skyhigh

EU & EEA Data Protection - and The Cloud

September 2015

Nigel Hawthorn, Skyhigh Networks
nigel@skyhighnetworks.com
@wheresnigel
+44 7801 487987

Data Equipment

Can Cloud & Data Protection Be friends?

Introductions and Agenda

- The Cloud Dilemma
- Cloud Risk Report – Europe
- Some Nordic Data
- Local Data Protection Authorities
- EU Data Protection
  - –Today’s Directive
  - –Tomorrow’s Regulation
- Recommendations

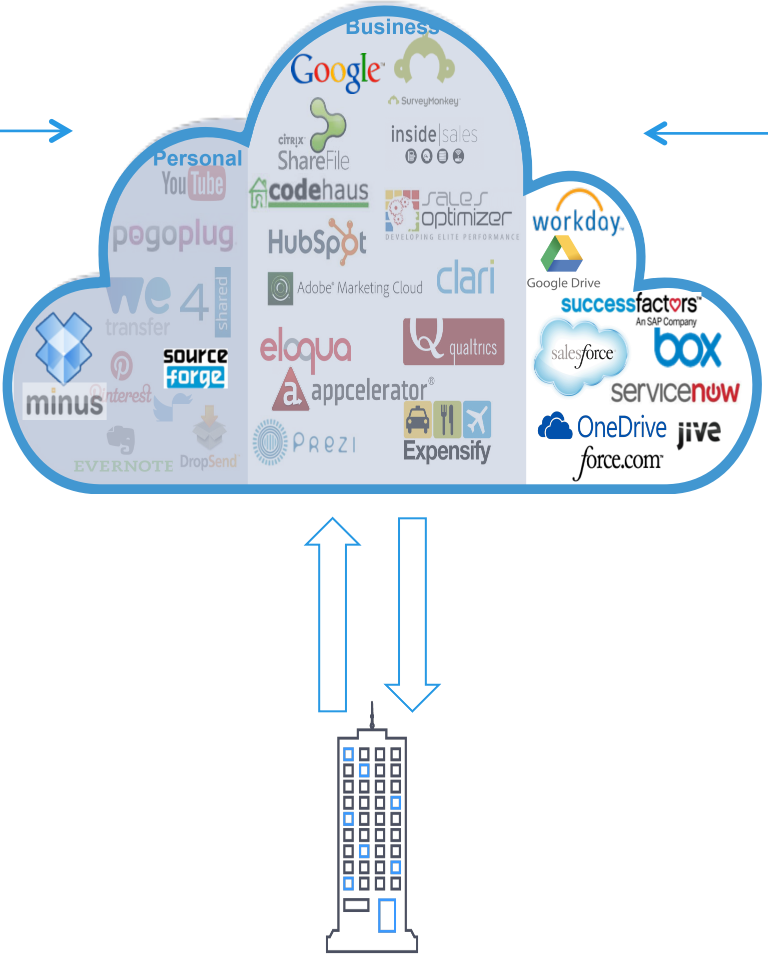
Data Equipment

skyhigh

The Cloud Dilemma

Shadow IT →

← Sanctioned IT



VISIBILITY: Understand services in demand. Quickly respond to requests from users.

RISK MANAGEMENT: Understand risk to business. Comply with corporate policies & Data Protection Laws

THREAT DETECTION: Identify exfiltration events indicating security breaches.

DATA SECURITY: Protect data from breaches and blind subpoenas.

COMPLIANCE: Comply with regulatory requirements. Enforce governance policies.

ENTERPRISE SECURITY: Detect and prevent compromised accounts and insider threats.

Data Equipment

skyhigh

CLOUD ADOPTION & RISK IN EUROPE REPORT

Q2 2015

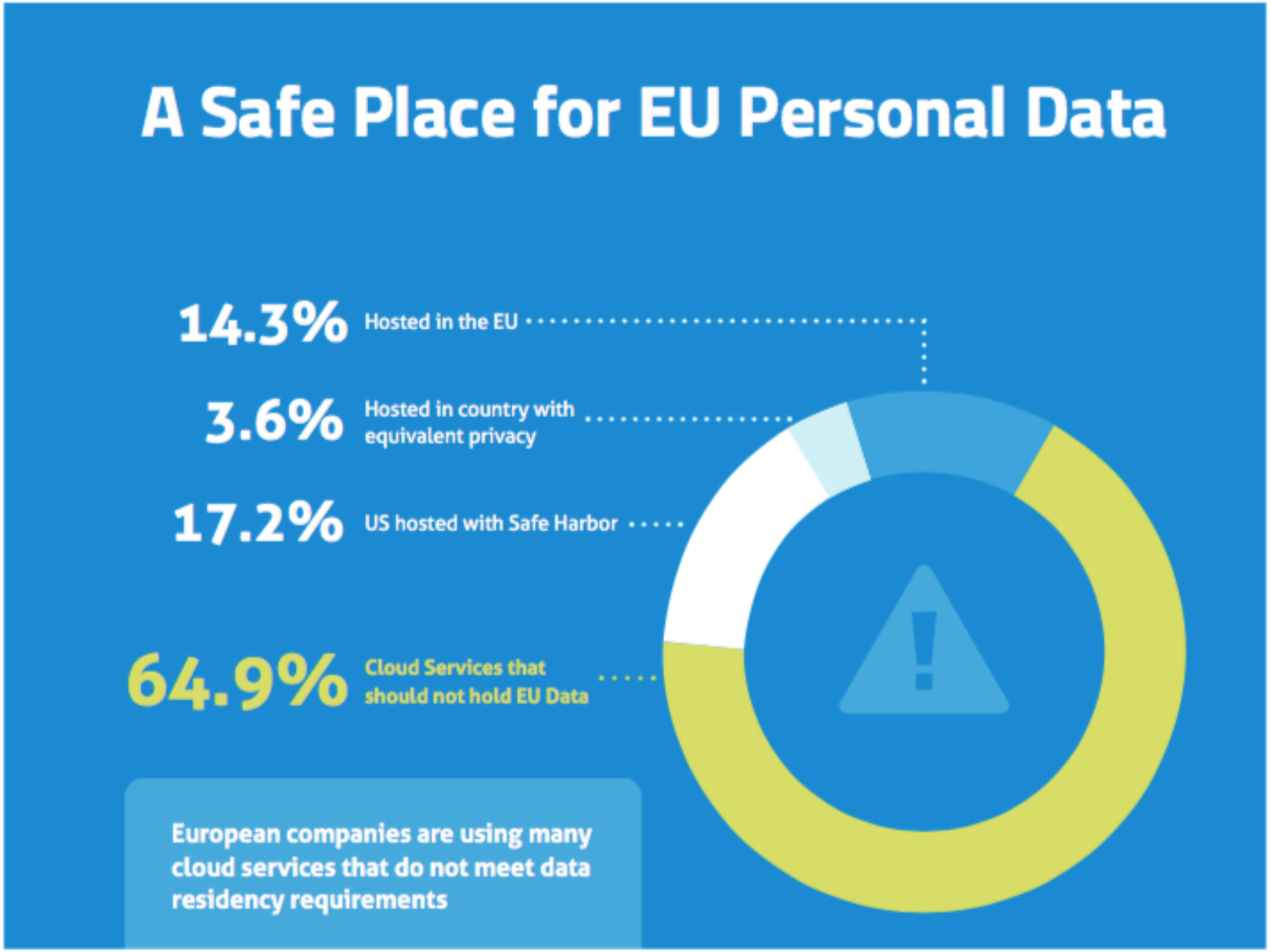
Published Q3 2015

skyhigh

Data Equipment

skyhigh

AVERAGE NUMBER OF CLOUD SERVICES IN USE BY EUROPEAN ORGANIZATIONS



A Safe Place for EU Personal Data

14.3% Hosted in the EU

3.6% Hosted in country with equivalent privacy

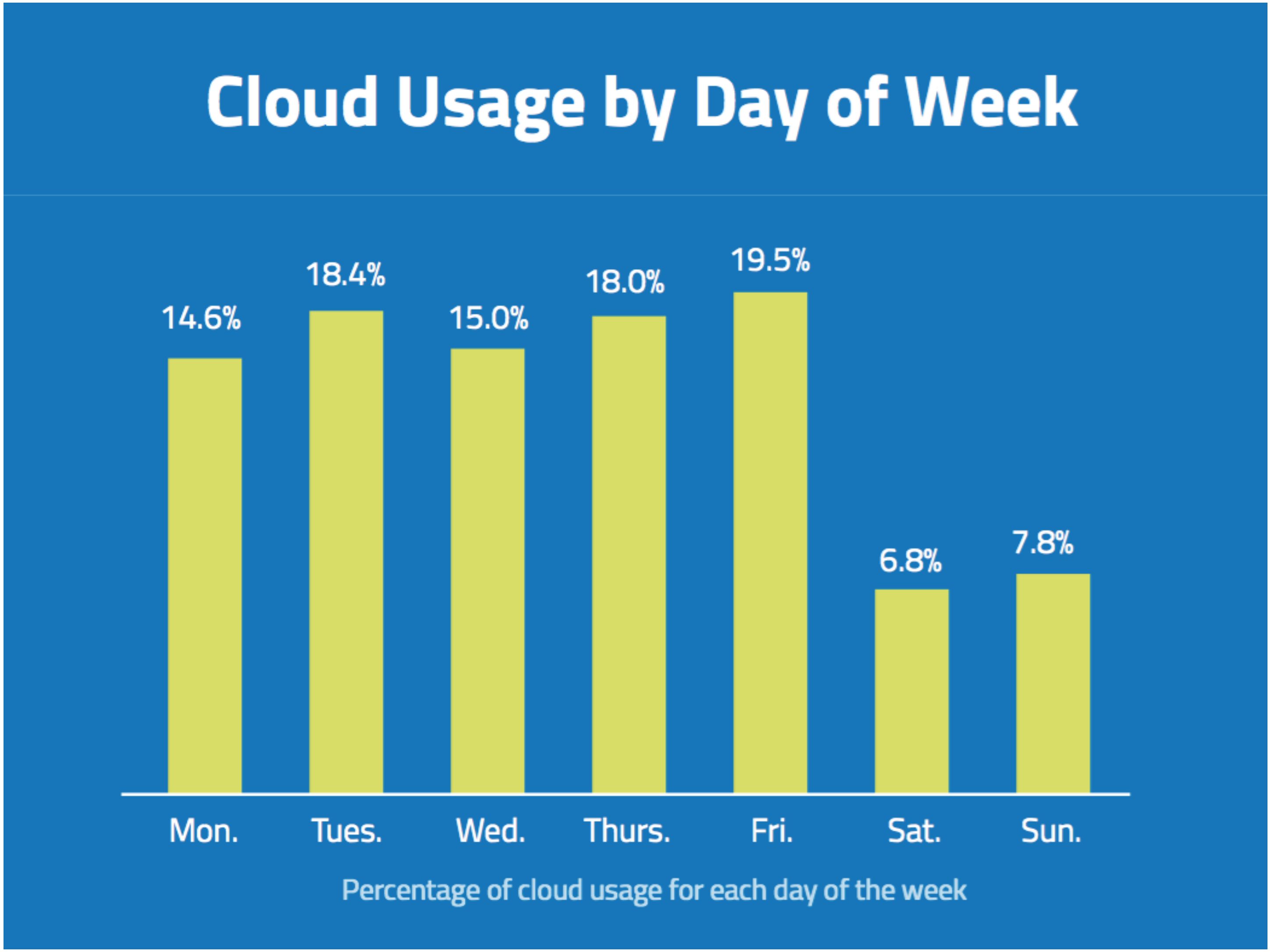
17.2% US hosted with Safe Harbor

64.9% Cloud Services that should not hold EU Data

European companies are using many cloud services that do not meet data residency requirements

Data Equipment

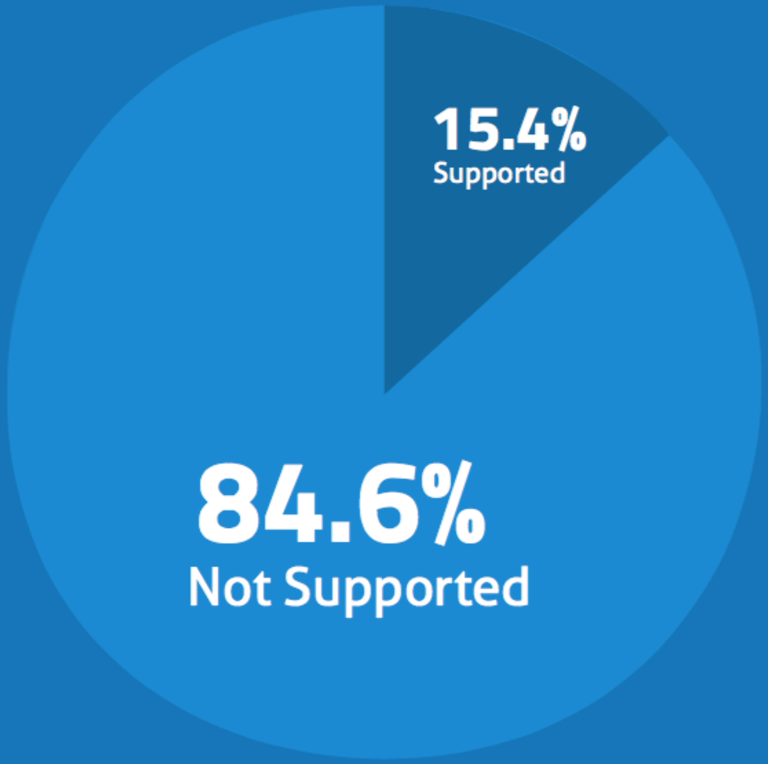
skyhigh



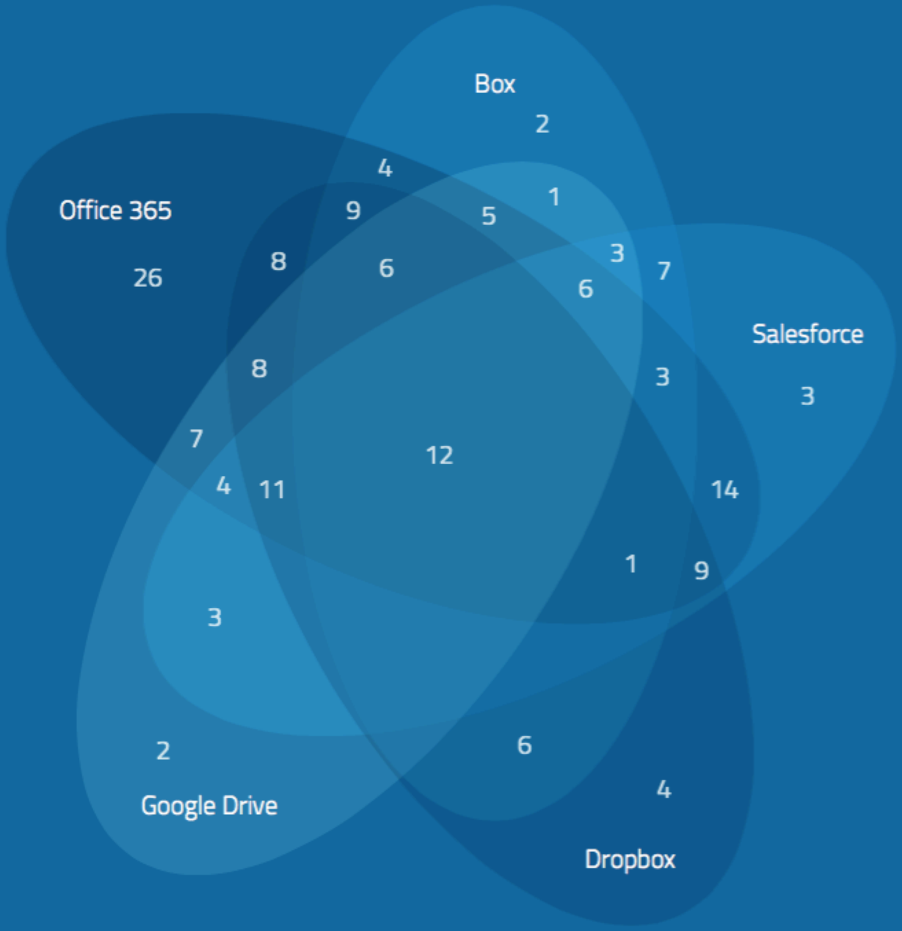
Data Equipment

skyhigh

SUPPORT FOR MULTI-FACTOR AUTHENTICATION REMAINS LOW

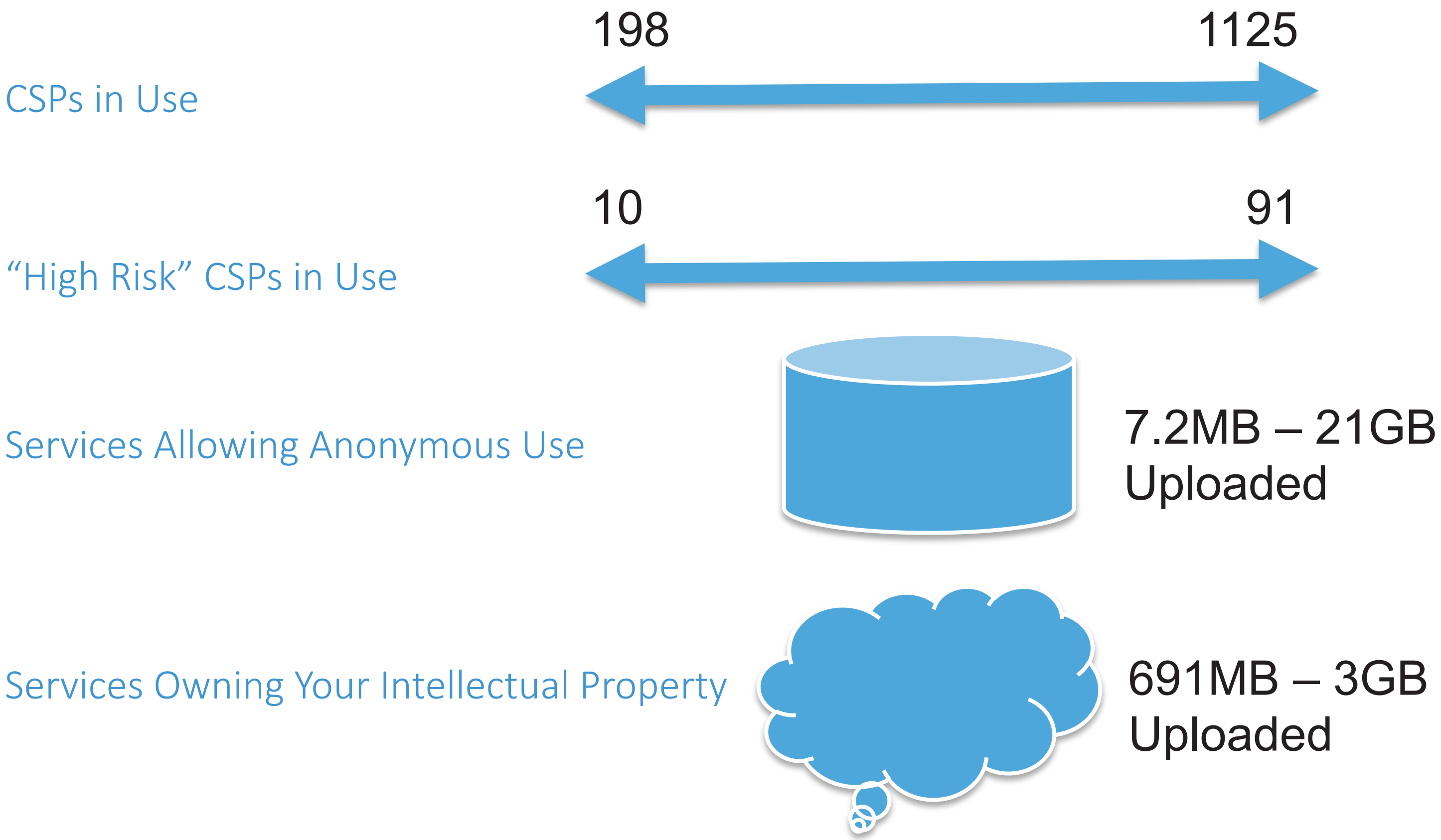


CLOUD USAGE IS NOT UNIFORM ACROSS USERS



skyhigh

Nordic Customer Results



CSPs in Use

198

1125

"High Risk" CSPs in Use

10

91

Services Allowing Anonymous Use

7.2MB – 21GB Uploaded

Services Owning Your Intellectual Property

691MB – 3GB Uploaded

PDF Converters	100%
Inconsistent Policies	100%

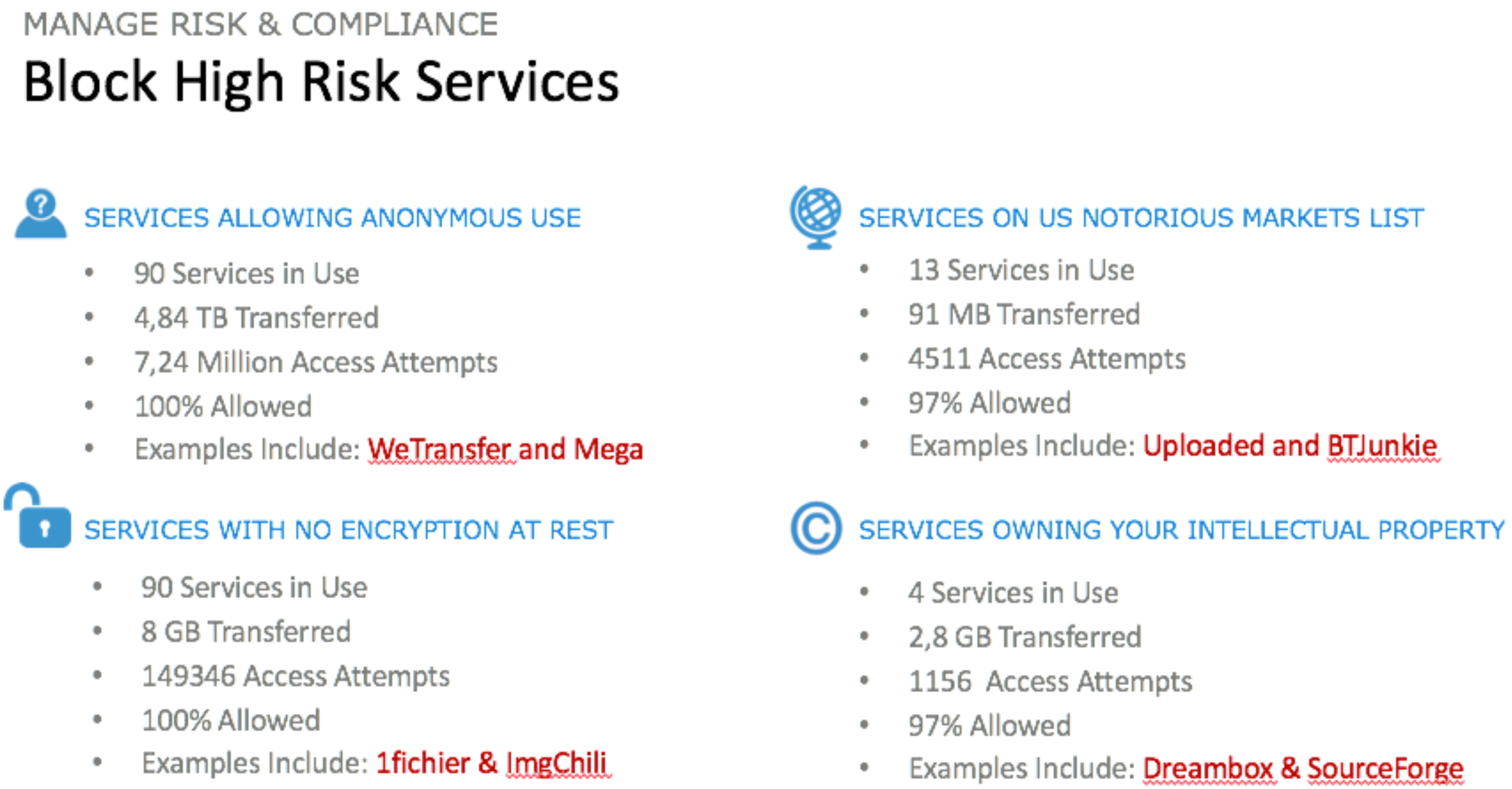
Data Equipment

skyhigh

Specific Example Findings - Nordic

- 413 cloud services with inconsistent blocking policies
- 56 Different cloud storage services in use
  - 18 of them high risk
- 499 Users of Prezi, though its not a supported service
- 185 services with unknown legal jurisdiction
- 8.4 TB of data uploaded to 152.115.57.233 by one user
- 41,000 requests to Fitbit in one day from one machine – infected?

Real Nordic Assessment



MANAGE RISK & COMPLIANCE

Block High Risk Services

SERVICES ALLOWING ANONYMOUS USE

- 90 Services in Use
- 4,84 TB Transferred
- 7,24 Million Access Attempts
- 100% Allowed
- Examples Include: WeTransfer and Mega

SERVICES ON US NOTORIOUS MARKETS LIST

- 13 Services in Use
- 91 MB Transferred
- 4511 Access Attempts
- 97% Allowed
- Examples Include: Uploaded and BTJunkie

SERVICES WITH NO ENCRYPTION AT REST

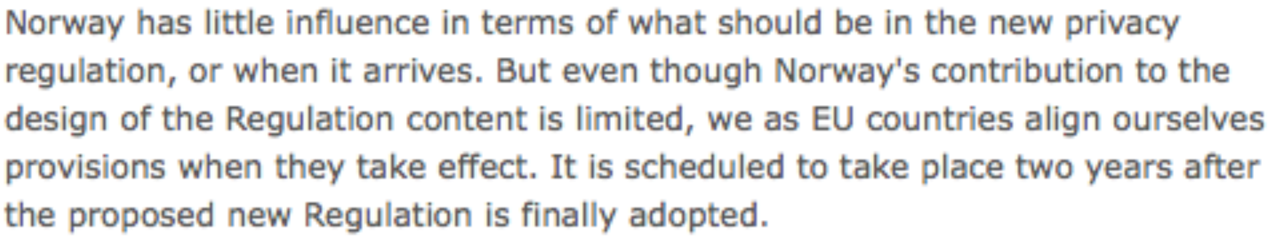
- 90 Services in Use
- 8 GB Transferred
- 149346 Access Attempts
- 100% Allowed
- Examples Include: 1fichier & ImgChili

SERVICES OWNING YOUR INTELLECTUAL PROPERTY

- 4 Services in Use
- 2,8 GB Transferred
- 1156 Access Attempts
- 97% Allowed
- Examples Include: Dreambox & SourceForge

Data Protection – Ever More Important

- 1995 – EU Data Protection Directive Published
  - Each of the 28 EU countries adopt into national legislation
  - Variations in exact laws, rigor and enforcement
- 2011 – Norway Published Data Processor Agreement Guide.
- Today – EU is Negotiating a New General Data Protection Regulation
  - Deadline December 31st 2015
  - Implement within two years



Norway has little influence in terms of what should be in the new privacy regulation, or when it arrives. But even though Norway's contribution to the design of the Regulation content is limited, we as EU countries align ourselves provisions when they take effect. It is scheduled to take place two years after the proposed new Regulation is finally adopted.

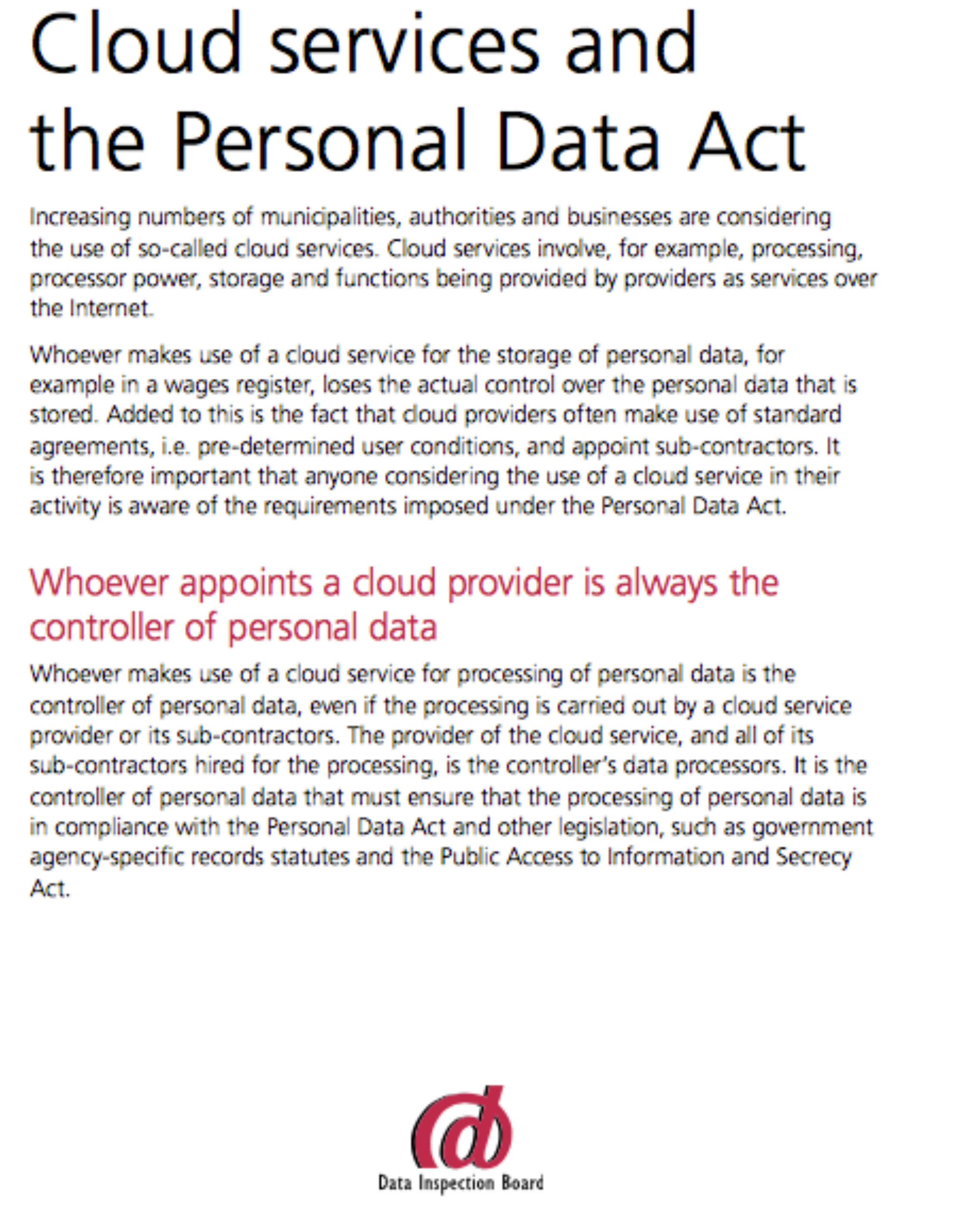
Get To Know Your Data Protection Authority

- http://www.datainspektionen.se
- https://www.datatilsynet.no
- http://www.tietosuoja.fi
- http://www.datatilsynet.dk

skyhigh

Swed

http://www dservices.pdf



Cloud services and the Personal Data Act

Increasing numbers of municipalities, authorities and businesses are considering the use of so-called cloud services. Cloud services involve, for example, processing, processor power, storage and functions being provided by providers as services over the Internet.

Whoever makes use of a cloud service for the storage of personal data, for example in a wages register, loses the actual control over the personal data that is stored. Added to this is the fact that cloud providers often make use of standard agreements, i.e. pre-determined user conditions, and appoint sub-contractors. It is therefore important that anyone considering the use of a cloud service in their activity is aware of the requirements imposed under the Personal Data Act.

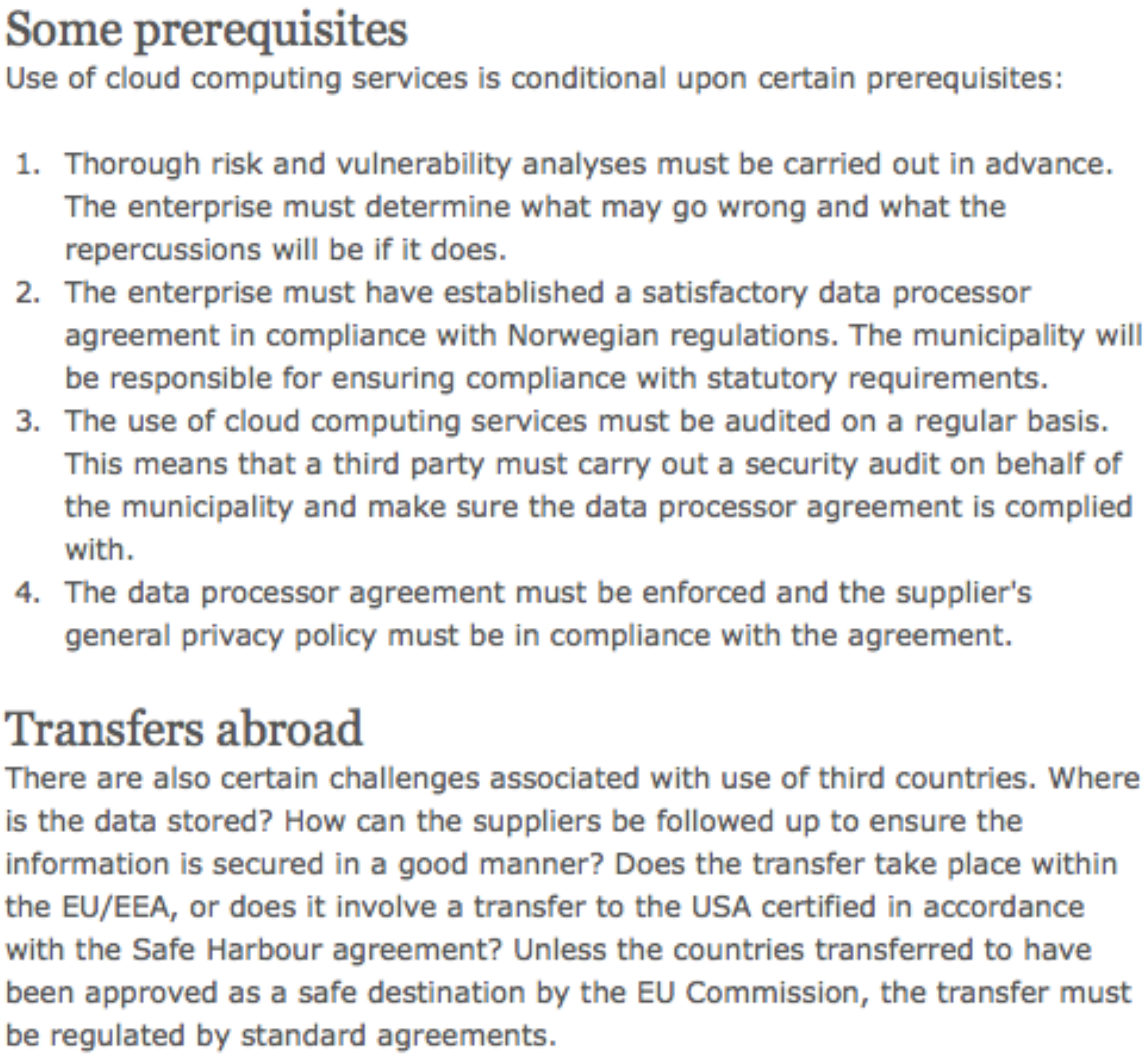
Whoever appoints a cloud provider is always the controller of personal data

Whoever makes use of a cloud service for processing of personal data is the controller of personal data, even if the processing is carried out by a cloud service provider or its sub-contractors. The provider of the cloud service, and all of its sub-contractors hired for the processing, is the controller's data processors. It is the controller of personal data that must ensure that the processing of personal data is in compliance with the Personal Data Act and other legislation, such as government agency-specific records statutes and the Public Access to Information and Secrecy Act.

Data Inspection Board

skyhigh

Norway: Narvik Request to Use Cloud Services



Some prerequisites

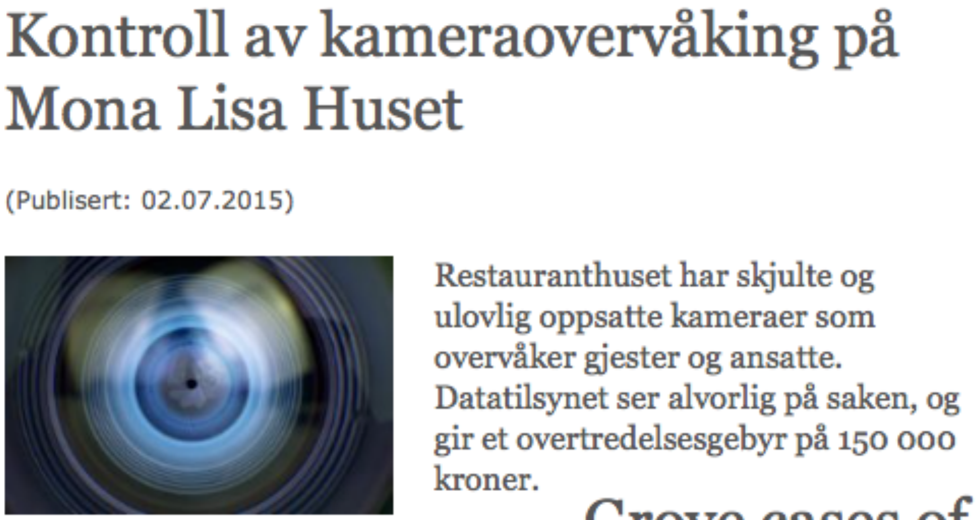
Use of cloud computing services is conditional upon certain prerequisites:

1. Thorough risk and vulnerability analyses must be carried out in advance. The enterprise must determine what may go wrong and what the repercussions will be if it does.
2. The enterprise must have established a satisfactory data processor agreement in compliance with Norwegian regulations. The municipality will be responsible for ensuring compliance with statutory requirements.
3. The use of cloud computing services must be audited on a regular basis. This means that a third party must carry out a security audit on behalf of the municipality and make sure the data processor agreement is complied with.
4. The data processor agreement must be enforced and the supplier's general privacy policy must be in compliance with the agreement.

Transfers abroad

There are also certain challenges associated with use of third countries. Where is the data stored? How can the suppliers be followed up to ensure the information is secured in a good manner? Does the transfer take place within the EU/EEA, or does it involve a transfer to the USA certified in accordance with the Safe Harbour agreement? Unless the countries transferred to have been approved as a safe destination by the EU Commission, the transfer must be regulated by standard agreements.

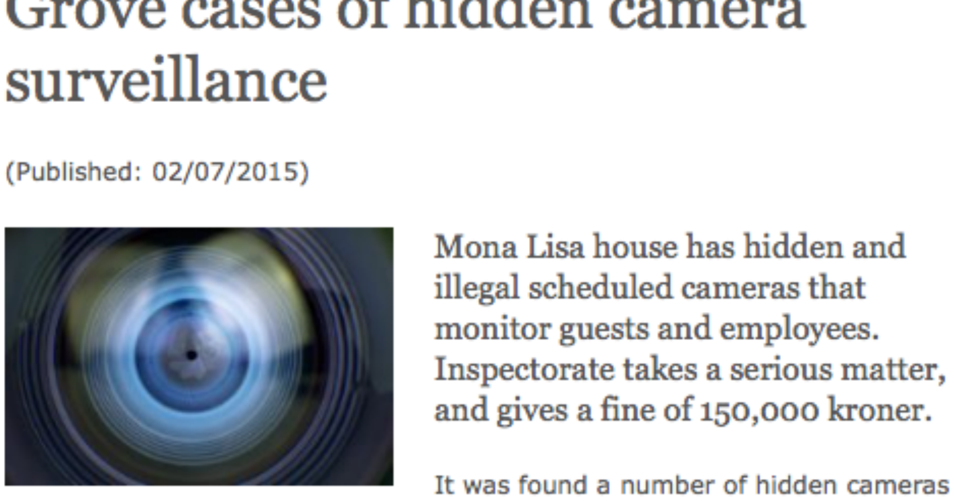
Fines Are Increasing



Kontroll av kameraovervåking på Mona Lisa Huset

(Publisert: 02.07.2015)

Restauranthuset har skjulte og ulovlig oppsatte kameraer som overvåker gjester og ansatte. Datatilsynet ser alvorlig på saken, og gir et overtredelsesgebyr på 150 000 kroner.



Grove cases of hidden camera surveillance

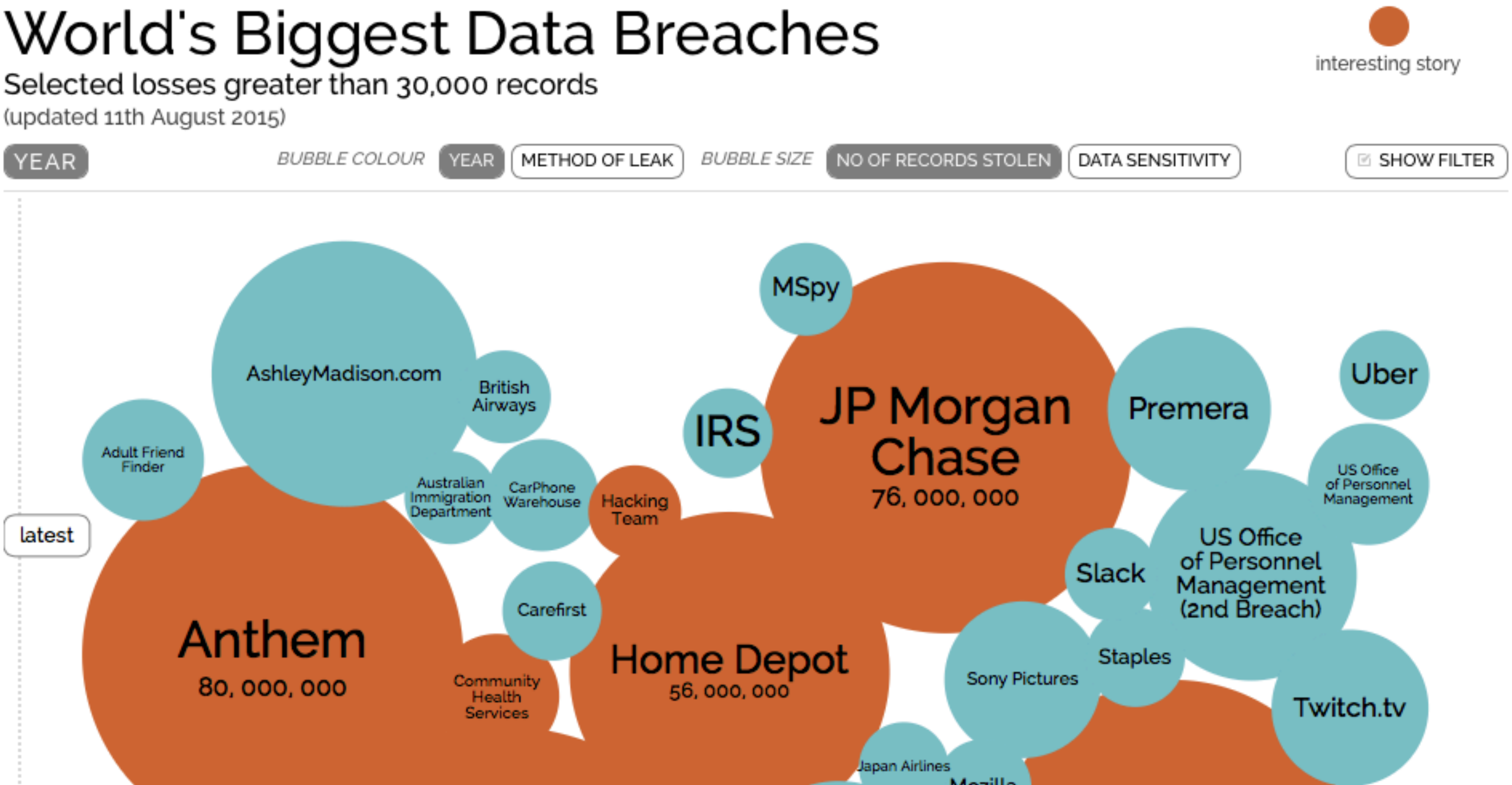
(Published: 02/07/2015)

Mona Lisa house has hidden and illegal scheduled cameras that monitor guests and employees. Inspectorate takes a serious matter, and gives a fine of 150,000 kroner.

It was found a number of hidden cameras

Information is Beautiful

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

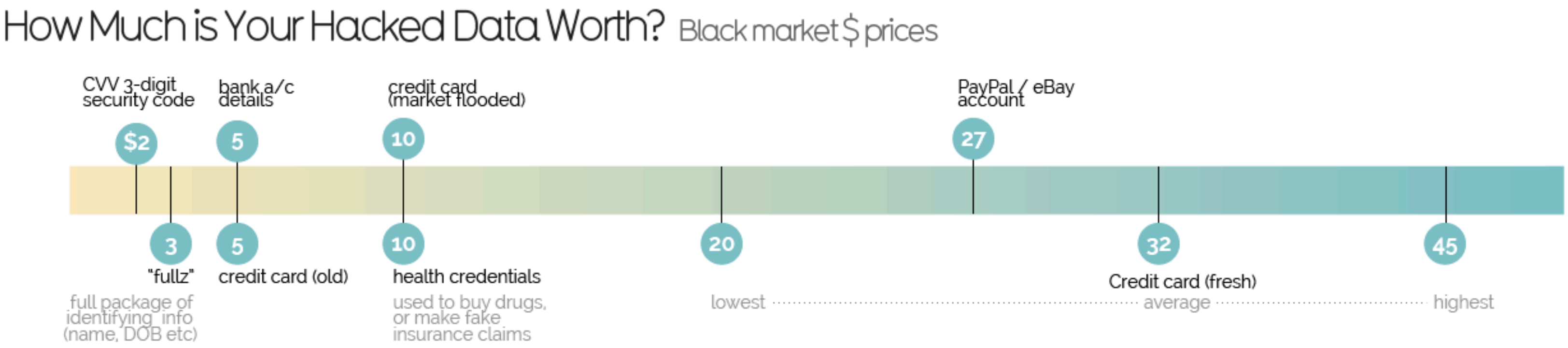


World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th August 2015)

How Much Is Data Worth



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

skyhigh

Definition of Personal Data

- Data “by which an individual can be identified”
- Not explicitly defined
  - Name
  - Address
  - Phone Number
  - Credit Card Number
  - Date of Birth
- What About?
  - Work Email Address?
  - IP Address of Computer?
  - Account Number or Code?

Recommendation: Assume all this (and more) are personal data

Key Principles

- Anyone in control of data is a Data Controller
- The Data Controller must register with their local body
- The Data Controller is responsible for all management of that data
- The Data Controller must keep the data secure
  - Technical, procedural, DC responsible for any outsourcer (such as cloud providers and 3rd parties)
- The data should only be used for the purpose it was originally collected

Recommendation: Review your data handling processes

The New Regulation

- Draft Available Now
- In final stages of negotiation, expect to be published soon, agreed by the end of the year & implemented in 2017
- Today's Draft
  - More prescriptive than directive
  - Heavier compliance burden on controllers
  - Impose new obligations on data processors (Eg. cloud providers)
  - Affect everyone with data on EU citizens (globally)
  - Tougher Sanctions
  - Common implementation across all 28 countries

Recommendation: Get advice on the implications for your business

The Right to Share Data

- Transparency
  - Inform User
  - Get Explicit Approval
- Must Meet Individual's "reasonable expectations"
- Tokenised Data
  - If data has been tokenised or pseudonymised, processing is presumed to meet the individual's reasonable expectations

Recommendation: Encrypt or tokenise data before uploading to the cloud - keeping the keys on-premise

Security – Widening Responsibility

- In today's Directive, only the data controller is officially responsible for data protection
- In the Regulation, this responsibility extends to the "Data Processor": 3rd parties, cloud providers
- Anyone who touches data on EU individuals, wherever they are based
- Recent 3rd Party Data Loss Examples: Target and TalkTalk

Recommendation: Confirm all cloud providers and all 3rd parties understand their responsibility

Recommendation: In your contract with cloud providers demand the right to inspect their procedures

Transferring Data Outside the EEA/EU

- The directive allows a data controller to decide if a 3rd party provider is safe.
- Under the regulation, only the commission can decide if a country is safe, a controller cannot decide
- US Safe Harbor is under scrutiny after the NSA revelations, though it is being more rigorously checked by US authorities so might not change
- More … long subject

Recommendation: Get visibility of the HQ country & data storage country of any provider

Individuals Access to Their Data

- Individuals can ask for their own data, each country defines how data controllers should respond (UK allows 40 days)
- In the new regulation, the deadline will be harmonised (proposed 20 days)
- Also users can demand erasure in the new regulation

Recommendation: Define your process to respond and erase – how do you erase from multiple data systems?

Informing Users & Authorities of Data Loss

- Different countries have different rules on data loss reporting for both the regulator and users
- The regulation is intended to harmonise; proposal of 72 hours to the regulator and users must be informed unless data was encrypted or tokenised

Recommendation: Define process and consider tokenising or encrypting data before uploading into the cloud.

Sanctions & Private Actions

- Each country has its own enforcement regulator
- Different enforcement, different policies on public "naming and shaming" and fines
- The Regulation will increase fines; proposal 2% - 5% of global turnover
- The Regulation allows users to claim damages, including collective redress

Recommendation: Ensure senior management understand the possible maximum fines

Risk Assessment

- Audit your current cloud services
- Look for risk factors
  - Data Risk (file sharing, encryption, keys …)
  - User Risk (anonymous use, enterprise identity, multi-factor auth …)
  - Service Risk (pen testing, known breaches …)
  - Business Risk (HQ country, data country, compliance …)
  - Legal Risk (IP ownership, dispute resolution, indemnity …)

Recommendation: Review today’s services in use, define acceptable services, train users & enforce

EU Data Protection – Primer Available

Whitepaper:

HOW EUROPEAN UNION DATA PROTECTION LEGISLATION AFFECTS YOUR DATA IN THE CLOUD

A primer for IT, security, compliance, and legal departments with a focus on the impact on cloud computing

"Enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs, and when combined with new digital business practices, can boost productivity, growth and jobs."

European Commission Communication on cloud computing strategy, September 2011

Brought to you by skyhigh DMH Stallard LLP

This paper features content that was published in the May 2014 edition of StrategicRISK 'Make IT Personal', authored by Anthony Lee, a partner at DMH Stallard. The content is reprinted with permission.

Data Equipment

skyhigh

Sample Assessment - EXECUTIVE SUMMARY

TOTAL CLOUD SERVICES
1985

HIGH RISK SERVICES
161

DATA TO HIGH RISK SERVICES
32,90 GB

PROOF OF CONCEPT PARAMETERS

DEVICES: Blue Coat Proxies

LOCATIONS: All worldwide egress points

TIMEFRAME: 4 Weeks Data

HIGHLIGHTS

- 2103 users with anomalous activity
- 358 services with inconsistent egress policies / exceptions
- 76 file sharing services in use

Resources

Anthony Lee Article: Is your business ready for Data protection Regulation?

http://www.strategic-risk-global.com/is-your-business-ready-for-the-data-protection-regulation/1408088.article

Skyhigh eBook: How EU Data Protection Legislation Affects Your Data in the Cloud

http://www.skyhighnetworks.com/offers/wp-eu-data-protection/

Skyhigh Report: Cloud Adoption
http://www.skyhighnetworks.com/cloud-report/

Cloud Assessment Process

Skyhigh's cloud discovery and risk assessment delivers visibility into cloud usage to allow IT to view the current situation in their network, quantify the risks, see the popular services, investigate anomalous activities and make data-based decisions on cloud usage for the future.

This service typically inspects two-weeks of traffic data from your existing network infrastructure and is delivered as an assessment document that outlines usage and risks that are often shared with multiple stakeholders in the organisation, including IT security, network team, legal/compliance and often provides useful data for departments such as finance, HR and senior management.

The assessment cross-references this cloud traffic with the Skyhigh Registry.   The Registry is a constantly updated database of over 12,000 cloud services, including SaaS, IaaS and PaaS. Each service is assessed and rated based on over 50 attributes developed in conjunction with the Cloud Security Alliance.

The process is conducted under mutual non-disclosure and the process has a few steps:

Skyhigh explains the log format requirements for the initial data, logs can be from log aggregation products, SIEM products, proxies or firewalls.
Skyhigh provides a on-premises Enterprise Connector application. This application removes all personally-identifiable information (such as email addresses, file names, IP addresses etc.), removes information not required (Eg. standard web browsing) and compresses the data to a small fraction of the initial log size
The log is then uploaded to Skyhigh's Hadoop cluster for processing
Skyhigh produces a report (typically 20 – 40 pages) of services, risks and anomalies for review
Skyhigh and the customer review the information together.

The assessment then provides a view into how the issues discovered can be addressed and allows IT to set plans for future cloud usage.

Once there is an accurate view on the cloud usage in the organization, policies can be set to support the business in the future. This may include setting new security policies, delivering regular reports to IT management, consolidating licenses to reduce costs, assessing individual cloud provider risks, review business practices and contracts and educate employees.

The assessment is intended to be a step in the process to allow enterprises to embrace cloud services without risk, to comply with regulatory policies and local data protection laws, identify compromised accounts and devices and insider threats.

skyhigh

Assessment Report

Each report is different, depending on what is found, but typically includes:

Total cloud services in use, high risk service overview, data upload to high risk services
Number of users with anomalous activity
Review of cloud access policies
Number of different file sharing services in use
Services allowing anonymous use, with traffic details
Services on US notorious markets list, with traffic details
Services known for malware distribution, with traffic details
Services owning your intellectual property, with traffic details
Services without encryption at rest, with traffic details
Services without encryption in transit, with traffic details
List of high-risk services, reviewed by data upload, download, user numbers etc.
List of sites known for watering hole attacks
Review inconsistencies in current security policies and/or sites that escape controls
Review potential insider threats, repeat offenders, unsupported device downloads, potentially infected devices, & uploads to unusual destinations
Service vulnerabilities (such as POODLE, Freak & Logjam vulnerabilities)
License counts of sanctioned services in use
Review of each service and its security rating based on the 50+ parameters in the Skyhigh Registry.

skyhigh

Thank You

Nigel Hawthorn, Skyhigh Networks
nigel@skyhighnetworks.com
+44 (0) 7801 487987
@wheresnigel

Data Equipment