdacht geratenden USA. Wirtschaftsverbände und Bundesregierung wollen nun gemeinsam eine Strategie gegen Wirtschaftsspionage erarbeiten. Doch der Aufbau nationaler oder europäischer Cloud-Strukturen ist kostspielig und benötigt Zeit – Zeit, die der Wirtschaft in Deutschland angesichts der massiven und weiter zunehmenden Spionageangriffe nicht zur Verfügung steht[4].

Trotz der Flexibilität und der Kostenfaktoren birgt Daten-Outsourcing in externe Rechenzentren (wie beispielsweise auch Cloud-Strukturen) zahlreiche Risiken, die es so in der Vergangenheit im Zusammenhang mit dem elektronischen Informations- und Kommunikationsmanagement noch nicht gegeben hat. Dies betrifft vor allem die Sicherheit, Vertraulichkeit, Unversehrtheit und Verfügbarkeit von unternehmenskritischen Daten von der Wiege (Generierung) über ihren Lebenszyklus (Bearbeitung, Transport) bis zum Grabe (Archivierung, Löschung). Gemeint sind hier die personenbezogenen und steuerrelevanten Daten, Geschäftsgeheimnisse (wie etwa Forschungs- und Entwicklungsdaten), Kundendaten, Mitarbeiterdaten etc. Für den Fall der personenbezogenen und steuerrelevanten Daten sind empfindliche Bußgelder für jeden Einzelfall der Zugriffsverhinderung oder der unzulässigen Datenverlagerung ins Ausland vorgesehen.

Externe Rechenzentren können einerseits neue Wertschöpfungsketten und erhebliche Einsparungspotenziale erschließen. Jedoch sind transparente und detaillierte Anforderungen sowie die Prüfung, ob diese Lösung technisch und rechtlich sicher umgesetzt werden können, unabdingbar. Die Rechtsprechung sieht es hier als Selbstverständlichkeit an, dass unternehmenskritische – und insbesondere auch beweiserhebliche - Dokumente bei den Unternehmen vorgehalten werden. Ist dies nicht der Fall kann ein Prozess bereits wegen Beweisfälligkeit verloren gehen. Von Unternehmen wird erwartet, dass sie die Verfügbarmachung elektronischer Dokumente in geordneter Weise

[4] Überblick und weitere Nachweise unter http://www.3sat.de/mediathek/?mode=play&obj=38719; http://www.capital.de/themen-newsbeitrag/die-deutsche-cloud.html; Breucher, Handelsblatt vom 17.09.2013; http://www.heise.de/newsticker/meldung/Kommentar-Schlandnetz-gegen-NSA-die-feuchten-Schengen-Traeume-der-Telekom-2044024.html?wt_mc=rss.ho.beitrag.rdf

gewährleisten können oder aber entsprechende Sanktionen zu erwarten haben. Oft genug entscheiden derlei Dokumente einen Rechtsstreit, indem sie eine Anspruchsposition belegen oder eine Gegenposition beweisrechtlich widerlegen.

Gerade auch Unternehmen mit effektiver Geschäftstätigkeit im UK und den USA sehen sich der besonderen Bedeutung (und erheblichen Sanktionsfolgen) eines lückenlosen und beweissicheren Dokumentmanagement ausgesetzt. Dementsprechend wurden die Zivilprozessordnungen beispielsweise im UK in 2010 ergänzt um Regelungen zur elektronischen Bereitstellung. Dasselbe gilt für Ergänzungen im US-Zivilprozessrecht im Jahre 2006. Im Zuge dieser Entwicklungen wurden zugleich neue Sanktionen für Vertraulichkeits- und Datenschutzverletzungen implementiert.

Unternehmen sehen sich aber auch im globalen Wettbewerb untereinander gesteigerten Anforderungen in Bezug auf den Schutz und die Vorhaltung ihres geistigen Eigentums ausgesetzt angesichts steigender Risiken von Datenverlust und dem Diebstahl von Daten, für den sich inzwischen ein grauer Markt entwickelt hat. Vor diesem Hintergrund arbeiten heutzutage unabdingbar die Abteilungen IT und Recht zusammen an der Schaffung und Implementierung neuer Policies und technisch-organisatorisch abgesicherter Geschäftsprozesse. Hier geht es zum einen um den Reputationsschaden, Auftragsverluste und weitere finanzielle Einbußen, wenn vertrauliche Daten verloren gehen, gestohlen werden oder kompromittiert werden. Schwere Verletzungen des Personendatenschutzes können zum anderen aber inzwischen auch sehr hohe direkte Strafsanktionen von in Deutschland bis zu 300 TEUR für jeden Einzelfall zur Folge haben. Und mit bis zu 250 TEUR kann jeder Einzelverstoß gegen das in der Abgabenordnung verankerte Recht der Außenprüfung auf Datenzugriff geahndet werden. Mit dieser Geldbuße können beispielsweise Fälle einer unzulässigen Auslandsverlagerung der elektronischen Buchhaltung sanktioniert werden. Damit, dass der Steuergesetzgeber dem Steuerpflichtigen unter bestimmten Voraussetzungen das Recht einräumt, elektronische Bücher in einem anderen Mitgliedstaat der EU zu führen und zu verwahren, trägt er einerseits dem unternehmerischen Bedürfnis der Arbeitsteiligkeit in internationalen Konzernen Rechnung, verbindet dies andererseits jedoch für den Fall der Unzulässigkeit mit einer scharfen Sanktion, unabhängig davon, ob es sich um einen In- oder Auslandssachverhalt handelt.

Die Verletzung der Aufbewahrungspflicht kann aber auch strafrechtliche Folgen haben, die über den Personendatenschutz, die Besteuerung und den Schutz von geschäftskritischen Daten noch hinausgehen. Wenn beispielsweise der Verlust oder die Unauffindbarkeit von Finanzdaten eine vollständige Übersicht über die Vermögensverhältnisse des Unternehmens erschwert, ist eine Haftung des Unternehmens und seiner Organe nicht ausgeschlossen. Ebenso kann dies der Fall sein bei der Gefährdung von Geschäftsgeheimnissen. So hat der Bundesgerichtshof die Haftung von Vorstand und Compliance-Officer erweitert in Bezug auf eine Garantenpflicht, im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern. Es besteht eine entsprechende Verpflichtung sicher zu stellen, dass keine Straftaten aus dem Unternehmen heraus begangen werden[5]. Neben dem Compliance-Beauftragten gilt dies grundsätzlich auch für andere Sonderbeauftragte wie den IT-Sicherheitsbeauftragten und ggf. auch den Datenschutzbeauftragten.

[5] BGH, Urt. v. 17.07.2009, 5 StR 394/08.

Eine in jeder Hinsicht rechtskonforme, geordnete und jederzeit verfügbare Aufbewahrung der elektronischen Geschäftspost ist aber - wie bereits dargelegt - auch prozessrechtlich aus Gründen der strategischen Rechtssicherheit unabdingbar, insbesondere um sich gegebenenfalls für eine künftige juristische Auseinandersetzung beispielsweise mit Vertragspartnern, Betriebsrat, einzelnen Mitarbeitern, Dritten oder auch den Steuerbehörden beweisrechtlich positionieren zu können. Denn das Hauptrisiko stellen in wirtschaftlicher Hinsicht die Haftungsfolgen infolge von Versäumnissen beim IT-Risikomanagement dar. Das Schadenspotenzial, das sich beispielsweise aus der Nichtverfügbarkeit beweiserheblicher Daten oder betriebswichtiger Systeme ergeben kann, ist beträchtlich. Neben der persönlichen Haftung des Managements ist hier wie eingangs angedeutet die volle Bandbreite der Schadenshaftung, von der Anfechtbarkeit des Beschlusses über die Vorstandsentlastung bis zur außerordentlichen Kündigung des Anstellungsvertrages (nebst Abberufung aus der Funktion des CEO), eröffnet.

Ein zentraler Bestandteil dieses Risiko-Controllings ist das Informations- und Kommunikationsmanagement, das insbesondere die Betriebs- und Angriffssicherheit der IT-Infrastruktur sowie die in dieser Infrastruktur verwalteten Informationen betrifft. Hier geht es um die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit betriebswichtiger Information wie z.B. der elektronischen Post, Entwicklungsdokumentationen, Geschäftsgeheimnisse, sonstige Unterlagen von besonderem Schutzniveau (z.B. Gesundheitsdaten), beweisrelevanter oder sonst betriebskritischer Unterlagen etc.. Die Umsetzung dieser Pflichten in der Unternehmenspraxis erfolgt oft nur zögerlich. Organisatorische Versäumnisse können hier freilich im Schadensfall (z.B. Verlust oder ungewollte Verbreitung wichtiger Daten) als Verschulden des Managements gewertet werden und - neben der Haftung der Verantwortlichen – auch den Verlust des Versicherungsschutzes (dazu sogleich unten) nach sich ziehen.

Tendenzen der Rechtsprechung

Die Rechtsprechung unterstreicht, dass eine zuverlässige IT-Sicherheit in Bezug auf Unternehmensdaten zu den unternehmerischen Selbstverständlichkeiten im Zeitalter digitaler Datenverarbeitungen gehört. Nicht zuletzt das höchste deutsche Zivilgericht, der Bundesgerichtshof, sieht die Sicherheit der Kommunikation als Compliance-relevante Verpflichtung an und hat entschieden, dass geschäftliche Interna nicht ungesichert per E-Mail zur Verfügung gestellt werden dürfen, da dem Unternehmen, das solche Daten in Kenntnis des Gefährdungspotentials beispielsweise ungesichert über Internet verschickt, der Vorwurf des strafbaren Geheimnisverrats zur Last liegen könnte[6]. Andere Gerichte fordern, dass eine Sicherung von Unternehmensdaten täglich, eine Vollsicherung mindestens einmal wöchentlich erfolgen müsse[7]. Selbst wenn Mitarbeiter externer EDV-Fachfirmen für den Verlust von unternehmenskritischen Daten verantwortlich wären, bleibe es dabei, dass dem Unternehmen selbst eine Alleinschuld am entstandenen Datenverlust und damit an dem hierdurch verursachten finanziellen Schaden vorzuwerfen wäre. Und die Arbeitsgerichtsbarkeit sieht im betrieblichen Interesse an Datensicherheit ein Rechtsgut, das höher zu werten ist als das der

[6] BGH, B. v. 26.02.2013, KVZ 57/12.
[7] Vgl. OLG Hamm, Urt. v. 01.12. 2003, 13 U 133/03.

unternehmerischen Mitbestimmung. In technischer Hinsicht angemahnt werden insbesondere zeitnahe Backups, revisionssichere Archivierungsprozesse, Firewalls, Filter- und Überwachungssysteme, eine Verschlüsselung jedenfalls bei besonders sensitiven Daten sowie eben auch ein Kontinuitätsmanagement, das einen Wiederanlauf nach Wiederherstellung von System und Daten im Schadensfall gewährleistet. Organisatorisch sind geeignete IT-Unternehmens- und Datenschutzrichtlinien und entsprechende Schulungen der Mitarbeiter erforderlich.

Zusammengefasst etabliert die Rechtsprechung zunehmend – und eben auch vor dem Hintergrund neuerer Regelwerke wie den SEC-Regeln, dem Sarbanes-Oxley-Act oder den Baseler Eigenkapitalübereinkünften – allgemeine Sorgfaltspflichten für eine effektive, zeitgemäße IT-Sicherheit. Allgemein lässt sich die Tendenz der Gerichte ersehen, eine Vorlage von Daten, auch wenn diese bereits vor langer Zeit in großen, gegebenenfalls auch externen oder auch internationalen (Backup-) Speichern abgelegt wurden und entsprechend schwer verfügbar gemacht werden können, für ein laufendes Gerichtsverfahren in einer beweisfesten Form zu verlangen. Dies bedingt ggf. den Einsatz zeitgemäßer IT-Systeme, die starke Indizien für Beweissicherheit – und damit letztlich Rechtssicherheit - liefern.

Schadensfolgen unzureichenden Informationsmanagements

Nachdem die unmittelbaren Haftungsrisiken erörtert wurden, stellt sich aus unternehmerischer Sicht im Folgenden die Frage nach den Möglichkeiten einer Haftungsentlastung bzw. Schadenskompensation bei Realisierung der zuvor aufgezeigten Risiken. Hier kommt der Aspekt des Versicherungsschutzes ins Spiel. Versäumnisse können im IT-Risikomanagement zum Verlust des Versicherungsschutzes führen, denn mangelnde IT-Compliance ist als Erhöhung der versicherten Gefahr z.B. in der IT Coverage Versicherung und in der Director's and Officer's Versicherung anzeigepflichtig. Das Fehlen bzw. die Ungeeignetheit einer dem Stand der Technik entsprechenden IT-Infrastruktur und deren Einbettung in ein ganzheitliches Risikomanagement können im Rechtsstreit als grobe Fahrlässigkeit zum Verlust des Versicherungsschutzes oder zum erfolgreichen Einwand des Mitverschuldens der Gegnerversicherung führen. Im Extremfall kann es zu einer Reduzierung der eigenen Schadensansprüche auf Null kommen, wenn Mängel der IT-Compliance den Schaden ermöglicht, mit verursacht oder erhöht haben.

Ausfälle der IT-Infrastruktur oder der Verlust wichtiger bzw. die Offenbarung vertraulicher Daten können aber sehr leicht zu einem über den bezifferbaren Schaden deutlich hinausgehenden Imageschaden führen, insbesondere wenn grobe Versäumnisse im Bereich des Datenschutzes an die Öffentlichkeit gelangen. Hinzu kommt ggf. die sog. „Skandalisierungspflicht". Hiernach ist der Verlust oder die Verbreitung besonders sensibler Daten (etwa Bankdaten, Kundendaten, Mitarbeiterdaten, Kommunikationsdaten mit Kunden, Mitarbeitern, Behörden, Wirtschaftsprüfern, Anwälten etc.) nicht nur der zuständigen Aufsichtsbehörde und der von der Datenschutzverletzung betroffenen Person anzuzeigen sondern dieser Umstand gegebenenfalls zudem in mindestens halbseitigen Anzeigen in zwei bundesweit erscheinenden Tageszeitungen zu veröffentlichen. Eine solche Benachrichtigung der Betroffenen und des Bundesbeauftragten für den Datenschutz und die Informationssicherheit ist jedoch nicht erforderlich bei einem entsprechenden Sicherheitskonzept und einer verschlüsselten

Speicherung. Auch hier zeigt sich, dass nur ein hoher Standard bei der IT-Sicherheit gewährleisten kann, dass Folgeschäden für das Image des Unternehmens verhindert werden.

Haftungsentlastung des Managements durch „IT-Compliance“

Ist von IT-Sicherheit die Rede, wird es also zumeist um die Sicherheit, Integrität, Vertraulichkeit und Verfügbarkeit von kritischen Daten gehen. Zu beachtende Rechtspflichten betreffen beispielsweise den sicheren Ein- und Ausgang von elektronischen Informationen (E-Mails, Buchungen, Bestellungen) sowie die Verwahrung und den Schutz von Kunden- und Mitarbeiterdaten. Über diese allgemeinen Anforderungen hinaus verlangt das Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG) im Bereich der Privatwirtschaft ein effizientes Risikomanagementsystem, das nach einhelliger Ansicht eine Überwachung und Früherkennung sowie entsprechende Reaktionsszenarien im Schadensfall (Desaster Recovery, Business Continuity) umfasst. Die Organe von Aktiengesellschaften und größeren Kapitalgesellschaften sind verpflichtet, geeignete Schutzmaßnahmen in Bezug auf die IT-Sicherheit, gerade auch für betriebswichtige Systeme und Daten, zu konzipieren und umzusetzen. Im Falle des Schadenseintritts wird ihr Verschulden vermutet. Besonders bemerkenswert ist, dass das KonTraG als Sanktion die persönliche Haftung der geschäftsführenden Organe zur Kompensation eines durch IT-Missmanagement hervorgerufenen Schadens beim Unternehmen vorsieht. Hierbei ist zu berücksichtigen, dass durch eine besondere gesetzliche Beweislastumkehr die Vorstände nachweisen müssen, dass sie ihren Pflichten in einem ausreichenden Maße nachgekommen sind. Ihr Verschulden wird quasi von Gesetzes wegen vermutet. Die Vorstände haften also persönlich und zusätzlich wird der Aufsichtsrat verpflichtet, Schadensersatzansprüche gegen sie zu verfolgen.

Die Einrichtung eines Risikomanagements war zwar ursprünglich unmittelbar nur für Aktiengesellschaften vorgeschrieben. Ausgehend von der Begründung zum KonTraG hat das Gesetz jedoch inzwischen erhebliche Ausstrahlungswirkung auf andere Gesellschaftsformen und den Inhalt der allgemeinen kaufmännischen und behördlichen Sorgfaltspflichten erlangt. Hinzu kommt, dass Vorstände von Konzernen, Beteiligungsgesellschaften etc. nach den Überlegungen des Gesetzgebers ihrer Verpflichtung zum Risikomanagement konzernweit nachkommen müssen. Da auch von Tochterunternehmen bestandsgefährdende Risiken ausgehen können, spielt deren Rechtsform insoweit keine Rolle. Die Verpflichtung zu einem effektiven Risikomanagement nach dem Vorbild des KonTraG ist infolge dieser Ausstrahlungswirkung nicht (mehr) auf den Bereich der Privatwirtschaft beschränkt. In der öffentlichen Verwaltung gelten diese Grundsätze in weiten Teilen entsprechend.

Fazit

Allen genannten Vorschriften und Rechtspflichten ist gemein, dass sie gerade auch die sichere Informationsverbreitung und Informationsaufbewahrung betreffen. Stets geht es um sensible Informationen und ihre Verfügbarkeit in bestimmter Form für eine bestimmte Dauer. Gehaftet wird in diesem Bereich unter anderem für die technisch und rechtlich sichere Aufbewahrung und die jederzeitige Vertraulichkeit, Integrität und Verfügbarkeit solcher Daten. Die Haftungsfolge tritt ein bei Fehlen oder Ungeeignetheit eines auf ihren Schutz, notfalls auf ihre Wiederherstellung gerichteten Konzepts. Das geforderte Risikomanagement ist als „ganzheitliches“ zu verstehen. Es beschränkt sich nicht auf die technischen Schutzvorkehrungen, sondern meint gleichermaßen seine rechtliche und organisatorische Einbindung in die innerbetrieblichen Abläufe. Gerade Backup und Archivierung sind

aus dem betrieblichen Alltag nicht mehr wegzudenken. Diese Maßnahmen rechts- und revisionssicher umzusetzen und praktikabel in den Arbeitsalltag einzubinden gehört zu den Herausforderungen des Managements. Die Wahl des Systems und die Komplexität der betrieblichen Umsetzungsorganisation müssen dem Wert der Information gerecht werden.

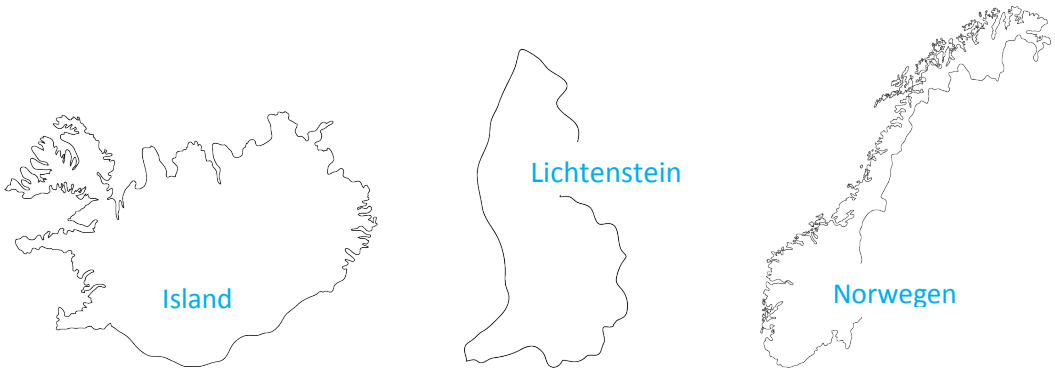
Teil 2: Datenexport in internationale Cloud-Strukturen am Beispiel Islands

Im Bereich des EU-Binnenmarktes (EU) und des Europäischen Wirtschaftsraums (EWR) können sich bei länderübergreifenden Datentransporten in externe Rechenzentren der Nutzer (als Datenexporteur) und der Betreiber (als Datenimporteur) gegebenenfalls auf das Privileg der sog. „Auftragsdatenverarbeitung“ berufen. Es bedarf dann grundsätzlich nicht mehr der Prüfung, ob im Drittstaat, d.h. im Land des Datenimporteurs, ein „angemessenes Datenschutzniveau“ besteht, wie es ansonsten notwendigerweise bei Datentransfers zunächst festgestellt werden müsste. Seitens des nutzenden Unternehmens muss hierbei eine besondere Zuverlässigkeitsprüfung des betreibenden Anbieters und der von diesem getroffenen technisch-organisatorischen Maßnahmen erfolgen, seitens des Betreibers müssen die entsprechenden Sicherheitsgarantien gegeben werden.

Ein angemessenes Datenschutzniveau wurde für Staaten wie Island durch die EU-Kommission zwar explizit festgestellt. Diese Angemessenheitsfeststellung hätte jedoch dennoch nicht automatisch zur Folge gehabt, dass die Daten verarbeitenden Stellen dort rechtlich als Auftragnehmer für die Auftragsdatenverarbeitung behandelt werden könnten. Sie blieben externe Dritte, sodass eine Datenweitergabe an diese Stellen als Datenübertragung zu qualifizieren ist, die nur unter sehr engen, strengen Voraussetzungen zulässig wäre.

Island: Datenfreihafen, Schweiz für Bits?

Den Mitgliedstaaten der EU stellt das deutsche Datenschutzgesetz allerdings nun die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum EWR (Island, Lichtenstein, Norwegen) gleich.



Denn dieses Abkommen verpflichtet in gleicher Weise zur Umsetzung der wichtigen EU-Datenschutzrichtlinie 95/46/EG. Darauf gründet ihre Einbeziehung in die Regeln des europäischen informationellen Binnenraums. Dahinter steht die Überlegung, einen „europäischen Wirtschaftsraum“ zu schaffen, der wie der EG-Binnenmarkt einen freien Waren-, Dienstleistungs- und Kapitalverkehr sowie die Freizügigkeit sichern soll. Da dies einen grenzüberschreitenden intensiven Datenaustausch mit sich bringt, zählt die EU-Datenschutzrichtlinie zu den auch für den EWR maßgeblichen Regelungen. Der Anwendungsbereich des EWR-Abkommens hat sich seit dem Beitritt Finnlands, Österreichs und Schwedens zur EU auf Norwegen, Island und Lichtenstein reduziert.

Für Island gilt die allgemeine Tendenz, bei globalen Datenverarbeitungen und Datenübermittlungen einheitliche Verarbeitungsregeln zugrunde legen zu können, in besonderem Maße: Das isländische Parlament hatte 2010 die Regierung in Reykjavik damit beauftragt, die gesetzliche Grundlage für einen sog. „Datenfreihafen“ zu schaffen. Der Begriff der „Schweiz für Bits“ machte die Runde. In 2011 wurde daraufhin das erste von insgesamt 13 Mediengesetzen erlassen, die unter dem Akronym IMMI firmieren. IMMI steht für „Icelandic Modern Media Initiative“. Auch Neubestimmungen zur Datensicherheit im engeren Sinne, ohne die ein effektiver Datenschutz nicht gewährleistet werden kann, sind Bestandteil der Initiative, insbesondere die Sicherheitsaspekte beim Betrieb von Großrechenzentren und bei der verteilten Speicherung und Verarbeitung großer Mengen von Daten (Cloud-Computing).

Der Anspruch des isländischen Gesetzgebers ist, eine Jurisdiktion zu schaffen, der die im Sinne der Meinungs- und Pressefreiheit liberalsten und im Sinne des Informationsschutzes strengsten Rechtsordnungen als Substrat in einem modernen nationalen Informationsschutzrecht miteinander vereinigt. Die Initiative stellt wenn man so will den Versuch eines „Best-Of“ verschiedener Mediengesetze aus unterschiedlichen Ländern dar.

Eine Preisgabe von Informationen auf rechtlicher Grundlage erscheint demnach ausgeschlossen. Dank dieser Gesetze sollen – vereinfacht dargestellt – Interessierte ihre Aktivitäten über Server laufen lassen können, die in Island und insofern unter dem Schutz der IMMI stehen. Dahinter steht die Gewährleistung einer sicheren Kommunikation und sicherer technischer Infrastrukturen gegenüber Eingriffen Dritter. Dies schaltet die klassischen Internetdiensteanbieter demnach von vornherein aus. In technischer Hinsicht wird es der Zuverlässigkeit der dortigen Betreiber von Rechenzentren und der von ihnen eingesetzten Systeme obliegen, die zu schützenden Daten gegen Angriffe Dritter zu sichern.

Damit soll nicht zuletzt die Gefahr des Informationsmissbrauchs durch internationale Nachrichtendienste gebannt werden. Als insoweit aus deutscher Sicht in der Vergangenheit immer wieder stark kritisiertes Vehikel solcher Eingriffe ist insbesondere der „US Patriot Act“ zu nennen, der den Zugriff auf Daten in Cloud-Strukturen auch außerhalb der USA erlaubt. Hierbei handelt es sich um eine Zugriffsbefugnis der US-Strafverfolgungsbehörden auf die digitalen Informationen, die US-Unternehmen speichern, unabhängig vom Speicherort. Maßgeblich ist nur, wo sich der Hauptsitz des Providers befindet. Per sog. „Gag-Order“ wird darüber hinaus unterbunden, dass die Firmen, deren Daten verwendet werden, darüber informiert werden. Die meisten Cloud-Anbieter, darunter die Marktführer, fallen in die Zuständigkeit der US-amerikanischen Rechtsprechung - entweder, weil sie US-Firmen sind oder aber, weil sie regelmäßig in den USA Geschäfte betreiben.

Schon vor der IMMI hatte Island im Jahre 2001 auf Grund seiner Verpflichtung aus dem EWR-Abkommen zur Umsetzung der EU-Datenschutzrichtlinie 95/46/EG ein neues Datenschutzgesetz nach Maßgabe des Beispiels von Norwegen in Kraft gesetzt, um über weitgehend aufeinander angestimmte Vorschriften eine wichtige Voraussetzung für einen schnellen und reibungslosen Zugriff zu schaffen. (Die EU-Datenschutzrichtlinie hatte sich demgemäß schon zuvor zu einem international genutzten

Regelungsmodell entwickelt; die fast gleichzeitig im April bzw. Mai 2000 verabschiedeten Neufassungen des isländischen und des norwegischen Datenschutzgesetzes waren weiteres Beleg hierfür.) Die isländischen Regelungen lassen sich ohne weiteres auf eine Ebene mit den Datenschutzgesetzen der EU-Mitgliedstaaten stellen und sind daher von den Mitgliedstaaten gleichermaßen zu beachten wie inländische Gesetze.

Datenübermittlungen nach Island sind demnach rechtlich privilegiert, da sie im Ergebnis nur eine Variation der Weitergabe von Daten an inländische Stellen darstellen. Eine Datenübertragung nach Island ist folgerichtig rechtlich und technisch-organisatorisch nicht weitergehend als im Falle rein inländischer Datenübertragungen. Die Feststellung eines angemessenen Datenschutzniveaus ist nicht geboten. Es bedarf daher weder der Verwendung spezieller Standardvertragsklauseln, wie sie die EU-Kommission für die Beauftragung von Datenverarbeitungen im außereuropäischen Ausland zur Verfügung stellt, noch unternehmensinterner verbindlicher Konzernrichtlinien (BCR: „binding corporate rules“), die ein angemessenes Schutzniveau durch entsprechende Vertragsgestaltung im Konzern sicherstellen, noch spezieller Zertifizierungen oder Selbstverpflichtungen wie insbesondere nach der „safe harbor“-Liste des US-Handelsministeriums.

Es gilt das Prinzip der Gleichbehandlung mit der inländischen Situation, sodass keine erst noch durch eine besondere Erlaubnisnorm im Einzelfall zu rechtfertigende Datenübermittlung an Dritte vorliegt. Insoweit liegt eine grenzüberschreitende Auftragsdatenverarbeitung nach § 11 BDSG vor. Diese ist immer dann anzunehmen, wenn beispielsweise Daten aus der Bundesrepublik Deutschland in einen EU/EWR-Staat exportiert werden. Ebenso ist dies der Fall, wenn eine rechtlich unselbstständige inländische Niederlassung Daten an die Unternehmenszentrale mit Sitz in dem entsprechenden EU/EWR-Ausland weitergibt.

Zu beachten ist allerdings noch, dass im Falle der automatisieren Übermittlung von Mitarbeiterdaten regelmäßig dem Mitbestimmungsrecht des Betriebsrates genügt werden muss. Empfohlen wird diesbezüglich, die Betriebsvereinbarungen in Vertragsklauseln oder BCR für verbindlich erklären zu lassen.

Auftragsdatenverarbeitung

Auch eine Auftragsdatenverarbeitung folgt freilich strengen Regeln in Bezug auf den Schutz und die Sicherheit von Daten, die sich in erster Linie an das Nutzerunternehmen richten, von diesem aber an den Betreiber weitergegeben werden. Verlangt werden von diesem u.a. die Absicherung der Abschottung der Daten seiner Kunden voneinander und die Zusicherung bestimmter Methoden zur Trennung dieser Daten. Erfolgt dies durch Verschlüsselung, so muss diese Verschlüsselung eine hinreichende Sicherheit auch für die Zukunft bieten und darf insbesondere nicht durch andere Kunden oder durch den Betreiber selbst kompromittiert werden können. Es bedarf daher beim Betreiber eines dokumentierten Datenschutz- und Datensicherheitsmanagements, eines allgemeinen IT-Sicherheitsmanagements und eines Vorfallmanagements. Da die Zuverlässigkeit des Betreibers und der von ihm eingesetzten Systeme maßgebliches Kriterium auch für die haftungsrechtliche Entlastung

im Schadensfalle sind, sollte hier bei der Auswahl ein erhebliches Augenmerk auf Transparenz und insbesondere die Auditierung durch unabhängige Stellen gelegt werden.

Im Falle Islands besteht daher zwar eine entsprechende Privilegierung als EWR-Mitgliedstaat, sodass ein weitgehend freier Datenfluss möglich ist. Einige nicht unerhebliche „Hausaufgaben" sind gleichwohl zu erledigen:

Technisch-organisatorische Datensicherheitsmaßnahmen

Die Feststellung eines angemessenen Datenschutzniveaus entbindet nicht von Folgeüberlegungen zu technisch-organisatorischen Maßnahmen (TOM) der Sicherheit beim Transfer der Daten (im Beispiel nach Island). Bei einem entsprechenden Auftragsdatenverarbeitungsvertrag sind die entsprechenden Schutzmechanismen zu Gunsten der Betroffenen (insbesondere Mitarbeiter, Kunden) zu berücksichtigen.

Das einschlägige nationale Recht, das auf einen solchen Datentransfer Anwendung findet, ist grundsätzlich das Recht des Staates, in dem die verantwortliche Stelle ihren Sitz hat. Diese Stelle ist für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Nach der EU-Datenschutzrichtlinie ist verantwortliche Stelle die Stelle, die „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". „Auftragsverarbeiter" ist die Stelle, die „im Auftrag des für die Verarbeitung Verantwortlichen" arbeitet. Mit Zweck ist das „Warum" der Datenverarbeitung gemeint, mit dem Mittel das „Wie". Maßgeblich ist, welche Stelle faktisch befugt ist, über diese Fragen zu entscheiden. Die deutschen Datenschutzbehörden bestimmen beim internationalen Datentransfer die exportierende Stelle mit der Kontrollfrage: „Wer öffnet die Tür zum Datenexport".

Bei dieser Auftragsdatenverarbeitung müssen bestimmte Regelungsbereiche vertraglich festgelegt werden um sicherzustellen, dass der beauftragte Betreiber (Auftragsverarbeiter bzw. Datenimporteur) die Daten tatsächlich nur nach den Weisungen des Kunden (Datenexporteurs) verarbeitet. Der deutsche Gesetzgeber hat hierzu in § 11 Bundesdatenschutzgesetz einen 10-Puntke-Katalog von Regelungsgegenständen festgeschrieben. Die EU-Datenschutzrichtlinie verlangt demgegenüber „nur" einen schriftlichen Vertrag. Als (weitere) deutsche Besonderheit liegt bei einem Transfer von einer verantwortlichen Stelle in Deutschland an einen Auftragsverarbeiter in der EU oder dem EWR überhaupt keine „Übermittlung" in rechtstechnischen Sinne mehr vor, da der Auftragsverarbeiter der verantwortlichen Stelle zugerechnet wird. Es bedarf dann keiner besonderen Erlaubnisnorm mehr.

Notwendiger Bestandteil des - demnach zwingend schriftlich zu fassenden - Auftragsdatenverarbeitungsvertrags ist insbesondere Festlegung der möglichen Standorte der Datenverarbeitung sowie entsprechende Kontrollrechte des Kunden gegenüber dem Betreiber einschließlich seiner Subunternehmer, wobei diese Kontrollen in Bezug auf die Subunternehmer auch durch den Betreiber selbst und nicht zwingend durch den Kunden erfolgen können. Der Betreiber ist dazu verpflichtet, über alle Unterauftragsverhältnisse und über alle Orte, an denen die Daten gespeichert oder verarbeitet werden, jeweils zu informieren. Unerlässlich sind ferner die Aufnahme

einer Verpflichtung zur unentgeltlichen Löschung oder Rückübertragung nach Weisung, insbesondere also nach Beendigung des Auftrages, und die Gewährleistung der Kontrolle der vom Betreiber getroffenen TOM - vor Vertragsbeginn und danach regelmäßig. Dabei gilt als gesicherte Rechtsmeinung, dass eine eigene Verpflichtung des Kunden zur Kontrolle vor Ort nicht besteht und die Zuverlässigkeit des Betreibers demnach auch durch transparente Audits geeigneter Prüforganisationen erfolgen kann. Der Vorbehalt eines Rechts zur Kontrolle vor Ort sollte allerdings vom Kunden in den Katalog von Maßnahmen, der vertraglich zu fixieren ist, einbezogen werden.

Es besteht eine strenge gesetzliche Verpflichtung zur sorgfältigen Betreiberauswahl. Ein Blick auf die Datensicherheit allein genügt dabei nicht. Vielmehr ist neben der Sicherstellung der jederzeitigen Verfügbarkeit, Vertraulichkeit und Integrität eine Compliance nach Maßgabe des gesamten TOM-Katalogs der Anlage 1 zu § 9 BDSG - den sog. „8 Geboten der Datensicherheit“[8] - zu gewährleisten. Mit einschlägigen Zertifikaten z.B. von Branchenverbänden wie dem VOI oder dem EuroPrise-Zertifikat des ULD können die Betreiber von Rechenzentren in der EU und dem EWR die Einhaltung der gesetzlichen Vorgaben verlässlich und transparent nachweisen (Cloud „Made in Europe“).

[8] Anlage zu § 9 Satz 1 BDSG: Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

- nbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder enutzt werden, zu verwehren (Zutrittskontrolle),
- verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die rer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der erarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden nnen (Zugriffskontrolle),
- gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres ansports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden nnen, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener aten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene aten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den eisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind erfügbarkeitskontrolle),
- gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Fazit

Die Auslagerung von Daten erfordert demnach gründliche Vorarbeiten im Hinblick auf den Schutz und die Sicherheit, Integrität, Vertraulichkeit und Verfügbarkeit von personenbezogenen Daten, Geschäftsgeheimnissen und steuerrelevanten Daten. Bei Nichtbefolgung drohen Bußgelder der zuständigen Behörden sowie im Falle der Nichtverfügbarkeit beweiserheblicher Dokumente, die - wie im ersten Teil dargelegt -in der Praxis das höchste Schaden- und Haftungspotenzial haben, materielle und immaterielle Schäden für die Unternehmen und deren Wahrnehmung in der Öffentlichkeit. Ein verantwortungsbewusstes IT-Management stellt demnach insbesondere im Zeitalter des Outsourcing von Diensten und Datenbestände einen essentiellen Bestandteil einer sicheren und versicherbaren Unternehmensstrategie dar. Ist die unternehmerische Entscheidung hierzu getroffen, bedarf es der Festlegung der rechtlich und technisch-organisatorisch geeigneten Lokation für den Datenhafen. Eine Datenübertragung nach Island wäre hiernach unbedenklich. Sie ist nicht weitergehend als für den Fall inländischer Datenübertragungen erforderlich. Unabdingbar bleibt freilich die Prüfung der besonderen Zuverlässigkeit des Rechenzentrumsanbieters.

*Autor: Dr. jur. Jens Bücking

Der Autor ist Rechtsanwalt und Fachanwalt für IT¬-Recht. Er ist darüber hinaus Gründungspartner der Rechtsanwaltskanzlei e/s/b Rechtsanwälte (http://www.kanzlei.de) sowie zugleich Fachbuchautor im IT¬-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart und als associate Professor an der E.N.U. in Kerkrade, Niederlande tätig.

Herr Dr. Bücking berät Industrie, Handel und öffentliche Verwaltung bei IT-¬Projekten. Er leistet hier zugleich Unterstützung bei der Schulung der Mitarbeiter und sämtlichen arbeitsrechtlichen Vertragsgestaltungen im IT- ¬und User-¬Umfeld.

***** Disclaimer***

Dieses Dokument stellt einen generellen Leitfaden dar. Es ersetzt nicht die verbindliche Rechtsauskunft durch einen spezialisierten Anwalt. Bitte haben Sie Verständnis, dass trotz Sorgfalt bei der Erstellung eine Garantie oder Haftung für die inhaltliche Richtigkeit nicht übernommen wird. Grundsätzlich ist jedem Unternehmen anzuraten, sich bei informations- oder datenschutzrechtlichen Fragen vor jeglicher Implementierung individuell rechtlich beraten zu lassen.

Über Verne Global

Verne Global entwickelt die erste klimaneutrale Rechenzentrumsanlage der gesamten Rechenzentrumsbranche. Das Ziel von Verne ist es, Rechenzentren in geografisch optimalen Lagen zu betreiben, die Unternehmen niedrige Gesamtbetriebskosten bieten und es erlauben, regenerative Energien kostenneutral einzusetzen. Aktuell errichtet Verne Global einen rund 178.000 m² großen Rechenzentrums-Campus auf dem Gelände des ehemaligen NATO-Kommandozentrums in Keflavik auf Island. Aufgrund der günstigen Bedingungen in Island mit seinen umfangreichen regenerativen Energieressourcen ist Verne Global in der Lage, für Kunden allein bis zu 100 Millionen US-Dollar Energiekosten innerhalb eines Zeitraums von zehn Jahren einzusparen. Für weitere Informationen zum Unternehmen: www.verneglobal.com.