heise Business Services

Ein eBook von

Powered by TechData Advanced Solutions

Handeln statt DSGVO-Panik

Mit einfachen Ansätzen den Datenbestand auf die Datenschutzgrundverordnung vorbereiten

Whitepaper

Objektspeicher als Basis DSGVO-konformer Speicherung für alle Daten...

Fallstudie

Datenschutz wird Pflicht

Prozesse für mehr Privatsphäre

Weniger ist mehr

Savapanf Photo / Fotolia.de

Editorial

Katharina Friedmann

Am 25. Mai 2018 ist es soweit: Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union tritt endgültig in Kraft. Für alle Unternehmen, die personenbezogene Daten von EU-Bürgern speichern und verarbeiten, heißt es nun tatsächlich: Gas geben bei der Umsetzung!

Sinnvoller als angesichts der auslaufenden Schonfrist in Panik auszubrechen, dürfte allerdings sein, nicht nur die bei Verstößen drohenden Strafen im Blick zu haben, sondern sich auch die Chancen vor Augen zu führen, die die neue Datenschutzverordnung birgt: So schafft die DSGVO Klarheit, indem sie den bisherigen Wirrwarr nationaler Datenschutzgesetze in der Europäischen Union ablöst und vereinheitlicht. Unternehmen können sich damit also künftig auf einen einheitlichen Rechtsrahmen stützen.

Gleichzeitig bietet das Inkrafttreten der EU-Verordnung Unternehmen den perfekten Anlass, die eigenen Geschäftsprozesse und die sie stützende IT-Infrastruktur grundsätzlich unter die Lupe zu nehmen – denn die Annahme, alle DSGVO-Anforderungen mit punktuellen technologischen Maßnahmen oder Nachrüstungen erfüllen zu können, ist eine Illusion...

In diesem eBook vermitteln wir Ihnen die wichtigsten Eckdaten der DSGVO, wir erläutern die Auswirkungen der neuen EU-Vorgaben auf organisatorischer und technischer Ebene sowie auf die Unternehmenskultur – und beschreiben, wie die passende IT-Infrastruktur die DSGVO-Compliance erheblich erleichtert.

Katharina Friedmann
Manager Solutions & Services, Heise Medien

© 2018 Heise Medien

Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10a
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

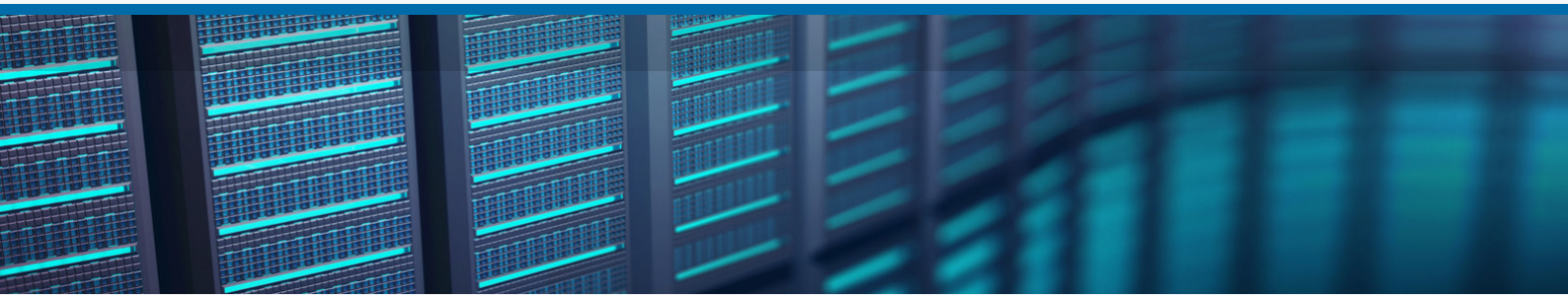
Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Frank Klinkenberg, fkl@heise.de

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de



Inhalt

Datenschutz wird Pflicht 4
Umsetzung dauert mindestens ein Jahr 5
Personenbezogene Daten im Fokus 6
Meldepflicht innerhalb von 72 Stunden 6
Strafen sollen abschrecken 7

Prozesse für mehr Privatsphäre 8
Sechs Schritte zur DSGVO-Compliance 9
Datenschutz wird Dauerthema 10
Alle sind in der Pflicht 11
Datenschutz gibt's nicht kostenlos 11

Weniger ist mehr 12
Automatisierte Prozesse 12
Register für personenbezogene Daten 13
Zentral verwalten, verteilt speichern 13
Speicher mit Spareffekt 14

Whitepaper
Objektspeicher als Basis DSGVO-konformer Speicherung für alle Daten 15

Fallstudie
Ein digitaler Tresor für optimierte Compliance-Prozesse anstelle statischer Datensilos – wie Datenkonsolidierung und -suche zur Leichtigkeit wird 16

ÜBER DEN AUTOR

Bernd Müller ist Journalist für Technologie und Wissenschaft in Bonn. Er war Redakteur bei Bild der Wissenschaft und der Wirtschaftswoche sowie PR-Referent bei der Fraunhofer-Gesellschaft. Seit vielen Jahren schreibt er für Verlage und Unternehmen zu Innovationsthemen, außerdem forscht und lehrt er zum Thema Wissenschaftskommunikation.

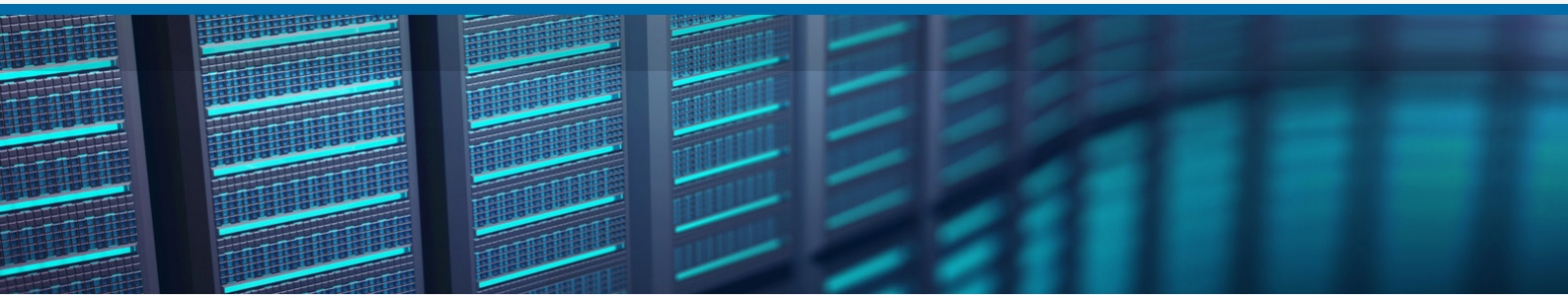
Datenschutz wird Pflicht

Foto: StillFx / Fotolia.de

Am 25. Mai 2018 tritt die neue Datenschutzgrundverordnung (DSGVO) in Kraft. Unternehmen müssen sich mit der Umsetzung beeilen – bei Nichteinhaltung der Frist drohen saftige Strafen. Doch wer rechtzeitig handelt und die Regeln ernst nimmt, hat wenig zu befürchten.

Datenschutz. Allein der Begriff löst bei vielen ein ungutes Gefühl in der Bauchgegend aus – bei Kunden und Bürgern, weil sie nicht erst seit den Enthüllungen von Edward Snowden den Verdacht haben, dass mit ihren Daten Schindluder getrieben wird, und bei Unternehmen, weil sie ständig auf der Hut sein müssen, keine Daten zu verlieren oder gegen gesetzliche Auflagen zu verstoßen. Eine Mitschuld an dieser Situation hat der Gesetzgeber: Die Datenschutzrichtlinien stammen aus den 1990ern, in Deutschland konkret von 1995. Und selbst wer hierzulande alles richtig macht, kann in einem anderen EU-Land unwissentlich in ein juristisches Fettnäpfchen treten.

Insofern ist es eine gute Nachricht, dass die Europäische Union nun endlich Klarheit schafft. Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in Kraft, die das Sammelsurium nationaler Gesetze in der Europäischen Union ersetzt und vereinheitlicht. Für die Unternehmen heißt das: Sie müssen sich nicht mehr durch 28 nationale Gesetze wühlen, sondern können auf einen einheitlichen Rechtsrahmen vertrauen. Damit spart die Wirtschaft in Europa laut Vorhersagen rund 2,3 Milliarden Euro pro Jahr. Doch es gibt auch eine nicht so gute Nachricht: Bei Verstößen drohen saftige Bußgelder. Sie sollen ausdrücklich abschreckenden Charakter haben. Das hat in der medialen Berichterstattung über die DSGVO zu teilweise apokalyptischen Prognosen geführt; spekuliert wird über Pleiten von Unternehmen, die sich nicht an die Regeln halten.

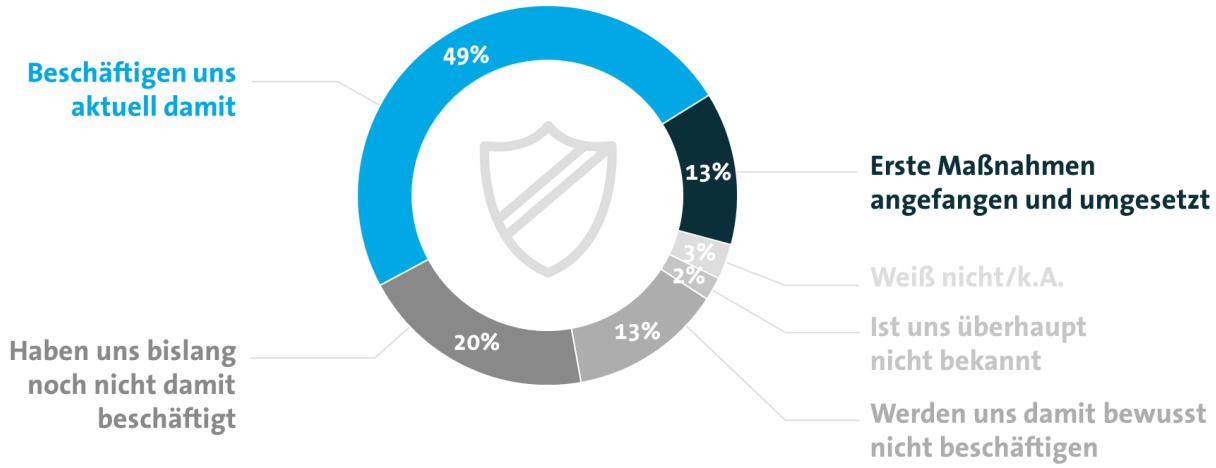


Umsetzung dauert mindestens ein Jahr

Auch wenn solche Szenarien im Prinzip möglich sind, so können Unternehmen doch einiges tun, damit es nicht so weit kommt – wenn sie rechtzeitig damit beginnen, die neuen Anforderungen umzusetzen. Doch daran hapert es leider – selbst in Deutschland, wo der Datenschutz traditionell einen höheren Stellenwert genießt als in anderen Ländern. Laut einer Studie des IT-Verbands Bitkom vom September 2017 haben nur drei Prozent der 500 befragten Unternehmen bereits mehr als die Hälfte der DSGVO-Vorgaben umgesetzt, und jedes dritte Unternehmen hat sich noch gar nicht mit der Verordnung beschäftigt. Das ist deshalb bedenklich, weil der Verband für dieses Vorhaben bei einem kleineren Mittelständler rund ein Jahr für die Umsetzung veranschlagt.

Jedes dritte Unternehmen ignoriert bislang die DS-GVO

Wie weit ist Ihr Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) zum aktuellen Zeitpunkt?



Basis: Unternehmen ab 20 Mitarbeitern (n=507) | Quelle: Bitkom Research

bitkom

Nur etwa die Hälfte der befragten Unternehmen gibt an, sich mit der neuen Datenschutzverordnung auseinandersetzen – und nur ein Bruchteil hat bereits begonnen, erste Maßnahmen umzusetzen. (Quelle: Bitkom)

> Unternehmen müssen sich nicht mehr durch 28 nationale Gesetze wühlen, sondern können auf einen einheitlichen Rechtsrahmen vertrauen.

> Der Schutz personenbezogener Daten ist nicht nur eine digitale Herausforderung.

Es ist also Zeit zu handeln. Doch statt in Panik zu verfallen, sollten sich Unternehmen erst einmal klarmachen, von welchen Daten in der DSGVO überhaupt die Rede ist:

„… alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind."

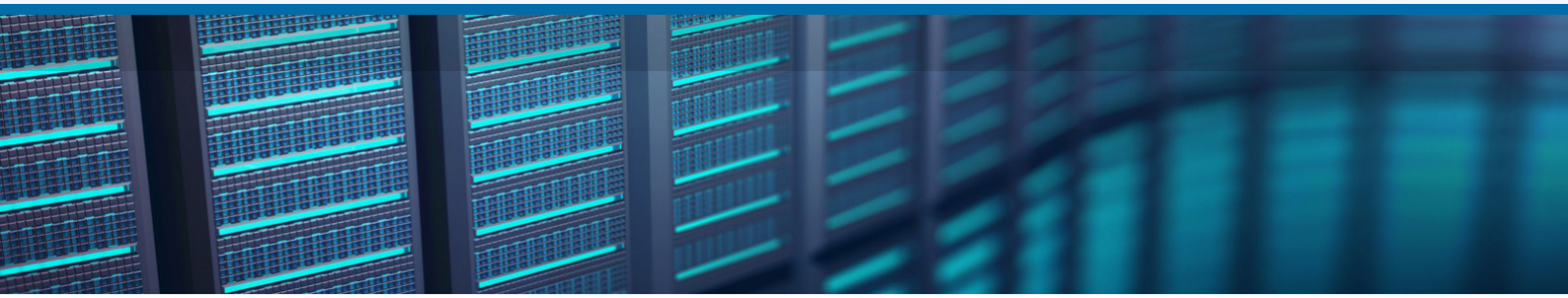
Personenbezogene Daten im Fokus

Daraus folgt: Verliert ein Ingenieur sein Notebook, auf dem Konstruktions- oder Businesspläne gespeichert sind, ist das ärgerlich und möglicherweise existenzbedrohend, es fällt aber nicht unter die DSGVO. Befinden sich auf dem Notebook aber Informationen über Geschäftspartner wie Name, Adresse, Passwörter, E-Mails oder Kreditkarteninformationen greift die neue Regelung. Daneben gibt es viele weitere Daten, die zu schützen sind – darunter Fotos und Videos, Patientenakten oder IP-Adressen von Computern. Mit dieser weitgehenden Interpretation möchte die EU den Datenschutz fit machen für die digitale Welt mit Google, Facebook und Co. Doch Vorsicht: Der Schutz personenbezogener Daten ist nicht allein eine digitale Herausforderung. Ein nicht abgeschlossener Aktenschrank mit Röntgenbildern auf dem Flur einer Arztpraxis ist ebenfalls ein Risiko im Sinne der DSGVO.

Meldepflicht innerhalb von 72 Stunden

Es gibt noch zahlreiche weitere Pflichten und Regeln für Unternehmen, hier die wichtigsten: Kommt es zu einem Verstoß gegen den Datenschutz, hat das Unternehmen zwei Meldepflichten: gegenüber der Aufsichtsbehörde und gegenüber den betroffenen Personen. Die Aufsichtsbehörde ist bei jeglicher Verletzung personenbezogener Daten zu informieren, sofern diese zu einem Risiko für Recht und Freiheiten der Personen führt. Die Meldung muss innerhalb von 72 Stunden erfolgen – dauert es länger, muss dies begründet werden.

Die Meldepflicht „in klarer und einfacher Sprache" gegenüber den betroffenen Personen ist weniger streng geregelt. Sie gilt, wenn ein „hohes Risiko für die persönlichen Rechte und Freiheiten" dieser Personen besteht. Sie kann aber



unterbleiben, wenn diesem Risiko durch organisatorische und technische Maßnahmen bereits vor der Panne entgegengewirkt wurde. Geht zum Beispiel ein Datenträger mit personenbezogenen Daten verloren, müssen die betroffenen Personen nicht benachrichtigt werden, wenn das Speichermedium ausreichend verschlüsselt ist. Die Meldepflicht gegenüber der Aufsichtsbehörde besteht allerdings auch in diesem Fall. Darüber hinaus hat jeder Bürger das Recht zu erfahren, welche Daten über ihn gespeichert sind. Diese Auskunft muss das Unternehmen zügig liefern, auch wenn es von Anfragen überrollt wird.

Die Regelungen der DSGVO gelten auch für Unternehmen, die keine Niederlassung in der EU haben, sofern sie EU-Bürgern Waren und Dienstleistungen (auch kostenfreie) anbieten oder deren Verhalten überwachen. Sowohl der Ort, an dem die betroffene Person lebt, als auch der Ort, wo die Daten verarbeitet werden, sind hier relevant. Der Teufel steckt im Detail: Ein nicht-europäisches Unternehmen fällt schon dann unter die DSGVO, wenn es nur Cookies im Webbrowser eines EU-Bürgers setzt und daraus Daten abfragt.

Strafen sollen abschrecken

Bei Verstößen drohen Unternehmen Geldstrafen vonseiten der Behörden. Diese können bis zu 20 Millionen Euro betragen oder vier Prozent des weltweiten Jahresumsatzes eines Unternehmens ausmachen – je nachdem, welcher Wert höher ist. Zwingend sind die Bußgelder allerdings nicht, sie sollen dem Einzelfall angemessen sowie verhältnismäßig sein und sich nach der Art, Schwere und Dauer des Vorfalls bemessen. Eine abschreckende Wirkung ist aber ausdrücklich vorgesehen. Die DSGVO enthält erstmals recht konkrete Regelungen und Hinweise zum technischen Umgang mit Datenschutz. Dieser soll bereits frühzeitig in die Entwicklung von Erzeugnissen und Dienstleistungen integriert werden. Datenschutzfreundliche Voreinstellungen werden beispielsweise in sozialen Netzwerken oder mobilen Apps zur Norm.

> Für den Bürger die vielleicht wichtigste Neuerung: das Recht auf Vergessen.

Für den Bürger die vielleicht wichtigste Verbesserung ist das Recht auf Vergessen. Wenn dieser es wünscht, muss die Organisation, die Daten über ihn gespeichert hat, diese unwiederbringlich löschen. In bestimmten Fällen, etwa bei abgelehnten Bewerbungsunterlagen, geht das Gesetz noch weiter: Diese Daten sind auch ohne Aufforderung auf jeden Fall zu vernichten. ■

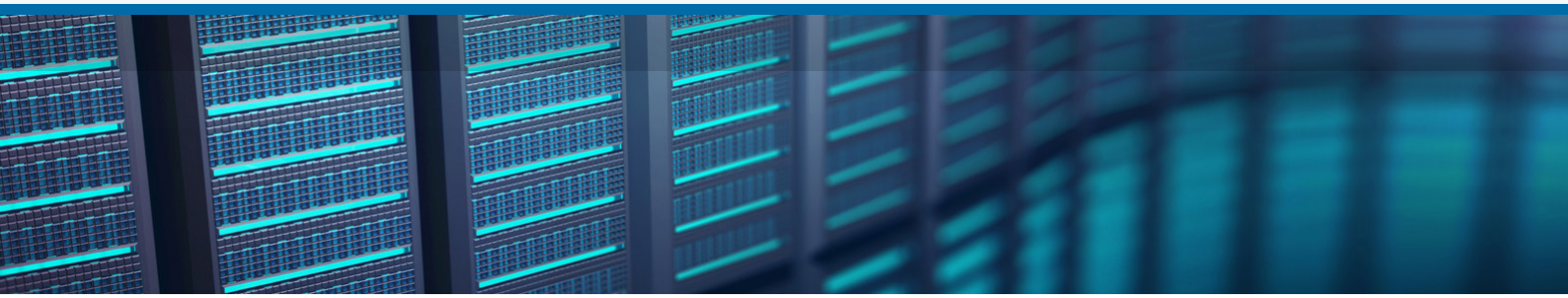
Prozesse für mehr Privatsphäre

Die DSGVO stellt hohe Anforderungen an den Datenschutz. Um sie zu erfüllen, müssen Unternehmen ihre Prozesse auf den Prüfstand stellen – und einen Kulturwandel einleiten.

Die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft tritt, sorgt derzeit in Unternehmen und Organisationen für hektische Betriebsamkeit. Und doch gibt es immer noch Akteure, die die Umsetzung vor sich herschieben oder sich zumindest schwer damit tun. Das liegt nicht nur am umfangreichen Gesetzestext, sondern auch an der Tatsache, dass die DSGVO tief in die Geschäftsprozesse eingreift. Während Unternehmen bisher weitgehend nach Gutdünken Daten sammeln und verarbeiten durften und selbst bei Verlust von personenbezogenen Informationen keine größeren Sanktionen zu befürchten hatten, zieht das neue Gesetz die Zügel merklich an.

Im Kern geht es in der DSGVO um folgende Leitlinien:

- Rechtstreue, Transparenz und Fairness
- Begrenzte Verwendung von Daten
- Minimierung von Daten
- Beschränkung der Speicherung
- Geheimhaltung und Integrität
- Haftung



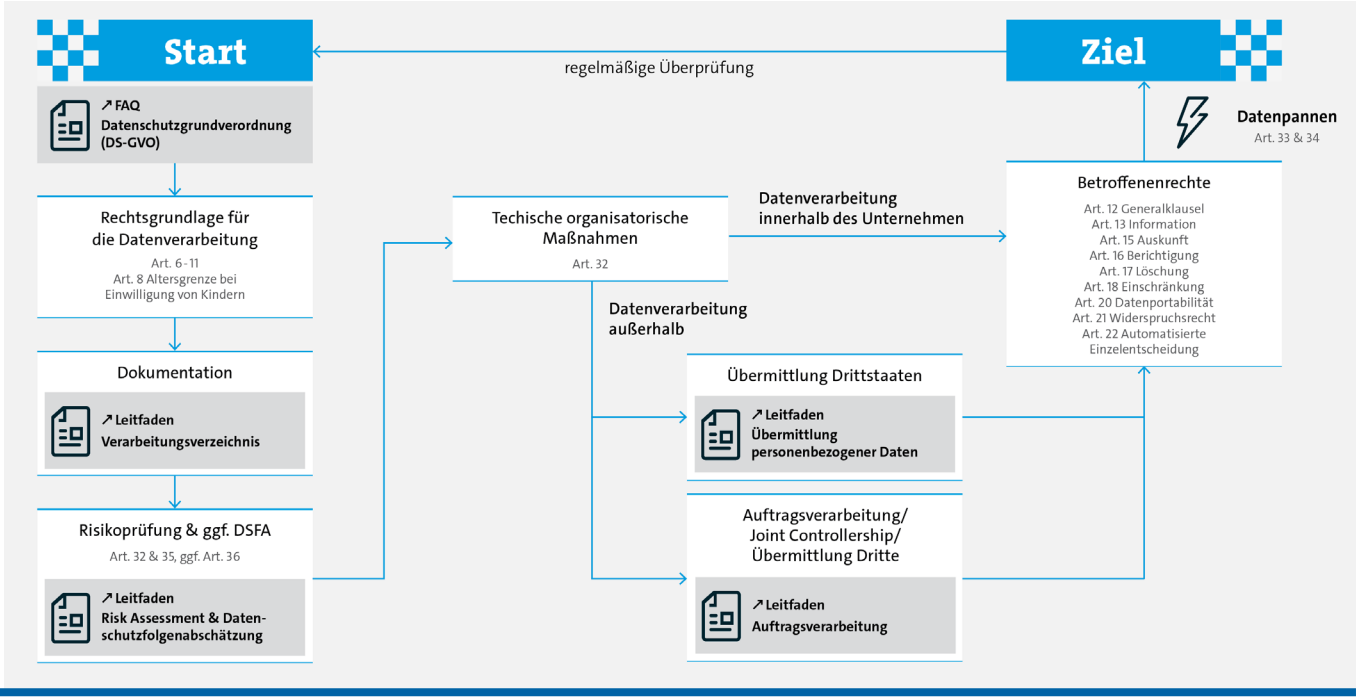
> Die DSGVO greift tief in die Geschäftsprozesse ein.

Sechs Schritte zur DSGVO-Compliance

Was es genau mit diesen Prinzipien auf sich hat, steht im Gesetz. Es ist aber nützlich, sich diese einfachen Leitlinien immer wieder in Erinnerung zu rufen, wenn man datenschutzrechtliche Anpassungen plant. Um sich für die DSGVO zu rüsten, empfiehlt sich ein mehrstufiges Vorgehen.

1. **Vorbereitungen:** Das Management sollte sich über die DSGVO informieren und externe Beratung hinzuziehen. Es ist empfehlenswert, schon zu diesem Zeitpunkt einen Datenschutzverantwortlichen einzustellen.
2. **Risikoanalyse:** In dieser Phase analysiert das Unternehmen, welche Datenschutzmaßnahmen bereits umgesetzt sind und wo die größten Lücken sind.
3. **Priorisierung:** Aus der Risikoanalyse folgt, welche Maßnahmen am dringlichsten sind und wie Mittel eingesetzt werden, um diese Lücken zu schließen.
4. **Risiken beheben:** Riskante „Altlasten" im Datenschutz werden beseitigt.
5. **Abschluss der Vorbereitung:** Bis zum 25. Mai 2018 sollten die größten Risiken beseitigt und alle notwendigen Datenschutzmaßnahmen umgesetzt sein.
6. **Laufender Betrieb:** Nach dem 25. Mai 2018 erfolgen die Verwaltung persönlicher Daten nach den Vorgaben der DSGVO und das laufende Nachjustieren bei Lücken.

Für die Vorbereitung, also die ersten fünf Schritte, kalkulieren Experten rund 15 Monate ein. Unternehmen, die sich bisher noch gar nicht mit der DSGVO befasst haben, sind also eigentlich zu spät dran. Das heißt natürlich nicht, dass sie nun aufgeben und sich zurücklehnen sollten – im Gegenteil: Jetzt sind erhöhte Anstrengungen nötig, um den Rückstand aufzuholen, indem die oben genannten Schritte – wo möglich – parallel angegangen werden.

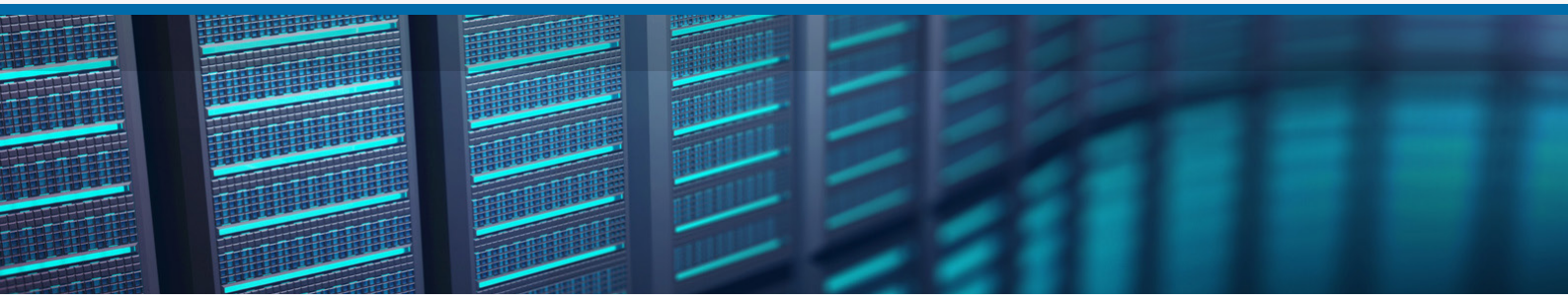


Datenschutzkonforme Datenverarbeitung nach der EU-DSGVO (Quelle: Bitkom)

Datenschutz wird Dauerthema

Unternehmen müssen sich darüber im Klaren sein, dass die Arbeiten zur DS-GVO mit dem 25. Mai 2018 nicht ein für alle Mal abgeschlossen sind. Vielmehr erfordert Datenschutz stetige Anstrengung. Diese umfasst und verzahnt immer Personen, Prozesse und Technologie zugleich – man kann also nicht einfach eine Software kaufen, die alles regelt. So unterliegt der Umgang mit Daten ständigen Veränderungen. Welche Daten werden gesammelt und wo und wie lange werden sie gespeichert? Warum werden sie gesammelt? Wer hat Zugriff? Diese Fragen sind laufend zu beantworten. Mitunter ist das gar nicht so einfach. Bei einem Customer Relationship Management (CRM) sind Art und Zweck der Datensammelei naheliegend. Nicht so offensichtlich ist es, wenn es um biometrische Daten wie Fingerabdrücke oder Spracherkennung geht. Und Arztpraxen sollten sich im Klaren sein, dass auch Röntgenbilder unter die DSGVO fallen.

Die DSGVO fordert „Privacy by Design“ – Datenschutz beziehungsweise Schutz der Privatsphäre ist nicht länger eine lästige Pflicht, mit dem Unternehmen mal mehr, mal weniger freigiebig sein können. Der Schutz persönlicher Daten wird



vielmehr Teil aller Innovationen, Produkte, Prozesse und Verträge. Für viele Unternehmen erfordert das ein Umdenken, geradezu einen Kulturwandel – und das nicht nur für die eigene Organisation, sondern auch für Dienstleister, die mit den Daten arbeiten, wie Cloud-Anbieter oder freie Vertriebsmitarbeiter. Sicherstellen lässt sich das durch regelmäßige Audits dieser Dienstleister, bei der die Einhaltung der DSGVO geprüft wird.

> Um sich für die DSGVO zu rüsten, empfiehlt sich ein mehrstufiges Vorgehen.

Alle sind in der Pflicht

In Schritt 1 wurde empfohlen, einen Datenschutzmanager einzustellen. Der Begriff Datenschutzbeauftragter, wie es ihn etwa in Landes- und Bundesbehörden gibt, sei hier bewusst vermieden, denn diese Personen treten in der Regel erst in Aktion, wenn es zu einem datenschutzrelevanten Vorfall größeren Ausmaßes gekommen ist. Hier ist etwas anderes gemeint: Ein Datenschutzmanager, im Englischen Data Protection Officer (DPO) genannt, kümmert sich laufend um die Einhaltung und Verbesserung der Datenschutzrichtlinien; er sollte gleichberechtigt neben anderen Personen im Management stehen. Doch Vorsicht: So wie ein Innovationsmanager nicht allein für alle Innovationen in einem Unternehmen sorgen kann, kann auch ein Datenschutzmanager nicht allein den Datenschutz sicherstellen. „Für Datenschutz ist bei uns Herr Meyer zuständig" – so eine Denkweise ist riskant, weil sie die Verantwortung der restlichen Belegschaft außer Acht lässt. Aus Sicht der DSGVO ist es zum Beispiel nicht ratsam, Mails oder andere personenbezogene Informationen lokal auf dem Notebook zu speichern. Mitarbeiter müssen hier umdenken.

> Die DSGVO fordert „Privacy by Design".

Datenschutz gibt's nicht kostenlos

Ein Unternehmen, das die DSGVO umsetzen möchte, tut also gut daran, ein schlagkräftiges Team zu bilden. Zu diesem gehören neben dem DPO auch Vertreter der Abteilungen Recht, Personal, Vertrieb, Marketing, Beschaffung sowie weiterer Abteilungen, die in irgendeiner Weise mit personenbezogenen Daten umgehen. Wie bei vielen Veränderungsprozessen kommt auch hier dem Management eine entscheidende Bedeutung zu. Vorstand beziehungsweise Geschäftsführung sollten das Thema DSGVO nicht nach unten wegdelegieren, sondern eine aktive Rolle in der Umsetzung spielen. Das hilft zudem, die erforderlichen Mittel bereitzustellen, denn wie bei jedem Veränderungsprogramm gilt: Auch die Umsetzung und das Aufrechterhalten der DSGVO-Compliance kosten Geld – allerdings weniger als eine Strafe bei einem schweren Datenschutzleck. ■

Weniger ist mehr

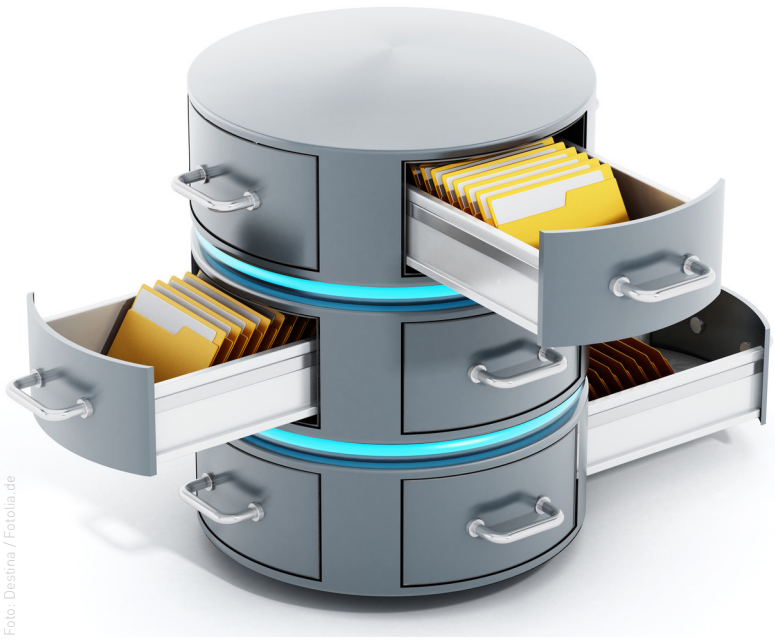


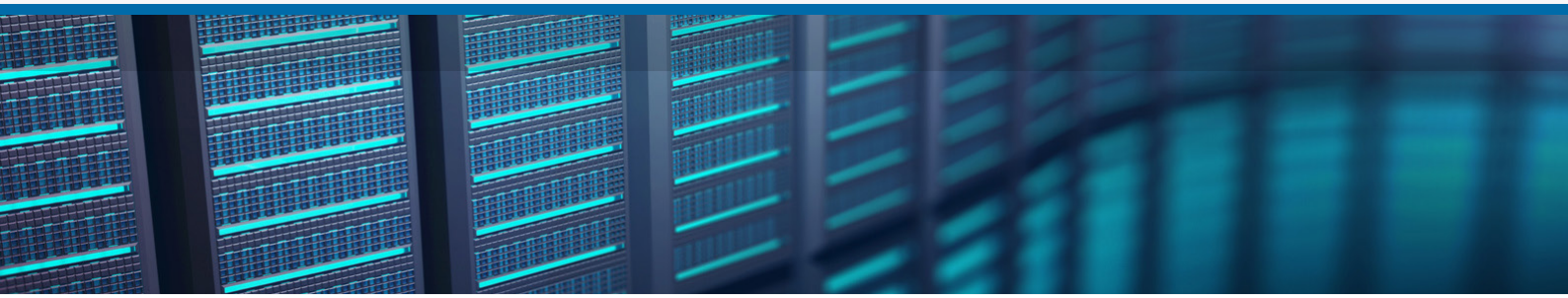
Foto: Destina / Fotolia.de

Wer die Datenschutz-Grundverordnung (DSGVO) souverän erfüllen möchte, braucht eine IT-Infrastruktur, die ihm die Arbeit erleichtert. Wohl dem, der seine Daten auf Objektspeichern lagert.

Das papierlose Büro? Ein Klassiker aus der Reihe von Technologien, die nie oder viel später kamen als gedacht. In vielen, vor allem kleinen und mittleren Unternehmen werden immer noch Informationen auf Papier dokumentiert, manchmal auch mit kuriosen Medienbrüchen wie der Excel-Tabelle, die ausgedruckt und in einem Hängeregister im Schrank abgelegt wird. Mit der Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft tritt, kommt nun Bewegung auch in diese Unternehmen. Sie müssen sicherstellen, dass personenbezogene Daten – Adressen, Passwörter, Fingerabdrücke, Steuerbescheide und vieles mehr – nicht in falsche Hände geraten. Die Datenhaltung auf Papier schließt das neue Gesetz zwar nicht aus, doch es empfiehlt digitale Technologien, um die Anforderungen zu erfüllen. Das ergibt Sinn, denn Unternehmen müssen künftig immer wissen und bei einem datenschutzrechtlichen Vorfall nachweisen, wer wo wann auf welche Daten zugreift, und das geht digital nun mal viel einfacher. Die DSGVO könnte also endgültig das Totenglöckchen des Papierbüros läuten.

Automatisierte Prozesse

Neben der Technologie sind die Prozesse und das Verhalten von Personen ebenso wichtige Säulen bei der Umsetzung der DSGVO. Doch bestimmte Anforderungen des neuen Gesetzes lassen sich nicht mehr händisch erledigen, sie erfordern automatisierte Prozesse:



Neben der Technologie sind Prozesse und Verhalten wichtige Säulen bei der Umsetzung der DSGVO.

- Automatisierung des Registers persönlicher Daten
- Automatisierung der Einverständniserklärung von Kunden zur Verarbeitung ihrer Daten
- Reporting der Einhaltung der Regeln
- Automatisierung von Datenanfragen
- Automatisierte Erkennung von Datenschutzverletzungen
- Schutzmaßnahmen für Daten und Netzwerk

Die Liste deutet schon an, dass es nicht die eine technologische Maßnahme gibt, mit der sich alle Anforderungen auf einmal erledigen lassen. Wahrscheinlicher ist, dass viele Unternehmen mit ihrer bestehenden IT-Infrastruktur gleich mehrere dieser Punkte nicht erfüllen können, auch nicht durch Nachrüsten einzelner Hard- und Software. Das Inkrafttreten der DSGVO ist daher ein idealer Zeitpunkt, alle Geschäftsprozesse und die damit verknüpfte IT-Infrastruktur auf den Prüfstand zu stellen.

Register für personenbezogene Daten

So ist es empfehlenswert, ein Register (siehe erster Punkt in der Liste) anzulegen, das automatisch protokolliert, wo personenbezogene Daten im Unternehmen verteilt sind, wie sie verarbeitet werden sowie durch wen und zu welchem Zweck. So ist es möglich, den Überblick zu behalten, wenn sich Prozesse ändern, etwa wenn Daten von einer Inhouse-Lösung zu einem Cloud-Dienstleister verlagert werden. Was tun, wenn personenbezogene Daten weltweit auf verschiedenen IT-Systemen verteilt sind? Die Anforderungen der DSGVO lassen sich nur dann sinnvoll automatisieren, wenn stets bekannt ist, wo bestimmte Daten liegen beziehungsweise wie sie leicht zu finden sind. Hier kommt der sogenannte Objektspeicher ins Spiel. Ein Objekt ist eine Datei, die mit Metadaten verknüpft ist. Jedes Objekt hat eine ID, die aus Inhalt und Metadaten berechnet wird. Eine Anwendung greift auf das Objekt zu, indem es dem Speicher die ID übergibt – nicht indem es sich einen Dateipfad entlanghangelt wie in herkömmlichen Dateisystemen. Vielmehr liegen hier alle Objekte auf einer Ebene.

Das Inkrafttreten der DSGVO ist ein idealer Zeitpunkt, Geschäftsprozesse und die damit verknüpfte IT-Infrastruktur auf den Prüfstand zu stellen.

Zentral verwalten, verteilt speichern

Objektspeicher haben viele Vorteile. So ist es völlig egal, ob die Daten in einem lokalen NAS-System oder in einer öffentlichen Cloud oder einem Mix gespeichert sind. Metadaten und die dazu gehörenden Objekte können sogar an verschiedenen Orten liegen. Anwendungen und mobile Apps können die schlanken

Metadaten auf lokalen Speichern schnell durchsuchen und dann die Objekte auf anderen Speichern ansprechen. So lassen sich Daten zentral verwalten, auch wenn sie gar nicht an einem gemeinsamen Ort liegen. Was in den Metadaten zu stehen hat, muss nicht von vornherein definiert sein. Jedem Objekt lassen sich beliebige Metadaten hinzufügen, etwa welche Sicherheitslevel für dieses Objekt gelten und wann es gelöscht werden soll.

Bei größeren Datenbeständen sind Objektspeicher ohnehin überlegen. Mit der DSGVO gibt es noch ein paar Argumente mehr. So fordert das Gesetz unter anderem ein Recht auf Auskunft und auf Vergessen. Möchte ein Kunde wissen, welche Daten über ihn vorhanden sind, und diese löschen lassen, muss dies umgehend und vollständig geschehen. Das gelingt jedoch nur, wenn die Daten auch alle auffindbar sind, was bei herkömmlichen Dateisystemen ziemlich knifflig werden kann. Bei Objektspeichern hingegen lassen sich alle Einträge, die zu einer Person gehören, über die Metadaten leicht per Knopfdruck einsammeln. Das oben erwähnte Register für personenbezogene Daten lässt sich aus Metadaten viel leichter automatisch erstellen und führen, auch wenn die Kundenbasis rasant wächst, denn Objektspeicher ist mühelos nahezu unendlich skalierbar. Zudem erfüllen Objektspeicher die Forderung der DSGVO nach einer Minimierung von Daten.

> IDC geht davon aus, dass der Markt für Objektspeicher jährlich um gut 30 Prozent auf knapp 20 Milliarden Dollar im Jahr 2020 anwächst.

Speicher mit Spareffekt

Ein angenehmer Nebeneffekt: Objektspeicher spart Softwarelizenzen. Beispiel Salesforce: Je nach Art der Lizenz gibt es Beschränkungen bei der Speicherzuweisung pro Benutzerlizenz. Werden lediglich Metadaten auf die Salesforce-Speicher und der große Objektspeicher in eine andere Cloud ausgelagert, kommt man sehr viel länger mit einer günstigeren Lizenz mit beschränkter Speicherzuweisung aus.

Die Analysten von IDC gehen davon aus, dass der Markt für Objektspeicher jährlich um gut 30 Prozent wächst und im Jahr 2020 knapp 20 Milliarden Dollar erreicht – Objektspeicher bei Cloud-Dienstleistern sind hier noch gar nicht enthalten. Und Gartner prognostiziert, dass 2019 mehr als 30 Prozent der weltweiten Speicherkapazität auf sogenannten Software-defined Storage entfällt, also auf Speicher, bei dem das Management des Speichers von der Hardware getrennt ist. Mit der DSGVO dürfte die Beliebtheit von Objektspeichern noch zusätzlich wachsen. ■

Tech Data
Advanced Solutions

Objektspeicher als Basis DSGVO-konformer Speicherung für alle Daten

Als einfache Antwort auf die Herausforderungen der EU-Datenschutzgrundverordnung stellt Hitachi Vantara mit der Hitachi Content Platform (HCP) eine Objektspeicherplattform bereit, die es IT-Organisationen und Cloud-Service-Anbietern ermöglicht, File-Daten in einem einzigen System zu speichern, zu teilen, zu synchronisieren, zu schützen, aufzubewahren, zu analysieren und abzurufen. Dabei ermöglicht die HCP, Daten richtlinienbasiert und automatisch in bevorzugte Clouds – public und/oder private – zu verschieben, und dabei jederzeit Kontrolle und Transparenz aufrecht zu erhalten, da die Metadaten sicher vor Ort gespeichert werden. HCP automatisiert alltägliche IT-Aufgaben wie die Datensicherheit und passt sich im Verlauf des Lebenszyklus der Daten an die vorgenommenen Änderungen hinsichtlich Skalierung, Umfang, Anwendungen, Speicher und Servertechnologien an. In IT-Umgebungen, in denen Daten schnell wachsen oder über Jahre aufbewahrt werden müssen, sind diese Funktionen von unschätzbarem Wert. HCP liefert hier die Lösung - skalierbar von 4TB bis 600PB.

Mit erneutem Blick auf die EU-Datenschutzgrundverordnung zeigt sich ein Datenschutzproblem, dass alle Firmen betrifft: Der Umgang mit Emails und Kommunikationsdaten. Hierbei ist nicht nur das Problem privater Emails gemeint, denn auch geschäftliche Emails können Informationen enthalten, die unter die Datenschutzgrundverordnung fallen: Bewerbungsschreiben, Hotelbuchungen mit den Pass- und Kreditkartennummern der Mitarbeiter, Krankmeldungen an die Personalabteilung oder aber auch personenbezogene Daten über Kunden und Interessenten.

Die Möglichkeit, Emails zu kategorisieren und in den Mailinhalten und Anhängen zu suchen wird heute häufig durch den Mail-Server oder eine spezielle Archivsoftware realisiert. Solche Lösungen skalieren meist schlecht, sind teuer im Unterhalt und lösen das Problem nur für ein einziges Anwendungsgebiet, nicht aber für beispielsweise Instant Messaging, Voice oder Papierdokumente.

Die folgende Fallstudie einer großen europäischen Bank zeigt auf, wie durch die Hitachi Content Platform eine DSGVO-konforme Managementplattform für sämtliche Kommunikationsdaten realisiert wurde, die nicht nur Emails aus 5 Ländern und mehreren Konzerntöchtern, sondern auch Sprachnachrichten, Skype/Lync, Trader-Chatrooms und Papierdokumente zentral verwaltet.

Mit der optionalen Hitachi Content Intelligence Such- und Kategorisierungslösung wurde hier ein „Digitaler Tresor“ für sämtliche Dokumentarten geschaffen, der es möglich machte, mehrere Silo-Lösungen, 20 Server und 7 Datenbankinstanzen einzusparen und dadurch eine Amortisierung innerhalb von 12 Monaten zu erzielen.

Das beschriebene System wurde ohne großen Aufwand im Rahmen eines DSGVO Projektes an die Anforderungen des Datenschutzbeauftragten angepasst und um ein Regelwerk zum Umgang mit privaten Daten ergänzt.

Wenn Sie mehr über die Hitachi Content Platform und ihre Anwendungsmöglichkeiten erfahren wollen, besuchen Sie unsere Informationsseite **„Der Umstieg in die Cloud“**. Dort erfahren Sie, warum Objektspeicher von Hitachi optimal zur Lösung unzähliger Herausforderungen in der Unternehmens-IT ist, wie beispielsweise:

- Erstellung eines sicheren Zugangs zu Cloud-Plattformen (Gateway)
- Metadatengenerierung für IoT und Big Data
- Kostenreduzierung für Archivdaten
- sicheres Filesharing im Unternehmensumfeld
- Zusammenführen unterschiedlicher Speichertechnologien und Systeme in einer Private Cloud

Tech Data AS GmbH, Lötscher Weg 66, D-41334 Nettetal

Fallstudie: Ein digitaler Tresor für optimierte Complianceprozesse anstelle statischer Datensilos – Wie Datenkonsolidierung und -suche zur Leichtigkeit wird.

„Die Hitachi Content Platform hat die Art, wie wir Ermittlungen in digitalen Daten (e-Discovery) durchführen, maßgeblich revolutioniert. Die Zeit zum Auffinden von Informationen kann von mehreren Wochen auf wenige Stunden reduziert werden“

Hintergrund

Gesetzliche Regulierungen und interne Vorschriften (Compliance) erfordern eine neue Herangehensweise im Umgang mit elektronisch gespeicherten Informationen (ESI). Eine große europäische Bank setzt in diesem Bereich neue Maßstäbe, indem sie die Gesamtdauer des Ermittlungsprozesses von Wochen auf Stunden reduziert – mit der Hitachi Content Platform.

Herausforderung

Compliance Teams die notwendigen Werkzeuge an die Hand zu geben, um effektiver gesetzesbezogene Ermittlungen auf globaler Ebene zu betreiben.

Lösung

Ein „Digitaler Tresor“ für Kommunikationsdaten auf Basis der Hitachi Content Platform, der Daten konsolidiert und durchsuchbar macht, um die vorhandenen Silos zu eliminieren und den Compliance Prozesse zu transformieren.

Ergebnis

Ein vollständig dokumentierter Lebenszyklus der Daten, Kontrolle über die Aufbewahrung und Löschung und Zugriff auf die gesamten weltweiten Kommunikationsdaten. Dadurch erhebliche Verbesserung der Complianceprozesse, bei gleichzeitiger Senkung der IT-Kosten.

Die Herausforderung

Als in der Europäischen Union ansässiges Unternehmen im Bereich Banken und Finanzdienstleistungen bedient der Anwender mehr als 10 Millionen Kunden in 47 Ländern. Mit mehr als 50.000 Mitarbeitern werden Werte von über 650 Milliarden EURO verwaltet.

Alle Unternehmen des Finanzsektors unterliegen einem breiten Spektrum an Regierungsauflagen und Gesetzen in jedem Land, in dem sie Geschäfte durchführen, und diese sind selbst in der Europäischen Union nicht immer einheitlich. Mit der steigenden Zahl von Überprüfungen seit der Finanzkrise 2008 und immer neuen gesetzlichen Vorgaben am Horizont, benötigte die Bank eine Lösung, die zukünftige Compliance-Ermittlungen schnell, flexibel und umfassend durchführbar macht und vor allem auch das Reporting von Verstößen an die Aufsichtsbehörden verbessert.

In der Vergangenheit sammelte die unternehmensinterne IT Kommunikationsdaten unterschiedlichster Quellen in verschieden Ländern. Diese beinhalten sowohl Emails, Aufzeichnungen von Anrufen, Instant Messaging Verläufe und Chat Applikationen, genauso wie Daten der Instant Messenger großer Nachrichtenportale. Dies war ein zeitaufwendiger, ressourcenintensiver und fehleranfälliger Prozess.

Wenn die interne Revision bestimmte Unternehmensaktionen untersuchen musste, sammelte die IT dazu spezifische Informationen aus diesen Quellen - Einige von Drittanbietern, andere von internen Systemen oder Backup-Tapes. Immer wenn eine Untersuchung ihren Fokus oder Umfang änderte, mussten dieselben Systeme und Quellen erneut mit anderen Kriterien durchsucht werden. Das kontinuierliche „Mining“ mehrerer Datenquellen verteilt über separate Silos wurde zu einer zentrale Herausforderung. Der Kunde startete eine Marktanalyse, um einen Weg zu finden, die Kommunikationsdaten sinnvoll zusammenzuführen, um die Arbeit der Compliance Teams flexibler und die Zusammenarbeit mit anderen Unternehmensbereichen einfacher zu machen.

Kundenprofil

Industrie: Finanzdienstleistungen, internationales Finanzinstitut
Lösung: File and Content, Compliance, Business Agility
Hardware: Hitachi Content Platform (Intelligent Extraction, Transformation, Loading and Indexing Capabilities)
Services: Zusätzliche User Interface Entwicklung

Ergebnis

- Ein einziger, zentraler „Digitaler Tresor“ für Kommunikationsdaten aus unterschiedlichsten Quellen
- Einfach zu nutzendes Webinterface für schnelle, einfache und wiederholbare Analysen
- Voll auditierbare, revisionssichere Datenspeicherung über verschiedene Quellen

Die Lösung

Um die Suche und Beschaffung der digitalen Informationen effizienter zu gestalten, sollte eine Lösung implementiert werden, die alle relevanten Daten in einer „Private Cloud“ sammelt und konsolidiert. Durch die Einrichtung eines globalen Datenpools für Mail, Chat, Voice und Social Media kann der Kunde Nachforschungen zentral in einem einzigen System durchführen, auch wenn sich der Umfang der Untersuchung ändern sollte. Darüber hinaus können die Daten rechtlich korrekt verwaltet werden, mit sicherer 2-Faktor Zugriffskontrolle, Audit Trails und automatisierter Löschung anhand vordefinierter Regeln. Die Datenspeicherung auf Objektebene macht es möglich, den gesamten Datenbestand mit der für das betreffende Element gültigen Aufbewahrungsvorschrift zu verwalten.

In einem Projekt der Global Compliance Group hat der Kunde gemeinsam mit Hitachi an der Implementierung einer modernen Ingest-and-Search-Lösung gearbeitet, die auf einer Erweiterung der HCP-Familie beruht: Hitachi Content Intelligence. Diese Lösung ermöglicht, dass strukturierte und unstrukturierte Daten nicht nur automatisiert gesammelt, sondern auch indexiert und kategorisiert werden.

Die Hitachi Content Platform konnte in diesem Projekt ihre einzigartigen Funktionalitäten für Compliance & e-Discovery unter Beweis stellen. In der umgesetzten Lösung werden Daten indexiert und kategorisiert, sobald sie von der HCP entgegen genommen werden. Im Anschluss werden die Daten anhand der Quellen (z.B. Email und Voice) sowie der Ursprungsländer getrennt, so dass Zugriff und Aufbewahrungsregeln an die Anforderungen des jeweiligen Rechtsraumes angepasst werden können.

Über dieses System wurde ein einfaches, interaktives Webinterface gelegt, das autorisierten Mitgliedern des Compliance Teams effektive Nachforschungen ermöglicht. Diese Lösung erlaubt der Global Compliance Group, ihre eigenen Abfragen zu definieren und sogar proaktive Benachrichtigungen bei verdächtigen Aktivitäten oder wahrscheinlichen Verstößen zu erhalten: Alle potenziellen Datenquellen wie eMail, Voice, SMS, Dokumente etc. können Screenings unterzogen werden, um eine korrekte Einhaltung regulatorischer Compliance zu gewährleisten.

Um selbst im Katastrophenfall den unterbrechungsfreien Betrieb der Lösung zu gewährleisten, wurden zwei HCP Appliances als Active-Active-Pair auf 2 europäische Länder verteilt.

Dieser hochverfügbare Verbund agiert als Backup und Archiv für alle lokalen Systeme, wodurch eines der größten Probleme des IT Teams ausgeräumt wurde, denn HCP braucht kein Backup!

Gleichzeitig ermöglicht die Hochverfügbarkeit der HCP, dass jederzeit die Vollständigkeit der gespeicherten Kommunikation sichergestellt und diese für Compliance Nachforschungen verfügbar ist.

Das Ergebnis

Mit der auf HCP basierenden Ingest-and-Search-Plattform hat die Global Compliance Group vereinfachten Zugriff auf alle notwendigen Daten – auf Knopfdruck in einem zentralen Portal.

Mit dieser Lösung wurde die Geschwindigkeit, Effizienz und Flexibilität von Nachforschungen maßgeblich erhöht und die Zeit vom Eröffnen bis zum Abschließen der Ermittlungen von Wochen auf Stunden reduziert. Berechtigte Nutzer können die Daten, die Sie benötigen, ganz einfach von ihrem Schreibtisch aus abrufen und direkt sichten, ohne in der IT um Unterstützung zu bitten. So kann das Compliance Team effektiver und effizienter arbeiten, während gleichzeitig die Arbeitsbelastung für IT-Mitarbeiter reduziert werden konnte.

Gleichzeitig wird das IT-Team von Tätigkeiten wie dem Exportieren oder Vorselektieren der Daten bzw. dem Rücksichern von Backups entlastet und kann andere geschäftliche Herausforderungen angehen. Die HCP gibt dem Kunden Kontrolle über das bisher Unkontrollierbare. Als revisionssichere Datenquelle kann das Compliance Team darauf vertrauen, dass die abrufbaren Informationen in keiner Weise verändert wurden. Daten, die in der HCP Lösung vorgehalten werden sind vollständig, umfassend sowie auditierbar.

Aufgrund des Projekterfolges plant der Kunde, der Plattform weitere Datenquellen hinzuzufügen, wie beispielsweise Trading Applikationen und eine Cloud-Instanz von Skype for Business.

Durch die HCP setzt der Kunde neue Standards für Regulatory Compliance & e-Discovery im Bankensektor, die von anderen Unternehmen bereits aufgenommen werden. Da sich die regulatorische Landschaft ständig verändert, ermöglicht die HCP auf neue Anforderungen schnell und zentral zu reagieren und Neuerungen sicher über alle globalen Geschäftseinheiten zu implementieren.
Am Wichtigsten ist aber, dass die HCP die Möglichkeit schafft, die volle Kontrolle über Daten zurückzugewinnen und das in einer flexiblen, umfassenden Lösung, die in der Lage ist, auch zukünftige Compliance Herausforderungen problemlos umzusetzen - kombiniert mit einem nicht unwesentlichen wirtschaftlichen Optimierungspotenzial, denn durch die Reduzierung der Systeme und Softwareprodukte sowie die Zentralisierung des Systems konnte sich das Projekt bereits nach einem Jahr amortisieren.

Über Hitachi Vantara

Hitachi Vantara, eine hundertprozentige Tochtergesellschaft von Hitachi, Ltd., hilft datenorientierten Führungskräften, den Wert ihrer Daten zutage zu bringen und zu nutzen, um Neuerungen intelligent einzubringen und Resultate zu erzielen, die sowohl für die Wirtschaft als auch für die Gesellschaft wichtig sind. Wir kombinieren Technologie, geistiges Eigentum und Branchenwissen, um Datenlösungen bereitzustellen, die es Unternehmen ermöglichen, das Kundenerlebnis zu verbessern, neue Einnahmequellen zu entwickeln und die Betriebskosten zu senken. Nur Hitachi Vantara steigert Ihren Innovationsvorsprung durch die Kombination von umfangreichem IT-, OT- und Fachgebiets-Know-how.

Über Tech Data Advanced Solutions

Tech Data verbindet die Welt mithilfe von Technologien. Unser End-to-End-Portfolio an Produkten, Services und Lösungen, sowie unsere spezialisierten Fähigkeiten und tiefe Expertise in Next Generation Technologien helfen Channel-Partnern, die Produkte und Lösungen bereitzustellen, die Vernetzung, Wachstum und Fortschritt ermöglichen. Tech Data nimmt auf der Liste der Fortune 500® den 107. Platz ein und steht seit neun Jahren in Folge auf der Liste der „World´s Most Admired Companies“ von Fortune. Nähere Informationen finden Sie unter www.techdata.com und www.techdata.de. Tech Data ist in Deutschland Distributor für das Portfolio von Hitachi Vantara.

Information

Wenn Sie sich für die vollständige Fallstudie inklusive Informationen zu Anwender und Feedback zur Lösung interessieren, nehmen Sie Kontakt mit werner.habicht@techdata.com auf. Wir senden Ihnen gerne weitere Informationen zu oder beraten Sie hinsichtlich der Einsatzmöglichkeiten der Hitachi Content Platform.

HITACHI
Inspire the Next