Pearl Harbor, Safe Harbor und datenschutzkonformes Cloud Computing

GI ITSECMGT, Frankfurt, 26.2.2016

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

www.datenschutz.rlp.de | poststelle@datenschutz.rlp.de

Helmut Eiermann
Gruppenleiter Technik
Hintere Bleiche 34 | 55116 Mainz
Tel (06131) 208 2226
Fax (06131) 208 2497
h.eiermann@datenschutz.rlp.de

Agenda

- Safe Harbor-Urteil – Ursache und Folgen
- Aktuelle Situation
- Konsequenzen / Lösungsansätze

Safe Harbor

HARBOR

MENT OF COMMERCE

ipien:

ht

- Weitergabe
- Zugangsrecht
- Sicherheit
- Datenintegrität
- Durchsetzung

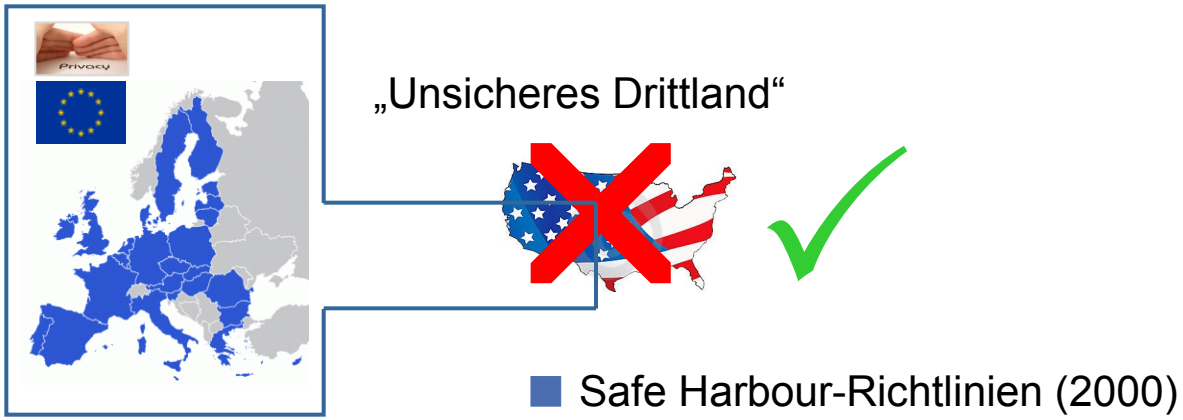
Was ist geschehen ?

Compliance / Verantwortlichkeit

„Unsicheres Drittland“

Sicherer Datenschutzhafen USA

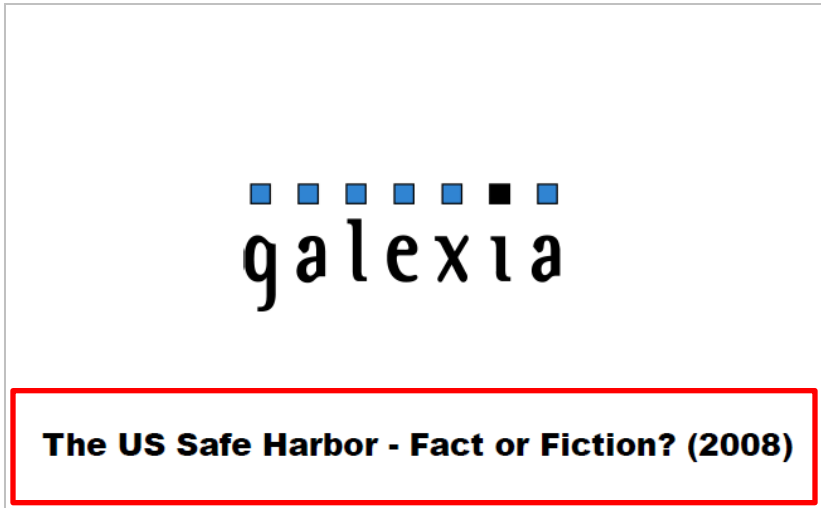
- DV beschränkt auf den Bereich der EU / EWR



- Safe Harbour-Richtlinien (2000)

Compliance / Verantwortlichkeit

Untersuchung zur Verlässlichkeit von Safe Harbour Vereinbarungen

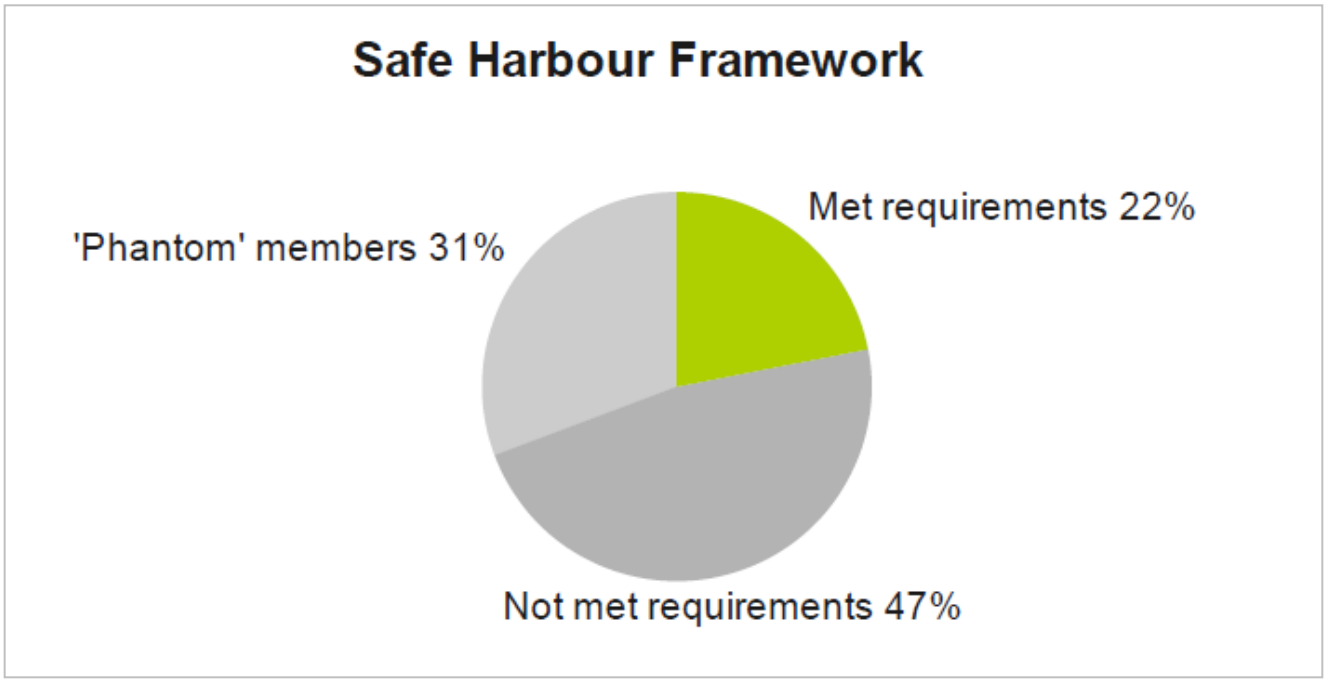


Safe Harbour Prinzipien:

- Informationspflicht
- Wahlmöglichkeit
- Weitergabe
- Zugangsrecht
- Sicherheit
- Datenintegrität
- Durchsetzung

http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

Sicherer Datenschutzhafen USA ?



http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

Compliance / Verantwortlichkeit

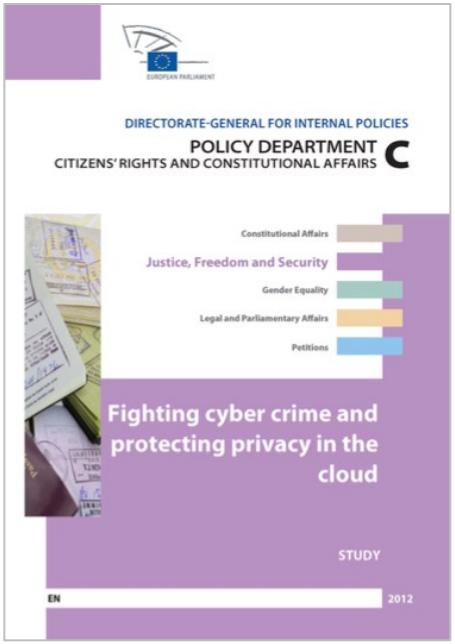
Entschließung der deutschen Datenschutzaufsichtsbehörden (2010) *

*„Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen […] nicht gewährleistet ist, trifft auch die **Unternehmen** in Deutschland eine **Verpflichtung**, gewisse **Mindestkriterien zu prüfen**, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.“*

- Gültigkeit und Nachweis der Selbst-Zertifizierung
- Einhaltung der Safe Harbour Grundsätze
- Einhaltung der Informationspflichten an die Betroffenen
- Dokumentation der Prüfungen

** www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20100429_safe_harbor*

Sicherer Datenschutzhafen USA ?



5.4. US/EU Relations

Particular attention should be given to **US law that authorizes the surveillance of Cloud data of non-US residents**. The EP should ask for further enquiries into the US FISA Amendments Act, the status of the 4th Amendment with respect to NONUSPERS, and the USA PATRIOT Act (especially s.215).

The EP should consider **amending the DP Regulation to require prominent warnings to individual data subjects** (of vulnerability to political surveillance) before EU Cloud data is exported to US jurisdiction. No data subject should be left unaware if sensitive data about them is exposed to a 3rd country's surveillance apparatus. The existing derogations must be dis-applied for Cloud because of the systemic risk of loss of data sovereignty. The EU should open new negotiations with the US for recognition of a human right to privacy which grants Europeans equal protections in US courts.

http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf

Microsoft

USA
Redmond

- Patriot Act
- Foreign Intelligence Surveillance Act (FISA) 1881a

30.06.2011 13:05

« Vorige | Nächste »

US-Behörden dürfen auf europäische Cloud-Daten zugreifen

vorlesen / MP3-Download

Cloud-Anbieter wie Microsoft müssen US-Strafverfolgungsbehörden Zugriff auf von Kunden gespeicherte Daten gewähren, berichtet der US-Branchendienst *ZDNet*. Das betrifft auch in der EU ansässige Firmen und in europäischen Rechenzentren liegende Daten, wie Microsofts britischer Direktor Gordon Frazer anlässlich der Markteinführung von Microsofts Office 365 in London erklärte. Er antwortete damit auf die Frage, ob Microsoft zusichern könne, dass in seinen EU-Rechenzentren gespeicherte Daten Europa niemals verlassen könnten.

Da das Unternehmen seinen Firmensitz in den USA habe, müsse es die dortigen Gesetze befolgen, sagte Frazer. Das gilt insbesondere für den Patriot Act, der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. Frazer zufolge würden Kunden über die Herausgabe von Daten "informiert, wann immer das möglich ist". Eine Garantie dafür könne er jedoch nicht geben. Denn in den USA kann das FBI mit einem National Security Letter (NSL) ein Redeverbot (Gag order) für den Betreffenden aussprechen. In diesem Fall darf er nicht einmal sagen, dass er einen NSL erhalten hat.

Microsoft Office 365

Microsoft

USA
Redmond

Microsoft

Great Britain
London

- Patriot Act
- Foreign Intelligence Surveillance Act (FISA) 1881a

IT-Sicherheit in der Cloud

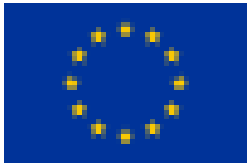
Microsoft[33]. A company representative was asked at the launch of their new cloud service Office365 whether Microsoft can

> "... guarantee that EU-stored-data, held in EU based data centers, will not leave the European Economic Area under any circumstances — even under a request from the Patriot Act."

The reply was:

> "Microsoft cannot provide these guarantees. Neither can any other company."

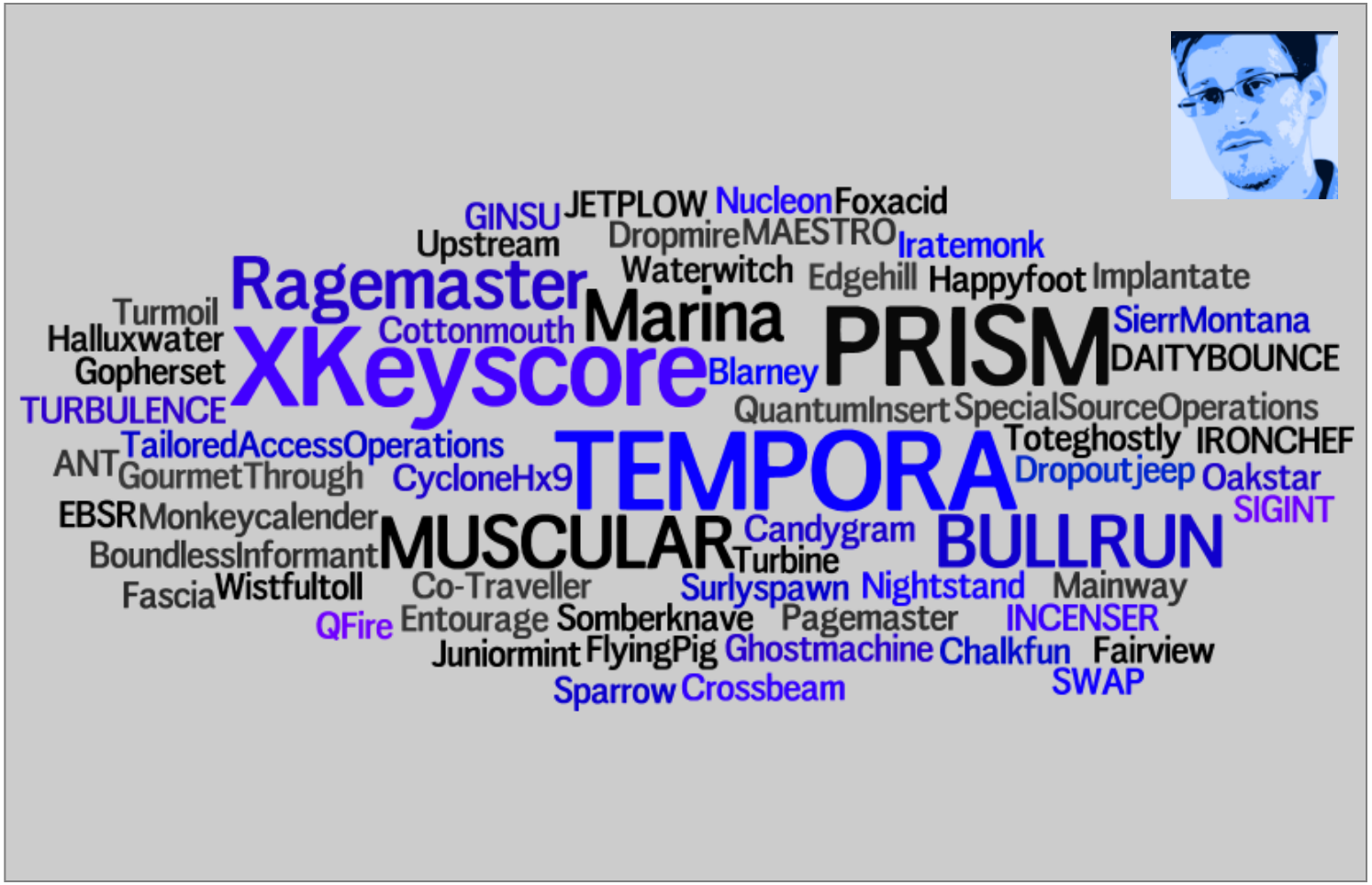
This would apply, for example, to all files stored in the Azure platform and Office365.

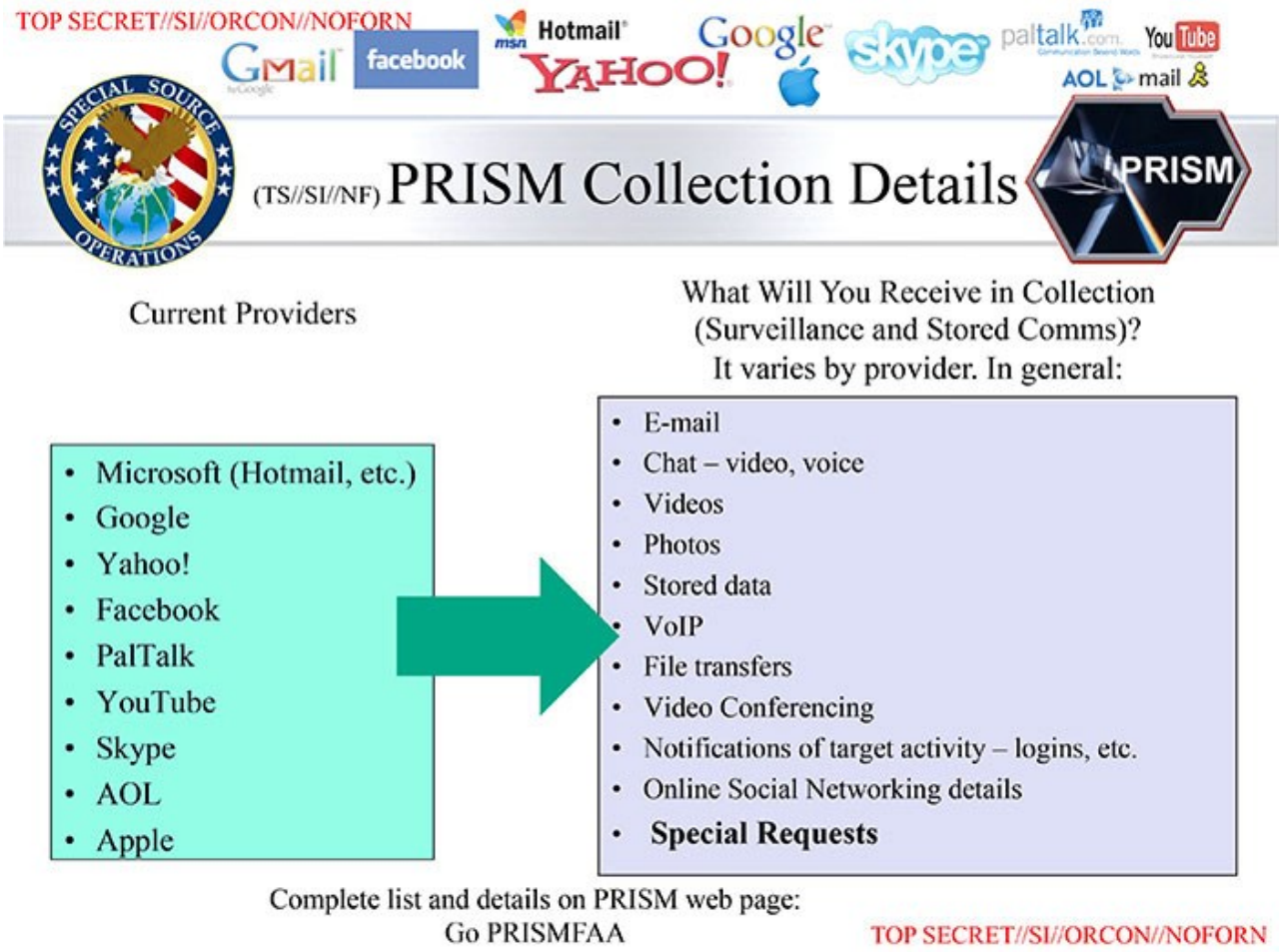


Art. 29-Gruppe

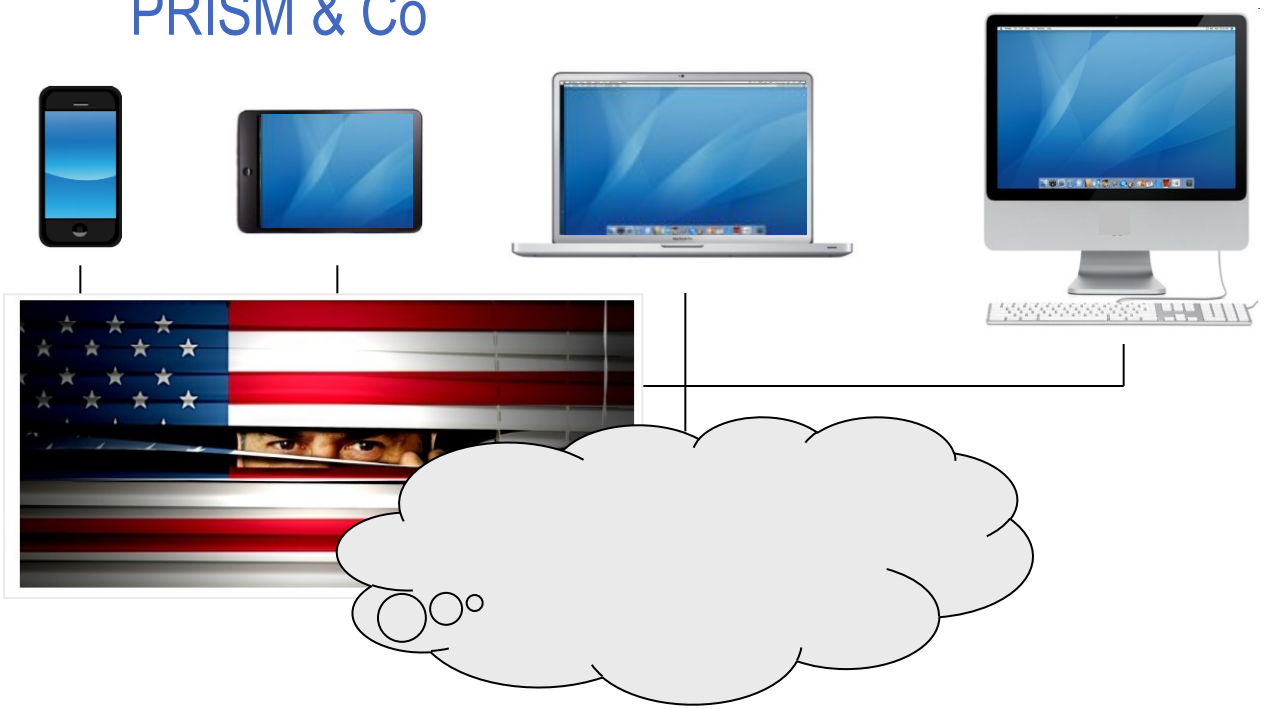
*„Die von den **Zugriffen** der ausländischen Behörden betroffenen personenbezogenen Daten unterliegen in den jeweiligen Staaten oft keinen datenschutzrechtlichen Restriktionen, die **europäischen Standards** auch nur ansatzweise genügen könnten.*

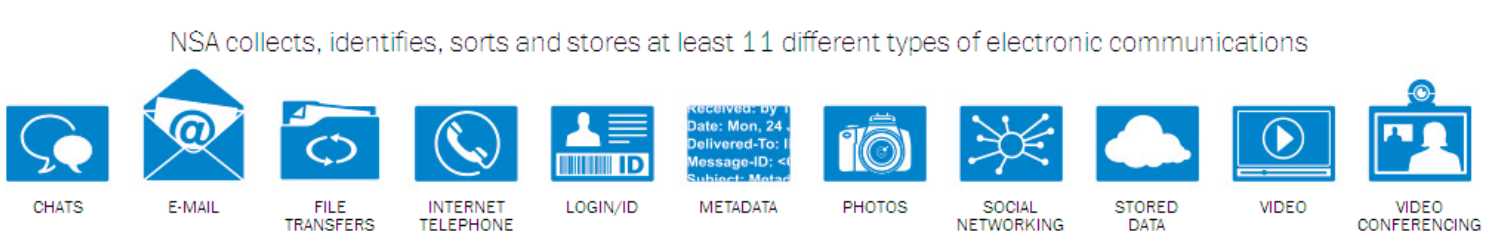
Juni 2013


GINSU
JETPLOW
Nucleon
Foxacid
Upstream
Dropmire
MAESTRO
Iratemonk
Ragemaster
Waterwitch
Edgehill
Happyfoot
Implantate
Turmoil
Halluxwater
Gopherset
Marina
PRISM
SierrMontana
Cottonmouth
XKeyscore
Blarney
DAITYBOUNCE
TURBULENCE
QuantumInsert
SpecialSourceOperations
TailoredAccessOperations
TEMPORA
Toteghostly
IRONCHEF
ANT
GourmetThrough
CycloneHx9
Dropoutjeep
Oakstar
SIGINT
EBSR
Monkeycalender
MUSCULAR
Candygram
BULLRUN
BoundlessInformant
Turbine
Fascia
Wistfultoll
Co-Traveller
Surlyspawn
Nightstand
Mainway
QFire
Entourage
Somberknave
Pagemaster
INCENSER
Juniormint
FlyingPig
Ghostmachine
Chalkfun
Fairview
Sparrow
Crossbeam
SWAP


TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
Microsoft (Hotmail, etc.)
Google
Yahoo!
Facebook
PalTalk
YouTube
Skype
AOL
Apple
E-mail
Chat – video, voice
Videos
Photos
Stored data
VoIP
File transfers
Video Conferencing
Notifications of target activity – logins, etc.
Online Social Networking details
Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

PRISM & Co




NSA collects, identifies, sorts and stores at least 11 different types of electronic communications
CHATS
E-MAIL
FILE TRANSFERS
INTERNET TELEPHONE
LOGIN/ID
METADATA
PHOTOS
SOCIAL NETWORKING
STORED DATA
VIDEO
VIDEO CONFERENCING

NSA-Cloud. A free Backup of your Life!

NSA CLOUD: The world's easiest cloud services.
It's simple. It's ubiquitous. It's free. No registration required.

Unlimited storage!

The first back-up of all your data: We offer a virtual cloud server which includes a full back-up of all your personal and non-personal data, incl.

- » transaction data,
- » electronic payments,
- » call data records,
- » all your private pictures,
- » all your stuff from work,
- » your complete search-history,
- » all your file-transfers,
- » all your social interactions,
- » your medical history,
- » your tax history,
- » and many, many more.

Everything you thought you had deleted or lost forever - we still got it.

Easy to use!

There is no registration required. We already did that for you.

Our data gathering practices constitute a circumscribed, narrow system directed at us being able to protect all people, companies and public authorities around the world from loosing their data.

Unfortunately, the following services have not been released for all of our customers yet:

- » data-export,
- » delete data and
- » sign out.

100% FREE !!!

You can learn a lot more about this product here: SIGAD US-984XN.

And, did you know that we have many more great ideas? Don't worry: You won't miss any of them.

But since they are so advanced that you might not even notice them, you should stay in touch for updates.

A word from our partners...

http://www.nsa-cloud.com/

Cloud Dienstleister

amazon web services™

iCloud

Google™

hp Cloud Services

Microsoft® Office 365

Windows® Azure™

amazon web services | Security Blog

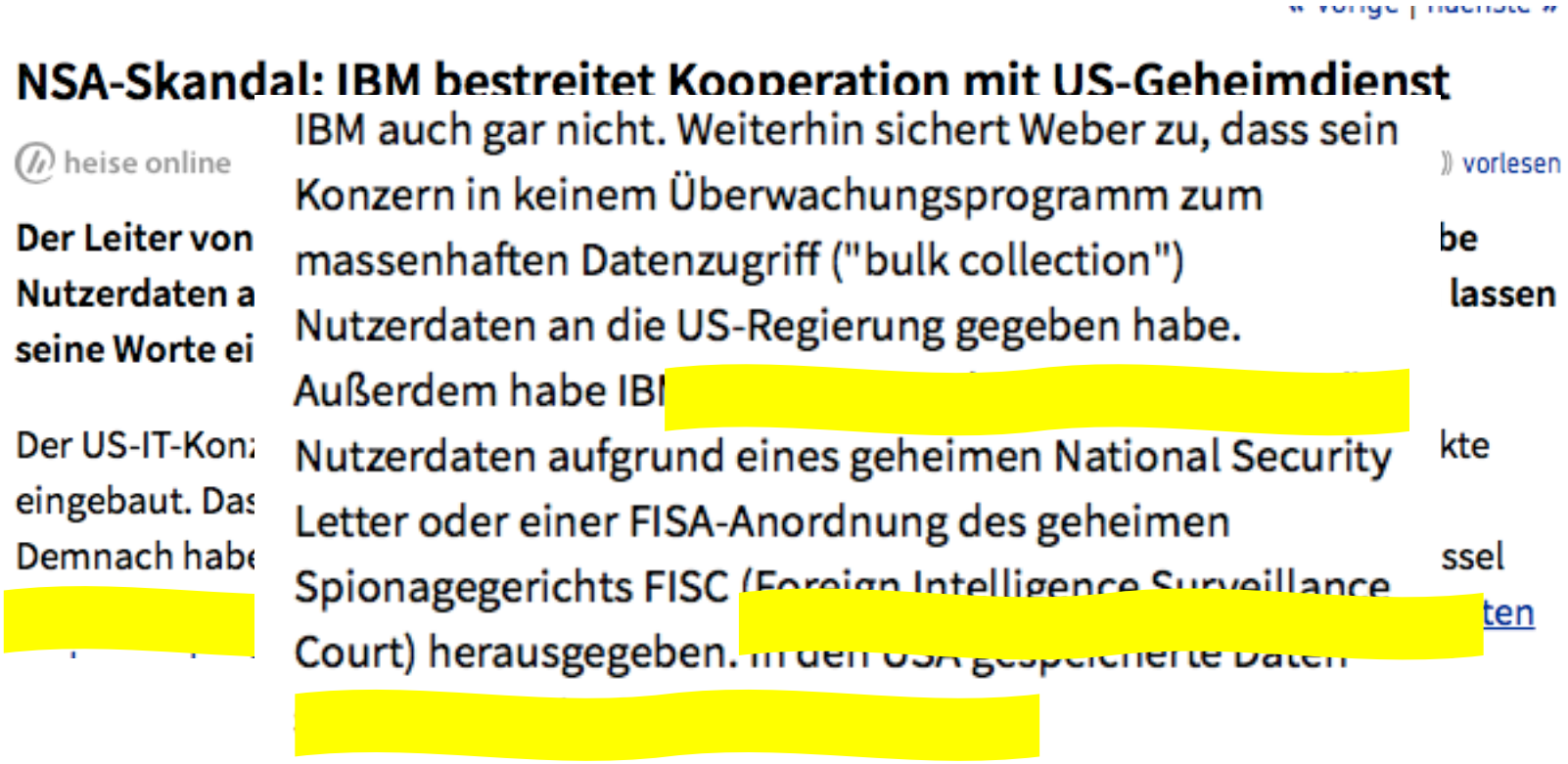
Stay up to date on security and compliance in AWS

- Where we need to act publicly to protect customers, we do. We have repeatedly challenged government subpoenas for customer information that we believed were overbroad, winning decisions that have helped to set the legal

Transparency report

- Amazon does not disclose customer information Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.

https://blogs.aws.amazon.com/security/post/Tx35449P4T7DJIA/Privacy-and-Data-Security



NSA-Skandal: IBM bestreitet Kooperation mit US-Geheimdienst

heise online

» vorlesen

Der Leiter von
Nutzerdaten a
seine Worte ei

Der US-IT-Kon
eingebaut. Das
Demnach habe

IBM auch gar nicht. Weiterhin sichert Weber zu, dass sein Konzern in keinem Überwachungsprogramm zum massenhaften Datenzugriff ("bulk collection") Nutzerdaten an die US-Regierung gegeben habe. Außerdem habe IBM [redacted] Nutzerdaten aufgrund eines geheimen National Security Letter oder einer FISA-Anordnung des geheimen Spionagegerichts FISC (Foreign Intelligence Surveillance Court) herausgegeben. [redacted]

be
lassen
kte
ssel
ten

http://www.heise.de/newsticker/meldung/NSA-Skandal-IBM-bestreitet-Kooperation-mit-US-Geheimdienst-2147415.html

Datenschutz bei Facebook & Co.: EuGH erklärt Safe Harbor für ungültig

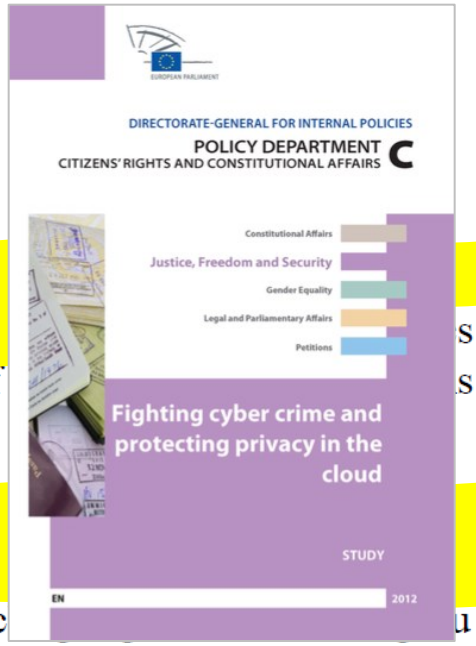
heise online 06.10.2015 09:52 Uhr – Martin Holland vorlesen

Der Europäische Gerichtshof in Luxemburg hat das Safe-Harbor-Abkommen zwischen den USA und der EU für ungültig erklärt. Persönliche Daten europäischer Nutzer seien in den

http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-Co-EuGH-erklaert-Safe-Harbor-fuer-ungueltig-2838025.html

EuGH-Urteil C-362/14

CVRIA
LUXEMBOURG



94 Insbesondere verletzt eine

durch Art. 7 der Charta garantierten Grundrechts auf

[…]

95 Desgleichen verletzt eine

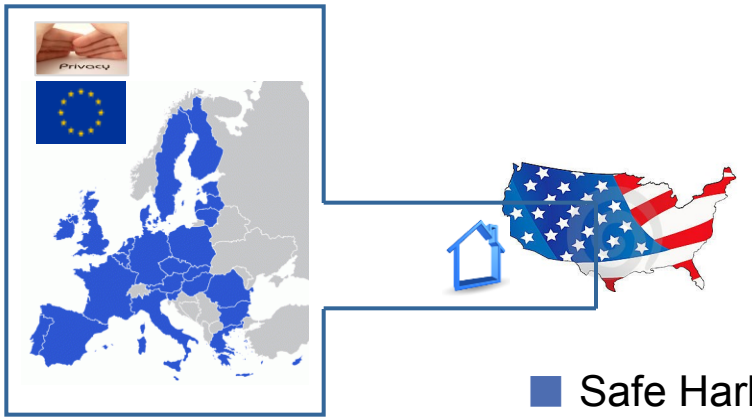
personenbezogenen Daten zu erlangen oder ihre Beric

erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingunge

einzulegen. Insoweit ist schon das Vorhandensein einer wirksamen, zur

Sicherer Datenschutzhafen USA

- DViA Beschränkt auf den Bereich der EU / EWR

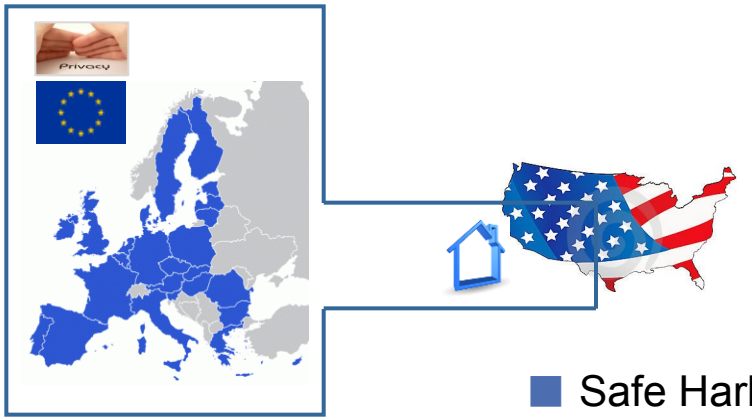


CVRIA
LUXEMBOURG

- Safe Harbour Richtlinien (2000)

Compliance / Verantwortlichkeit

- Beschränkt auf den Bereich der EU / EWR



CVRIA
LUXEMBOURG

- Safe Harbour Richtlinien (2000)
- EU-Standard-Vertragsklauseln ?
- Binding Corporate Rules ?

- Patriot Act
- Foreign Intelligence Surveillance Act (FISA) 1881a

Cloud Dienstleister

pwc
März 2015

70% der deutschen Unternehmen nutzen Cloud Computing

90% der deutschen Unternehmen geben Informations-sicherheit, Compliance, Server-Standort und Vertrauenswürdigkeit des Anbieters als Kriterium an

hp Cloud Services

Microsoft® Office 365

Windows® Azure™

SPIEGEL ONLINE NETZWELT

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Netzwelt > Netzpolitik > Cloud Computing > Cloud Computing: Microsoft und Apple klagen gegen Datenzugriff

Verfahren in New York: Microsoft und Co. wollen Cloud-Daten vor US-Zugriff schützen

Daten, die amerikanische Firmen im Ausland speichern, müssen auf Gerichtsbeschluss auch in den USA offengelegt werden. Apple, Microsoft und andere IT-Firmen fürchten deshalb um ihr Geschäft mit dem Cloud-Computing - und wehren sich.

Dienstag, 17.06.2014 – 00:23 Uhr

Drucken | Senden | Merken

Nutzungsrechte | Feedback

Kommentieren | 6 Kommentare

THEMA
Cloud Computing

US-Überwachung

New York - Der Zugriff der US-Regierung auf außerhalb der USA gespeicherte Daten macht den großen IT-Unternehmen Sorgen - nicht zuletzt aus wirtschaftlichen Gründen. Microsoft, Apple und drei weitere US-amerikanische Firmen wollen nun vor Gericht erreichen, dass die Daten nicht mehr abgegriffen werden dürfen.

Andernfalls, so fürchten die Unternehmen, könnten sie Milliarden Dollar verlieren. Das Problem: Das Geschäft mit dem sogenannten Cloud-Computing, bei dem Daten auch außerhalb der USA auf Servern in einer "Wolke" im Internet gespeichert werden, gehe kaputt, wenn Kunden sich nicht auf deren Sicherheit verlassen könnten.

http://www.spiegel.de/netzwelt/netzpolitik/cloud-computing-microsoft-und-apple-klagen-gegen-datenzugriff-a-975576.html

ZDNet / Cloud

New York Times: Deutschland drängte Microsoft zu NSA-Klage

von Florian Kalenda am 21. Juli 2014, 16:26 Uhr

Microsoft hat erst auf Drängen deutscher Behörden gegen den NSA-Durchsuchungsbefehl geklagt, der in einem irischen Rechenzentrum gespeicherte Kundendaten betraf. Diese Information findet sich in einem Porträt von Microsofts Chefjurist Brad Smith in der New York Times.

Demnach war es ein "Regierungsmitarbeiter", der den Konzern aufforderte, gegen den Haftbefehl vorzugehen. Andernfalls, so soll er gedroht haben, werde die deutsche Regierung nie wieder die Cloud-Speicherdienste eines amerikanischen Unternehmens wie Microsoft in Anspruch nehmen. Dies sei zu einer Zeit gewesen, als Deutschland gerade wegen der gegen das Handy von Kanzlerin Angela Merkel gerichteten US-Abhörmaßnahmen erzürnt gewesen sei, heißt es in dem Bericht.

Der Durchsuchungsbefehl wurde im Dezember 2013 ausgestellt. Im April beantragte Microsoft, ihn für nichtig zu erklären. Dies wurde abgewiesen. Im Juni legte Microsoft neue Einwände gegen diese Entscheidung vor. Die nächste Anhörung ist für 31. Juli geplant.

http://www.zdnet.de/88199194/new-york-times-deutschland-draengte-microsoft-zu-nsa-klage/

Wie ist die aktuelle Situation ?

Datenübermittlung in die USA

- Safe Harbor-Richtlinien
  - angemessenes Datenschutzniveau
  - Feststellung durch EU-Kommission

- EU-Standard-Vertragsklauseln (EU SCC) ?
  - ausreichende Garantien
  - Genehmigung durch die Aufsichtsbehörde

- Verbindliche Unternehmensregelungen (BCR) ?
  - ausreichende Garantien
  - Genehmigung durch die Aufsichtsbehörde

- Einwilligung

- Vertragserfüllung im Interesse der Betroffenen

Sondersitzung der DSK am 21. Oktober 2015 in Frankfurt

Positionspapier

der Konferenz der unabhängigen Datenschutzbehörden

des Bundes und der Länder

- Datenübermittlung aufgrund Safe Harbor unzulässig
- EU-Standard-Vertragsklauseln und BCR fraglich
- Derzeit keine weiteren Genehmigungen von SCC und BCR
- Einwilligung nicht widerholt, massenhaft und routinemäßig

http://www.datenschutz.rlp.de/de/grem_dsbkonferenz/sonstiges/20151021_Positionspapier_DSK_Safe_Harbor.pdf

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Mainz, 26. Oktober 2015

Folgerungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz aus dem Urteil des EuGH vom 6. Oktober 2015 (C-362/14) „Safe Harbor“

http://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf

Position LfDI Rheinland-Pfalz

- Datenübermittlungen auf Safe Harbor-Grundlage unzulässig
- Standard-Vertragsklauseln prüfungsbedürftig (Kündigung)
- keine neuen Genehmigungen für Binding Corporate Rules
- Einwilligung nur in Ausnahmefällen; unzulässig im Beschäftigteverhältnis
- Datenübermittlungen in die USA nur noch ausnahmsweise zulässig / Genehmigungsvorbehalt
- keine Sanktion zurückliegender Datenübermittlungen

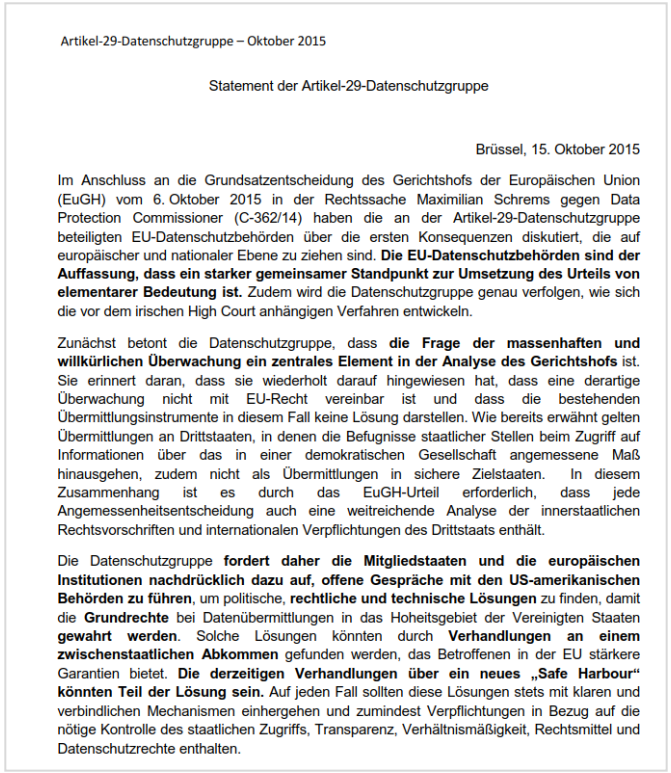
http://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf

Prüfungspflicht der Unternehmen

- Prüfung der Rechtsgrundlage
- Prüfung der außerordentlichen Kündigung von Verträgen nach EU-Standard-Vertragsklauseln
- keine neuen Genehmigungen für Binding Corporate Rules
- Prüfung alternativer Übermittlungsmöglichkeiten
- Prüfung technischer Lösungsansätze

http://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf

Aktuelle Situation – Art. 29-Gruppe



Artikel-29-Datenschutzgruppe – Oktober 2015

Statement der Artikel-29-Datenschutzgruppe

Brüssel, 15. Oktober 2015

Im Anschluss an die Grundsatzentscheidung des Gerichtshofs der Europäischen Union (EuGH) vom 6. Oktober 2015 in der Rechtssache Maximilian Schrems gegen Data Protection Commissioner (C-362/14) haben die an der Artikel-29-Datenschutzgruppe beteiligten EU-Datenschutzbehörden über die ersten Konsequenzen diskutiert, die auf europäischer und nationaler Ebene zu ziehen sind. **Die EU-Datenschutzbehörden sind der Auffassung, dass ein starker gemeinsamer Standpunkt zur Umsetzung des Urteils von elementarer Bedeutung ist.** Zudem wird die Datenschutzgruppe genau verfolgen, wie sich die vor dem irischen High Court anhängigen Verfahren entwickeln.

Zunächst betont die Datenschutzgruppe, dass **die Frage der massenhaften und willkürlichen Überwachung ein zentrales Element in der Analyse des Gerichtshofs** ist. Sie erinnert daran, dass sie wiederholt darauf hingewiesen hat, dass eine derartige Überwachung nicht mit EU-Recht vereinbar ist und dass die bestehenden Übermittlungsinstrumente in diesem Fall keine Lösung darstellen. Wie bereits erwähnt gelten Übermittlungen an Drittstaaten, in denen die Befugnisse staatlicher Stellen beim Zugriff auf Informationen über das in einer demokratischen Gesellschaft angemessene Maß hinausgehen, zudem nicht als Übermittlungen in sichere Zielstaaten. In diesem Zusammenhang ist es durch das EuGH-Urteil erforderlich, dass jede Angemessenheitsentscheidung auch eine weitreichende Analyse der innerstaatlichen Rechtsvorschriften und internationalen Verpflichtungen des Drittstaats enthält.

Die Datenschutzgruppe **fordert daher die Mitgliedstaaten und die europäischen Institutionen nachdrücklich dazu auf, offene Gespräche mit den US-amerikanischen Behörden zu führen**, um politische, **rechtliche und technische Lösungen** zu finden, damit die **Grundrechte** bei Datenübermittlungen in das Hoheitsgebiet der Vereinigten Staaten **gewahrt werden**. Solche Lösungen könnten durch **Verhandlungen an einem zwischenstaatlichen Abkommen** gefunden werden, das Betroffenen in der EU stärkere Garantien bietet. **Die derzeitigen Verhandlungen über ein neues „Safe Harbour" könnten Teil der Lösung sein.** Auf jeden Fall sollten diese Lösungen stets mit klaren und verbindlichen Mechanismen einhergehen und zumindest Verpflichtungen in Bezug auf die nötige Kontrolle des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit, Rechtsmittel und Datenschutzrechte enthalten.

- Verhandlungen mit den USA
- rechtliche & technische Lösungen
- Frist bis Ende Januar 2016

https://www.datenschutz.hessen.de/download.php?download_ID=335

Safe Harbor 2.0

Einigung zwischen EU und USA: Safe Harbor heißt jetzt "EU-US-Privacy Shield" UPDATE

heise online 02.02.2016 16:33 Uhr vorlesen

Das Logo der neuen Vereinbarung (Bild: Andrus Ansip)

Die EU-Kommission hat mit den USA einen Nachfolger für das vom EuGH gekippte Safe-Harbor-Abkommens ausgehandelt. Unter anderem soll das US-Handelsministerium die Firmen kontrollieren, die Daten aus Europa verarbeiten.

http://www.heise.de/newsticker/meldung/Einigung-zwischen-EU-und-USA-Safe-Harbor-heisst-jetzt-EU-US-Privacy-Shield-3091607.html

European Commission - Press release

EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield

Strasbourg, 2 February 2016

The European Commission and the United States have agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield.

- Robuste Verpflichtungen für Unternehmen / FTC-Kontrolle
- Transparenzverpflichtungen für Behördenzugriffe
- FTC-Beschwerde / Ombudsmann

➔ Absichtserklärung / keine Unterlagen (April an Art. 29-Gruppe)

➔ Keine Anpassung der Rechtslage in den USA

➔ Kein formeller Rechtsbehelf (Gericht)

Umfrage LfDI Rheinland-Pfalz

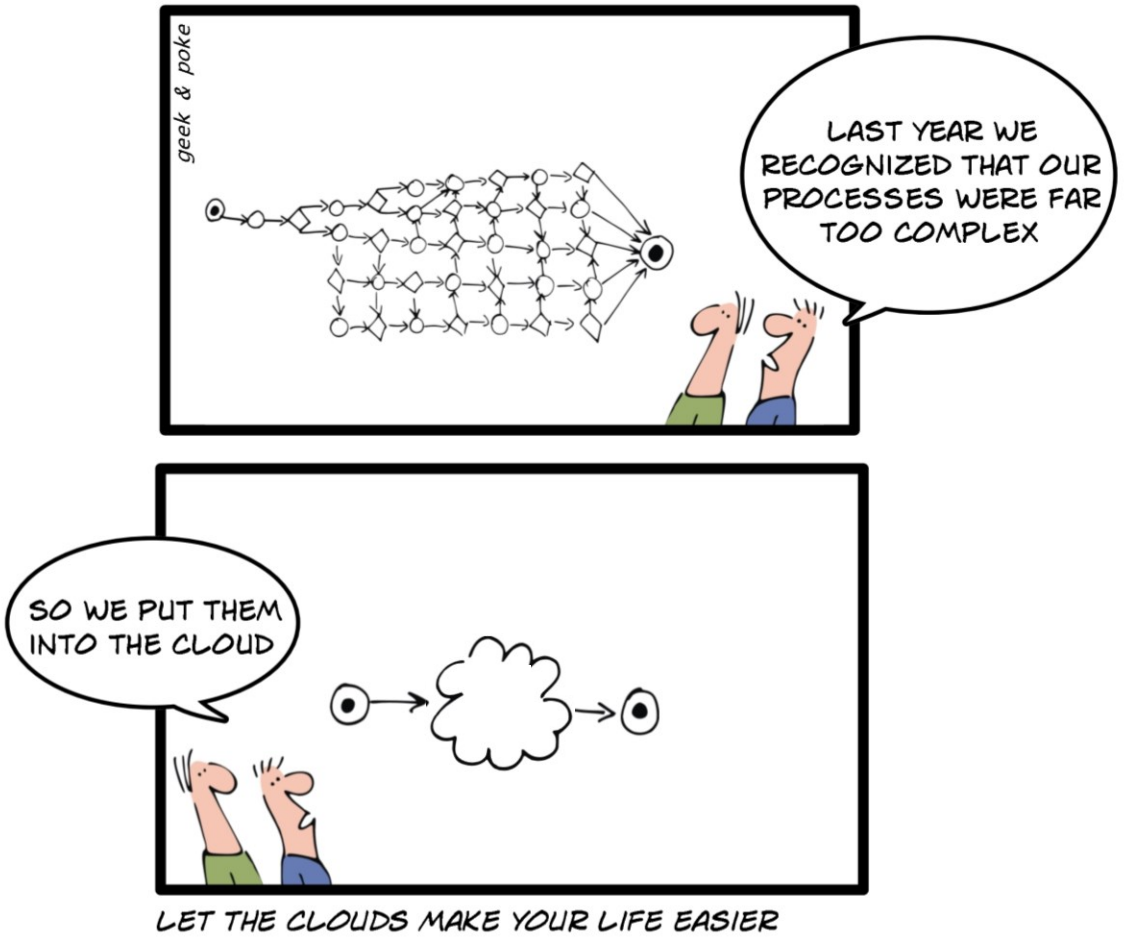
TOP 120-Unternehmen in Rheinland-Pfalz

- 47 % mit erheblichen Defiziten
- 15 % konnten die Fragen nicht innerhalb der Monatsfrist beantworten
- 15 % mit fehlerhafter Auffassung zum Datenschutzniveau in den USA
- 17 % mit fehlerhafter Auffassung zu Datenübermittlungen in die USA

z.B.:

- Cloud-Lösungen zur Datenspeicherung (IaaS, PaaS)
- SaaS-Lösungen (Office 365, Salesforce)
- Windows 10 / Office365
- E-Mail
- Online-Shops
- Dropbox, Onedrive, WeTransfer
- Virtuelle Telefonanlagen
- Fernwartung durch US-Stellen
- ...
- Alltagsdaten / Beschäftigtendaten „nicht personebezogen"

Let the Cloud make your Life easier!



Was kann man Unternehmen raten ?

Was kann man Unternehmen raten ?

- Situation klären
- Übermittlungsgrundlage prüfen / ändern
- IT-Strukturen umstellen
- Ggf. Anbieter wechseln
- Technische Lösungsansätze prüfen

Möglichkeit 1:

Umstrukturierung / Wechsel von Cloud-Lösungen

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

News ▾ Artikel ▾ Apps ▾ Aktuelles

iX > 7-Tage-News > 2014 > KW 33 > IBM ordnet die Cloud nach geographischen Regionen

News-Meldung vom 11.08.2014 10:55 Uhr « Vorige | Nächste »

IBM ordnet die Cloud nach geographischen Regionen

vorlesen / MP3-Download

Mit einem neuen Patent geht IBM das Speichern von Daten in der Cloud nach geographischen Regionen an. Kunden sollen selbst entscheiden und einsehen können, wo genau und bei wem sich ihre Daten befinden.

IBM arbeitet an einem System, das Daten in der Cloud nach unterschiedlichen geographischen Regionen ordnen soll. Der Konzern hat dafür in den USA das Patent 8,676,593 eingereicht, das einige technische Details der Umgebung beschreibt. Es handelt sich um eine Kombination aus Hardware und Software, die Programme sind auf dem lokalen Speicher vorgehalten. Sie präsentieren dem lokalen Client eine Liste der verfügbaren Regionen in denen passende Rechenzentren für die Cloud des Kunden stehen.

Daten kann die Plattform anhand zweier Vorgehensweisen auswählen: Entweder analysiert sie die zu speichernden Dateien anhand ihrer Eigenschaften oder man markiert sie eindeutig. Alle Daten, die ausschließlich in einer spezifischen Region gespeichert werden dürfen, sollen sich so auch nur auf einem dortigen Rechenzentrum wiederfinden.

IBM hat den Antrag für das Patent bereits im September 2010 eingereicht und im März 2014 erteilt bekommen. Obwohl die Cloud prinzipiell global zur Verfügung steht, schränken interne und staatliche Vorgaben bei vielen Unternehmen den Standort des Rechenzentrums stark ein. Jedoch schützt auch ein Speichern in der EU nur bedingt vor externem Zugriff: Als US-Unternehmen sieht sich Microsoft momentan damit konfrontiert, dass die US-Regierung Zugriff auf Daten in EU-Rechenzentren verlangt. (fo)

http://www.heise.de/ix/meldung/IBM-ordnet-die-Cloud-nach-geographischen-Regionen-2289770.html

Was kann man Unternehmen raten ?

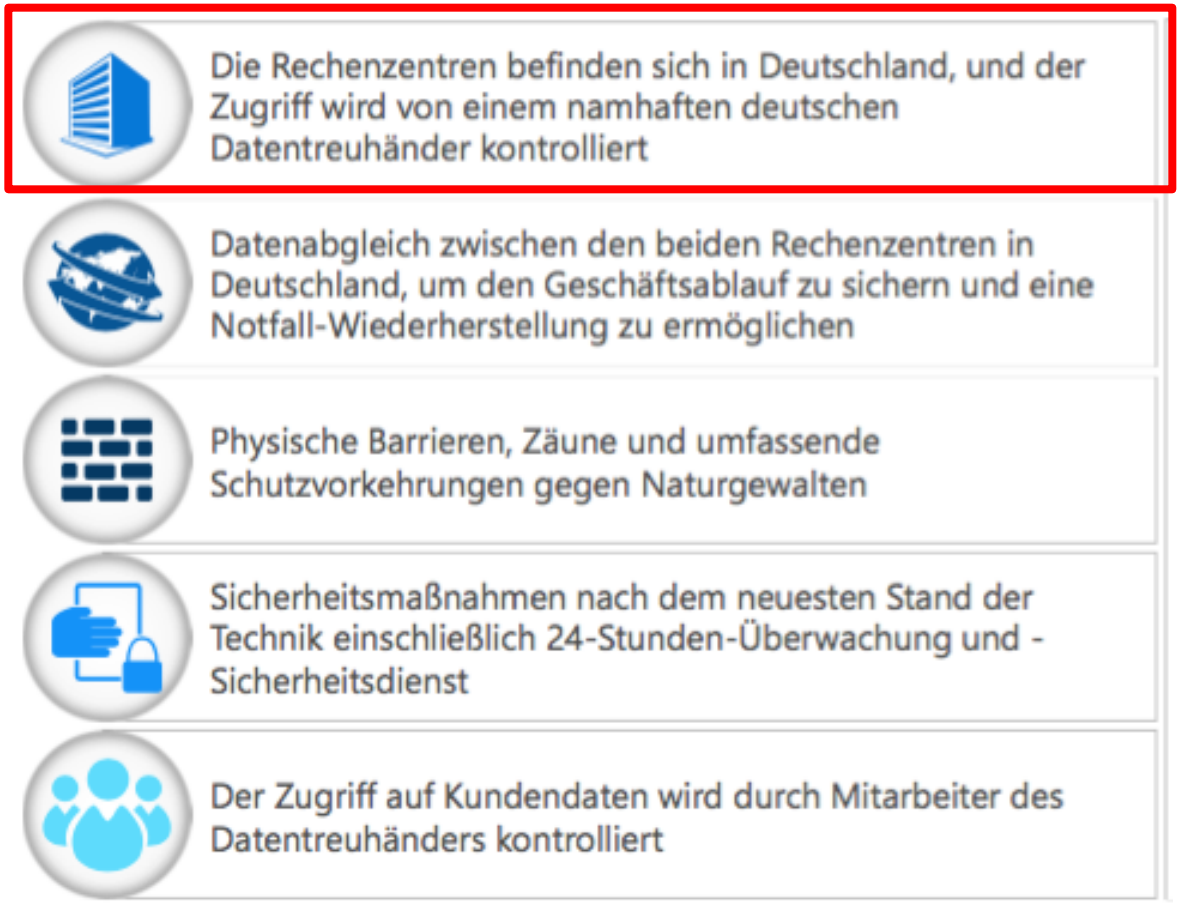
Microsoft

Partner Network

Eine Microsoft Cloud mit deutscher Datentreuhand

Die Microsoft Cloud mit deutscher Datentreuhand steht für die Bereitstellung der Microsoft-Dienste Azure, Office 365 sowie Dynamics CRM Online über eigenständige deutsche Rechenzentren. Sie können sich zukünftig für eine neue Cloud entscheiden – mit einem deutschen Datentreuhänder, der unter deutschem Recht agiert. Ihre Daten befinden sich damit nur auf deutschem Boden.

Erfahren Sie mehr


Die Rechenzentren befinden sich in Deutschland, und der Zugriff wird von einem namhaften deutschen Datentreuhänder kontrolliert
Datenabgleich zwischen den beiden Rechenzentren in Deutschland, um den Geschäftsablauf zu sichern und eine Notfall-Wiederherstellung zu ermöglichen
Physische Barrieren, Zäune und umfassende Schutzvorkehrungen gegen Naturgewalten
Sicherheitsmaßnahmen nach dem neuesten Stand der Technik einschließlich 24-Stunden-Überwachung und -Sicherheitsdienst
Der Zugriff auf Kundendaten wird durch Mitarbeiter des Datentreuhänders kontrolliert

Ein deutscher Datentreuhänder kontrolliert den Zugriff auf die Daten

Ein namhafter deutscher Datentreuhänder führt alle Handlungen oder Aufgaben mit Zugriff auf Kundendaten oder auf die Infrastruktur, auf der sich Kundendaten befinden, selbst durch oder überwacht diese.

Role Based Access Control (RBAC)-Tools kontrollieren jeglichen Zugriff auf Kundendaten	Ausschließlich der deutsche Datentreuhänder hat Zugriff auf Server mit Kundendaten	Mitarbeiter von Microsoft haben keinerlei administrative Top-Level-Rechte, um Zugriff auf Kundendaten zu gewähren	Mitarbeiter von Microsoft können sich nicht auf Server mit Kundendaten einloggen

Ménage à Trois

Microsoft

Deutsche Telekom

- Lizenzen
- Technischer Support
- Kunden-Support

- Datenspeicherung
- IT-Sicherheit
- WAN-Anbindung

Microsoft

USA
Redmond

Microsoft

Great Britain
London

Möglichkeit 2:
Kryptografische Lösungen

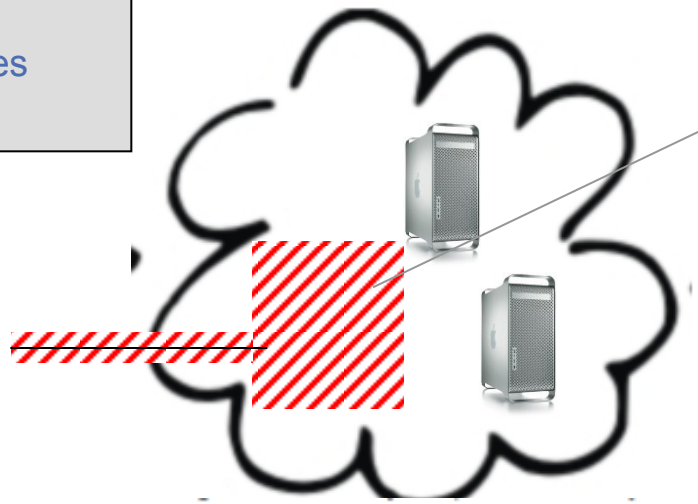
Lösungsansatz Verschlüsselung (IaaS)

- Verfahren
- Schlüssel

unter der Kontrolle des Auftraggebers

Krypto-Reglementierung

- Key Recovery
- Key Escrowing

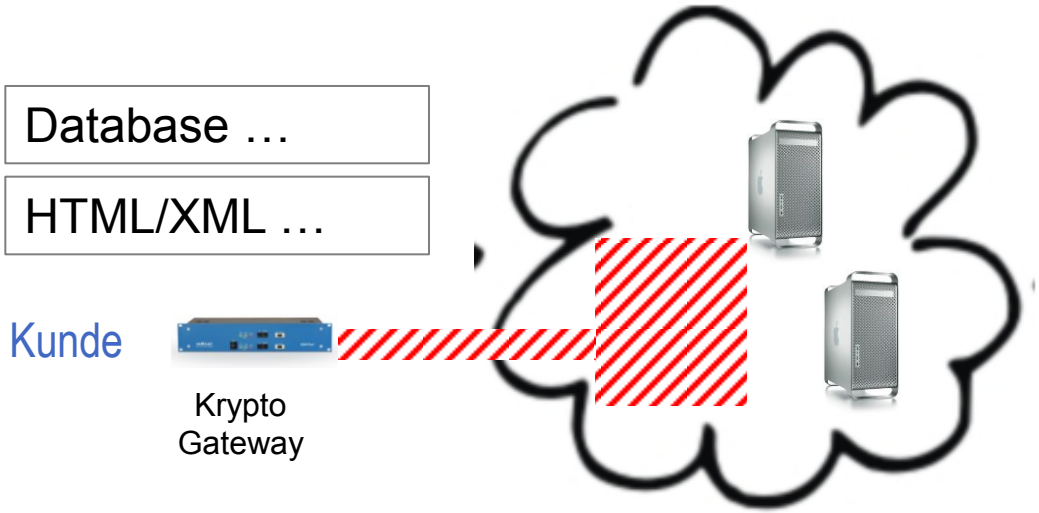


amazon web services

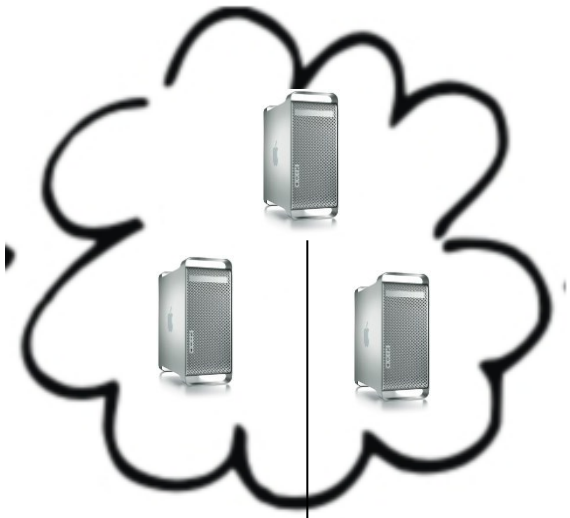
use, whether they be individual consumers or business customers. We offer AWS clients strong encryption as one of many standard security features, and

We publish security best practices documents on our website and

Lösungsansatz Verschlüsselung (SaaS, PaaS)



Lösungsansatz Verschlüsselung (SaaS, PaaS)



HTML/XML …

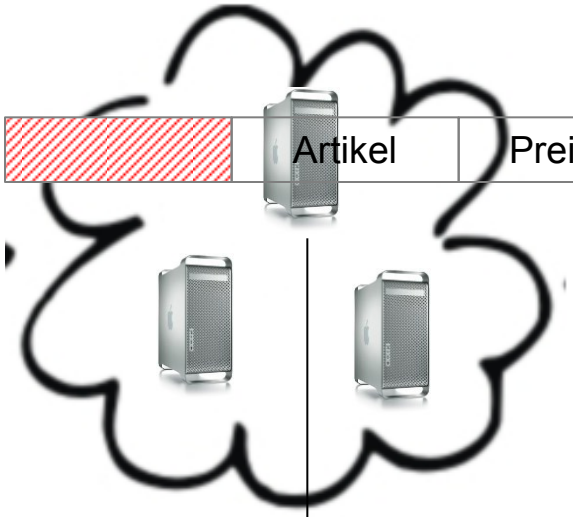
Database …

Krypto Gateway

	Artikel	Preis	Datum		

Name	Artikel	Preis	Datum	E-Mail	Adresse

Lösungsansatz Verschlüsselung (SaaS, PaaS)



Artikel	Preis	Datum		

HTML/XML …

Database …

Krypto
Gateway

Name	Artikel	Preis	Datum	E-Mail	Adresse

Was kann man Unternehmen raten ?

Verschlüsselungs-Gateways für die Cloud

Name des Unternehmens	CipherCloud	eperi GmbH	Origin Storage Ltd. / Marketing- und Vertriebsbüro Deutschland	Perspecsys, ein Unternehmen der Blue Coat Systems GmbH	Skyhigh Networks	Stratokey	Vormetric	Wintermute
Homepage	www.ciphercloud.com	eperi.de	www.originstorage.com	www.bluecoat.com	www.skyhighnetworks.com	www.stratokey.com	www.vormetric.com/de	wintermute.ai
Produkt	CipherCloud Platform	eperi Gateway	DataLocker SafeCrypt (vormals SkyCrypt)	Blue Coat Cloud Data Protection	Skyhigh Cloud Access Security Broker	StratoKey	Vormetric Cloud Encryption Gateway	wintermute.ai server
Preis	keine Angabe	keine Angabe	42€ zzgl. MwSt., lebenslange Lizenz	keine Angabe	keine Angabe	keine Angabe	keine Angabe	keine Angabe
Realisierungsform des Produkts (Appliance, Softwarepaket, Sonstiges)	Software as a Service (SaaS) / virtuelle private Cloud-Appliance / Software für den Eigenbetrieb (on Premise)	Software / virtuelle Appliance (OVA-Image) / Flex Image (SoftLayer) und Microsoft Azure Image / Appliance	Software	Software / gehostet bei Third-Party-Infrastruktur-Provider / Managed-Security-Service von Blue Coat oder anderem MSSP	virtuelle Appliance (on Premise) / Cloud-Dienst / Hybrid-Lösung	Software	Appliance	Software
Betriebssystem, auf dem das Gateway läuft	Red Hat Linux 6.x 64-Bit und CentOS 6.x 64-Bit	Linux, Windows, POWER8, Unix, AIX, alle Betriebssysteme, die Oracle JDK, IBM JDK oder OpenJDK unterstützen	keine Angabe	Linux (Red Hat, CentOS, Ubuntu, Novell SUSE) und Solaris	angepasstes Linux-Betriebssystem	Windows, Linux	eigenes, gehärtetes Betriebssystem	Linux (Debian, Ubuntu, RHEL, Fedora, CentOS und SLES)
unterstützte Client-Betriebssystem(e)	Windows, Mac, iOS, Andriod	alle	Windows bis 10, Mac OS X bis El Capitan	Zugang zu Cloud-Anwendungen über den Webbrowser	alle	alle	alle	alle
deutsche Version verfügbar	–	✓	✓	–	–	–	–	✓
Support auf Deutsch	✓	✓	–	✓	–	–	–	✓
Unterstützte Krypto-Algorithmen	AES 256	AES 256, RSA 2048, austauschbare Java-Krypto-Library	AES 256	AES 256	AES 256	AES 128, AES 256	AES 256	AES 256
unterstützte Cloud-Dienste (Dropbox, OneDrive, iCloud ...)	Box, Office 365, SharePoint, OneDrive, Dropbox, Google	Dropbox, OneDrive, iCloud, Amazon AWS, Microsoft Azure, SoftLayer, IBM Bluemix, Telekom, Dienste, die über offene Schnittstellen kommunizieren	Amazon Cloud, Bitcasa, Box, Dropbox, Google Drive, SkyDrive	Dropbox, Box, OneDrive (unterstützt durch Blue Coat Cloud Data Protection Policy Builder und Blue Coat DLP)	Box, Dropbox	alle Cloud-Anwendungen, auch viele proprietäre Web-anwendungen	Box, S3, weitere Plattformen in Kürze	Amazon Web Services (AWS), OpenStack (beta)
unterstützte SaaS-Anwendungen (Office 365, Salesforce.com ...)	Salesforce.com, Chatter, Force.com, SAP, Adobe und ServiceNow; außerdem kompatibel mit Anwendungen von Informatica, Apttus, Conga, Marketo, Servicemax, Dell Boomi, Castiron, Talend, Pardot, Avaya und anderen	Office 365, Salesforce.com, Success Factors, IBM Connections, Google Apps for Work, Kenexa sowie über den „eperi Analyzer" weitere SaaS-Anwendungen, die auf HTTP aufsetzen (z. B. Ajax oder JSON)	–	Salesforce.com, ServiceNow, Oracle Sales & CRM, Success-Factors, Office 365 Yammer; weitere SaaS-Clouds via Blue Coat Cloud Data Protection Policy Builder	Office 365 OneDrive for Business, Office 365 SharePoint, Office 365 Yammer, Salesforce.com, ServiceNow, Jive, Google Docs	Office 365, OneDrive, SharePoint, Dynamics, Yammer, NetSuite, SugarCRM, Salesforce.com, Evernote, Freshbooks, Confluence, JIRA und Inhouse-Anwendungen	–	–
unterstützte Hardware-Security-Module (HSMs)	alle KMIP-kompatiblen (Key Management Interoperability Protocol) HSM, einschließlich SafeNet	Utimaco, Thales	–	SafeNet, Thales	jedes KMIP-kompatible HSM, beispielsweise SafeNet Key-Secure	Thales, SafeNet	Vormetric-eigener DSM (Data Security Manager)	–
Sicherheitszertifizierungen (z. B. FIPS-140)	FIPS-140-2 Evaluierung der Verschlüsselungstechnik, Evaluierung durch Coalfire (unabhängiger IT-Auditierungs- und Compliance-Anbieter)	FIPS-140-2 über eigene Algorithmen, Grundschutz-Baustein des BSI	FIPS-140-2	unterstützt Nutzung von FIPS 140-2-Modulen (vollständig betrieben im FIPS-Modus); Tokenisierungsmethode durch Drittanbieter evaluiert	FIPS-140-2, ISO 27001, US-EU Safe Harbor, CSA STAR (Cloud Security Alliance), TRUSTe (True Ultimate Standards Everywhere)	FIPS-140-2 (über HSM und NSS (Network Security Services)	DSM ist nach FIPS 140-2 Level-3-zertifiziert.	–
Tokenisierung	✓	✓	–	✓	✓	–	✓ (eigenständiges Produkt)	–
spezielle Verschlüsselungsfunktionen (z. B. partielle, formaterhaltende, operationserhaltende Verschlüsselung)	durchsuchbare starke Verschlüsselung und Tokenisierung (komplexe Suche nach Sprache und booleschen Ausdrücken durch zwischengespeicherten Suchindex auf dem Gateway) / formaterhaltende, längenerhaltende, funktionserhaltende Verschlüsselung	✓	–	✓, kritische Cloud-Operationen und -Funktionen bleiben erhalten, ohne Notwendigkeit zur Nutzung spezieller proprietärer Verschlüsselungsschemata	selektive Verschlüsselung auf Feldebene oder über DLP-Policy / durchsuchbare, formaterhaltende, reihenfolgeerhaltende Verschlüsselung / Wildcard-Suche / Verschlüsselung mit Komprimierung / formaterhaltende Tokenisierung	verschiedene Mechanismen der formaterhaltenden Verschlüsselung für unterschiedliche Anwendungszwecke (Längen-, Alphabet- und Zahlentreue) / selektive Feld- und Anhangverschlüsselung	Dateiformat wird beibehalten, nur Inhalt der Dateien wird verschlüsselt (MetaClear encryption)	–
Möglichkeiten zur Schlüsselverwaltung (z. B. eigener Schlüssel für jeden Anwender, ein Schlüssel pro Anwendergruppe)	regelmäßiger Schlüsselwechsel / Schlüsselaufteilung / beschränkte Gültigkeitsdauer für Schlüssel / Nutzung eines externen HSM / verschlüsselte Schlüsselablage	eigener Schlüssel für Anwender / ein Schlüssel pro Anwendergruppe, einer pro Datenfeld / Schlüsselrotation / Schlüsselverwaltung unabhängig von Datenbank oder Applikation / unternehmensinterne Zertifizierungsstelle / externes Trust Center / HSM	gemeinsamer Schlüssel für ein Team oder separater Schlüssel für jeden Benutzer	vollständiges Spektrum an Schlüssel-Management-Optionen, außerdem Nutzung von Schlüssel-Management-Systeme von Drittanbietern / Kunde hat Kontrolle über Tokentransfer und Verschlüsselung	ein Schlüssel pro Organisation / Möglichkeit, für Organisationseinheiten eigene Schlüssel festzulegen	Schlüsselgenerierung zur Installationszeit, alternativ können Administratoren eigenen Schlüssel einsetzen. Speicherung der Schlüssel in einem HSM oder einer verschlüsselten Datei.	Kunde definiert, wo er seine Schlüssel-Server (Vormetric DSM) implementieren möchte / umfangreiche Schlüssel-Management-Optionen, Rechtetrennung, Mandantenfähigkeit usw.	eigener Schlüssel für jeden Benutzer
Gateway-Hosting beim Anbieter möglich	Hosting bei Drittanbietern	✓, als Dienstleistungen bei Kunden on Premise, bei Drittanbietern, über Cloud-Anbieter wie IBM und Microsoft	–	✓, auch bei Partnern wie T-Systems oder Tech Mahindra	✓, über verschiedene Rechenzentren in den USA, Europa und Australien	✓	–	✓
zusätzliche Funktionen des Produkts (Logdaten-Erfassung, Policys, Data Loss Prevention (DLP) ...)	Visibilität / Monitoring der Anwenderaktivitäten / Entdeckung und Analyse von Anomalien / Data Loss Prevention (eigenständig und mit anderen DLP-Systemen) / nichtlinientreue Überwachung des internen und externen File Sharing / Cloud Discovery (Nutzungsanalyse und Evaluierung der Risiken)	Policys (konfigurierbare Sicherheitsregeln, Templates) / Element Protection (Erkennung von Manipulation durch nicht berechtigte Administratoren) / standardkonforme Verschlüsselung von XML, SOAP (XML-Encryption, WS-Security) / (Cloud-)Single Sign-on / serviceorientierte Architektur, erweiter-/änderbar über SOAP-over-HTTP-Schnittstelle	verschlüsselte Dateinamen / optionale Zwei-Faktor-Authentifizierung / Abwehr von Brute-Force-Attacken / Logdaten-erfassung	Cloud-Visibilität und Risikoanalyse / Logdatenerfassung für Auditierung und Compliance / Malware-Analyse und Data Loss Prevention / Cloud-Zugangskontrolle	Logdatenerfassung / Anomalieerkennung / DLP, auch Drittanbieter / Kollaborationskontrolle / On-Demand-Scans in der Cloud / Management von Regelverstößen / kontextabhängige Zugangskontrolle für Geräte / Berücksichtigung der geografischen Position in Richtlinien / Anwenderverhaltensanalyse / SSO-Integration	Visibilität / Einbinden anderer Kryptoanwendungen über ein SDK / Monitoring und Analyse / Anwenderüberwachung, Vergleich mit früherem Verhalten / konfigurierbare DLP-Maßnahmen (Data Loss Prevention) für Anwendungen, Nutzergruppe oder Plattform / Anomalieerkennung	Verschlüsselungs-Suite mit Datei- und Verzeichnisverschlüsselung (on Premise oder in der Cloud) / Anwendungsverschlüsselung / Tokenisierung über API / Schlüssel-Server (KMIP-kompatibel, Oracle- und Microsoft-TDE-Schlüssel-Management, frei nutzbarer Schlüssel-Server)	verschlüsselter Datentransport / Policys für Cloud- und Datenzugang / Multi-Cloud-Unterstützung (auch bei verschiedenen Anbietern) / Cloud-Instanz-Härtung / wiederverwendbare Cloud-Templates / Cloud-Anpassung über Scripting / SSH-Client (browserbasiert)
weitere Besonderheiten des Produkts	zentralisiertes Management über mehrere Cloud-Anwendungen hinweg / Daten werden für die Verarbeitung entund wieder verschlüsselt / Verschlüsselung von Dokumenten und Anhängen / Malware-Scans des gesamten Datenverkehrs / unbegrenzte Skalierbarkeit / Gateway- und API-Unterstützung, Optionen für Inline-Schutz und Out-of-Band-Scanning / Unterstützung mobiler Clients / div. Compliance-Templates	Security made in Germany, ohne Patriot-Act-Offenlegungspflicht / Basis ist unter Open-Source-Lizenz veröffentlicht, dadurch Prüfbarkeit der Sicherheit und Hintertürenfreiheit sowie Erweiterungsmöglichkeiten / integrierte Zertifizierungsstelle und PKI / austauschbare Krypto-Algorithmen / Unterstützung von Suchfunktionen in SaaS-Anwendungen	unterstützt auch die Verschlüsselung lokaler Verzeichnisse	optionale Integration in Blue Coat ProxySG7 Secure Web Gateway	Teil einer Plattform zur sicheren Cloud-Nutzung / patentierte Architektur, mit Integration von Single Sign-on und Cloud-Serviceproviders, gesamter Funktionsumfang ohne Agentsoftware, Pac-Dateien, ein VPN oder einen weiteren Proxyserver verfügbar / Reverse Proxy Mode und API-Integration	Single-Sign-on- und Active-Directory-Unterstützung transparent für Anwender / unendlich skalierbar / keine Latenzzeit / einfache Konfiguration über XML-Dateien / DLP und AV über ICAP / Malware- und Bot-Erkennung / Device-Fingerprinting / Anwenderaudit-ierung / Anwenderbefragung zur Zugangskontrolle	Verschlüsselungslösung mit einer zentralen Komponente und keine von Drittanbietern erworbenen, nicht miteinander kompatiblen Kryptografieprodukte	„wintermute.ai server" ist ein IaaS-Security-Gateway und Cloud Broker / automatisches Ver- und Entschlüsseln von EBS Storage Volumes mit beliebigem Inhalt / Schlüsselverwaltung / gesicherte Datenübertragung / weitere Funktionen, die über Cloud-Verschlüsselung hinausgehen

Die Tabelle beruht auf den Angaben der Hersteller. ✓ ja/vorhanden/trifft zu; – nein/nicht vorhanden/trifft nicht zu

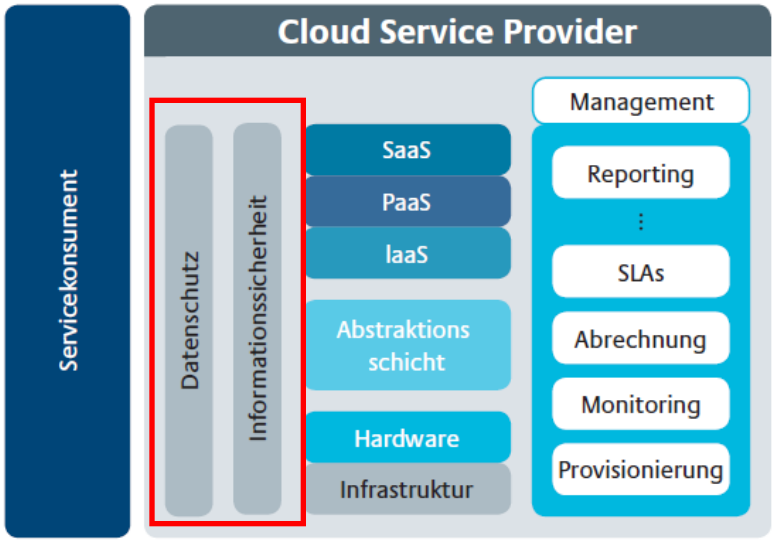
Was kann man Unternehmen raten ?

- **16 %** der mittelständische Unternehmen setzen derzeit Cloud Dienste ein
  - **19 %** davon kennen die Sicherheitsanforderungen und rechtlichen Rahmenbedingungen nicht
  - **42 %** kennen sie teilweise.

➔ **Fast 2/3** der Cloud-Anwender lassen ihre Daten unter teils ungeklärten Bedingungen verarbeiten

** Quelle: http://heise.de/-1816308*

Sicherheit + Datenschutz



- Gewährleistung einer angemessenen IT-Sicherheit
- Verlust von Einwirkungs- und Kontrollmöglichkeiten
- Compliance / Verantwortlichkeit

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

- Transparenz über die technischen, organisatorischen und rechtlichen Rahmenbedingungen
- verlässliches IT-Sicherheits- und Datenschutzkonzept
- Vereinbarungen zum Ort der Datenverarbeitung und zur Benachrichtigung bei geplanten Veränderungen
- Kontroll- und Einwirkungsmöglichkeiten der Cloud-Nutzerinnen und -Nutzer
- Regelungen zur Umsetzung von Auskunftsansprüchen Betroffener und zur Datenlöschung
- aussagekräftige Nachweise (z.B. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen)

Orientierungshilfe Cloud Computing:
http://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf

Bedeutung Cloud Computing

Deutschland sicher im Netz e.V.

Gemeinsam für mehr IT-Sicherheit

DsiN-Cloud-Scout

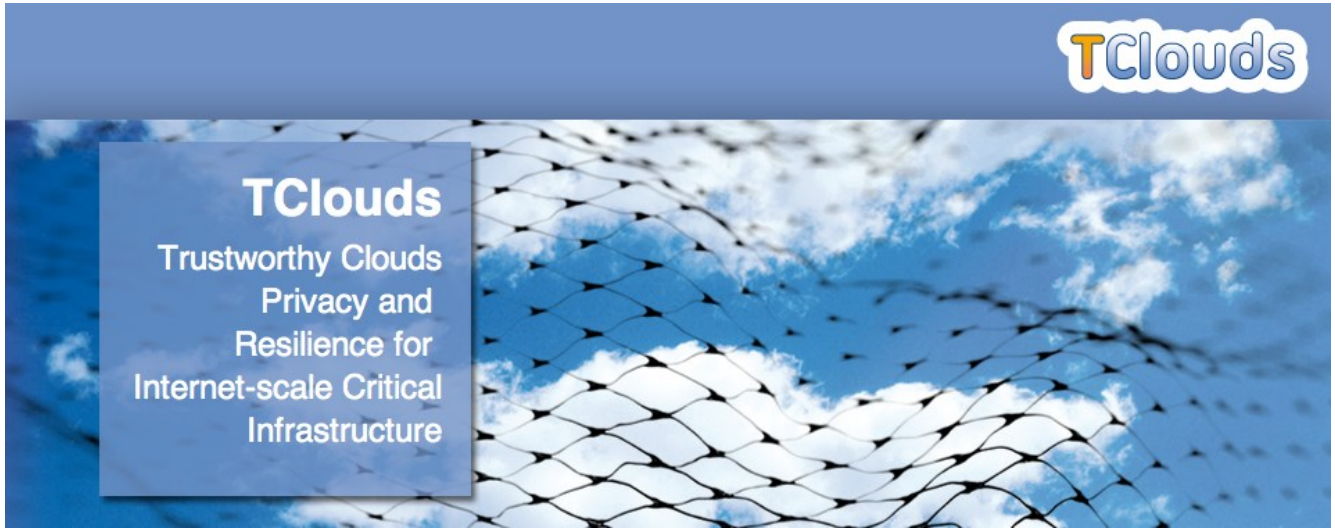
Cloud Computing sicher nutzen

DsiN unterstützt vor allem kleine und mittelständische Unternehmen, die IT-Sicherheitsvorteile von Cloud Computing zu nutzen und Schwachstellen zu vermeiden. Mit dem DsiN-Cloud-Scout erfahren Sie in 10-15 Minuten, in welcher Weise Sie Cloud Computing sicher für Ihr Unternehmen nutzen und dadurch sogar die Informationssicherheit in Ihrem Unternehmen verbessern können.

https://www.sicher-im-netz.de/unternehmen/DsiN-Cloud-Scout.aspx

TClouds-Projekt 2010-2013
Cloud Computing, angereichert mit einer Prise Vertrauen

Prototypische Entwicklung einer vertrauenswürdigen Cloud-Infrastruktur, die den europäischen Datenschutzanforderungen entspricht.



www.tclouds-project.eu/

Vertrauenswürdige Cloud Services für die Wirtschaft

http://rechtsinformatik.saarland/images/trustedcloud/pdf/TCDP_v0.9.pdf

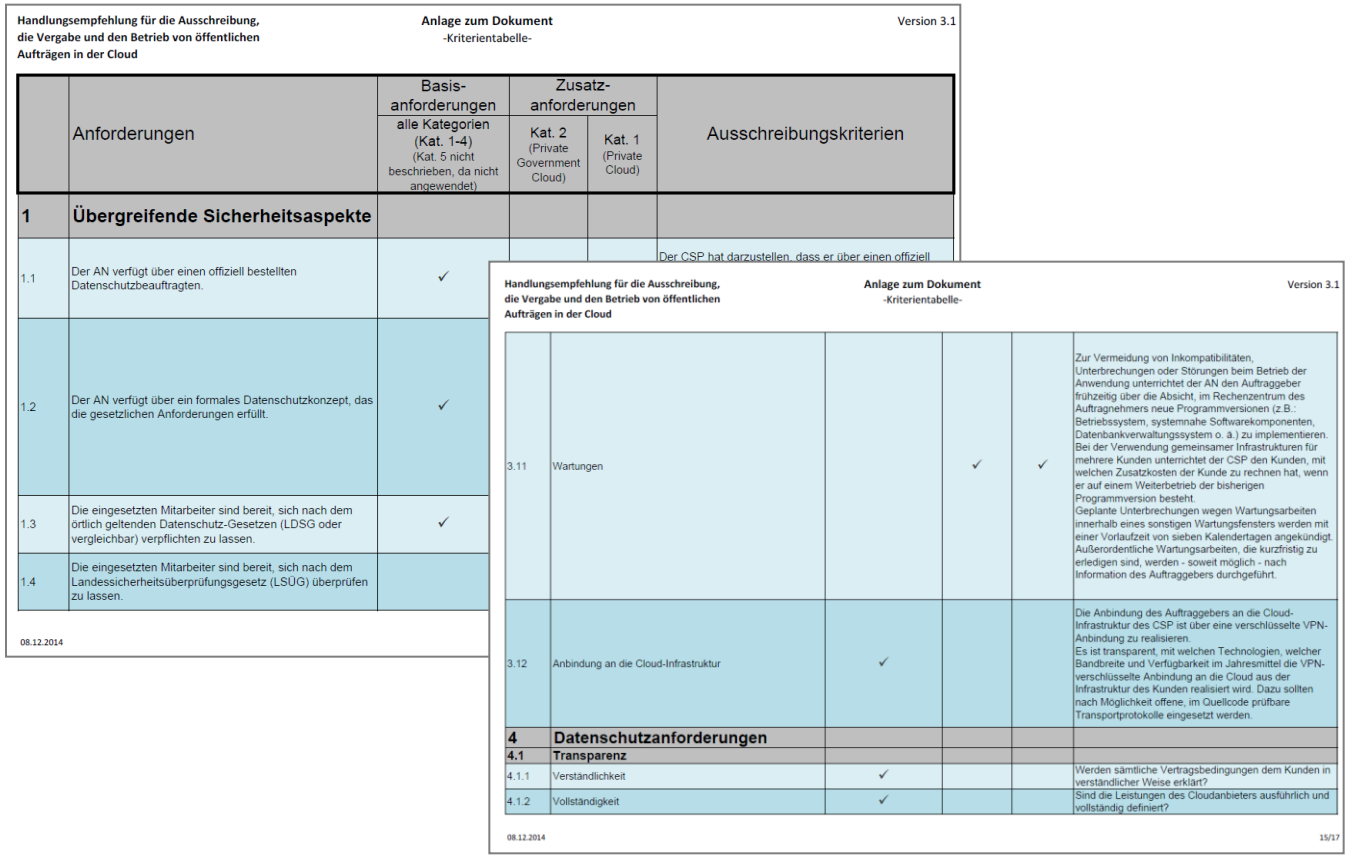
http://s.rlp.de/w6O

Aspekte bei der Auswahl von Cloud-Lösungen

Schutzbedarf	**Kategorie 1**: Private Cloud	**Kategorie 2**: National/European Private Government Cloud	**Kategorie 3**: Managed Cloud (deutsches Recht)	**Kategorie 4**: Public Cloud (europäisches Recht)
normal	X	X	X	X*)
hoch	X	X		
sehr hoch	X			

*) *Anmerkung: Die Verarbeitung von Daten mit normalem Schutzbedarf in einer Public Cloud (Kategorie 4) ist besonders kritisch zu prüfen und kann nicht generell vorgesehen werden. Eine Verarbeitung ist nur dann akzeptabel, wenn es sich um Daten ohne Vertraulichkeitsanforderungen handelt.*

Handlungsempfehlungen für Ausschreibung, Vergabe und Betrieb von Cloud-Leistungen



Handlungsempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud

Anlage zum Dokument
-Kriterientabelle-

Version 3.1

	Anforderungen	Basis-anforderungen	Zusatz-anforderungen		Ausschreibungskriterien
		alle Kategorien (Kat. 1-4) (Kat. 5 nicht beschrieben, da nicht angewendet)	Kat. 2 (Private Government Cloud)	Kat. 1 (Private Cloud)	
1	**Übergreifende Sicherheitsaspekte**				
1.1	Der AN verfügt über einen offiziell bestellten Datenschutzbeauftragten.	✓			Der CSP hat darzustellen, dass er über einen offiziell
1.2	Der AN verfügt über ein formales Datenschutzkonzept, das die gesetzlichen Anforderungen erfüllt.	✓			
1.3	Die eingesetzten Mitarbeiter sind bereit, sich nach dem örtlich geltenden Datenschutz-Gesetzen (LDSG oder vergleichbar) verpflichten zu lassen.	✓			
1.4	Die eingesetzten Mitarbeiter sind bereit, sich nach dem Landessicherheitsüberprüfungsgesetz (LSÜG) überprüfen zu lassen.				

08.12.2014

Handlungsempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud

Anlage zum Dokument
-Kriterientabelle-

Version 3.1

3.11	Wartungen		✓	✓	Zur Vermeidung von Inkompatibilitäten, Unterbrechungen oder Störungen beim Betrieb der Anwendung unterrichtet der AN den Auftraggeber frühzeitig über die Absicht, im Rechenzentrum des Auftragnehmers neue Programmversionen (z.B.: Betriebssystem, systemnahe Softwarekomponenten, Datenbankverwaltungssystem o. ä.) zu implementieren. Bei der Verwendung gemeinsamer Infrastrukturen für mehrere Kunden unterrichtet der CSP den Kunden, mit welchen Zusatzkosten der Kunde zu rechnen hat, wenn er auf einem Weiterbetrieb der bisherigen Programmversion besteht. Geplante Unterbrechungen wegen Wartungsarbeiten innerhalb eines sonstigen Wartungsfensters werden mit einer Vorlaufzeit von sieben Kalendertagen angekündigt. Außerordentliche Wartungsarbeiten, die kurzfristig zu erledigen sind, werden - soweit möglich - nach Information des Auftraggebers durchgeführt.
3.12	Anbindung an die Cloud-Infrastruktur	✓			Die Anbindung des Auftraggebers an die Cloud-Infrastruktur des CSP ist über eine verschlüsselte VPN-Anbindung zu realisieren. Es ist transparent, mit welchen Technologien, welcher Bandbreite und Verfügbarkeit im Jahresmittel die VPN-verschlüsselte Anbindung an die Cloud aus der Infrastruktur des Kunden realisiert wird. Dazu sollten nach Möglichkeit offene, im Quellcode prüfbare Transportprotokolle eingesetzt werden.
4	**Datenschutzanforderungen**				
4.1	**Transparenz**				
4.1.1	Verständlichkeit	✓			Werden sämtliche Vertragsbedingungen dem Kunden in verständlicher Weise erklärt?
4.1.2	Vollständigkeit	✓			Sind die Leistungen des Cloudanbieters ausführlich und vollständig definiert?

08.12.2014 15/17

http://s.rlp.de/gkP

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

www.datenschutz.rlp.de | poststelle@datenschutz.rlp.de

Helmut Eiermann
Gruppenleiter Technik
Hintere Bleiche 34 | 55116 Mainz
Tel (06131) 208 2226
Fax (06131) 208 2497
h.eiermann@datenschutz.rlp.de