Paper

Bitdefender

The emotional side of virtualization: how trust affects cloud adoption and security decisions

(A survey of US, UK and German IT decision makers)

Author

- Răzvan Mureșan

Executive summary

Virtualization is a strategic priority at large companies, and trust plays a crucial role in their choice of cloud service provider and in determining the type of data they store outside company infrastructure, according to a Bitdefender survey of 503 IT decision makers at companies in the US, the UK and Germany with more than 1,000 PCs.

Hybrid infrastructures, a mix of public cloud services and privately owned data centers, have become the major architecture in the enterprise environment, and CIOs have to adapt to the new world. This survey, carried out by iSense Solutions, reveals why companies virtualize, which countries CIOs trust and what kind of data companies care most about.

Key findings

- Half of IT decision makers in the US see cloud as more secure than on-premise infrastructure, while the majority in Germany and the UK trust their own data centers most
- Companies choose hybrid infrastructures for their greater flexibility and room for expansion (55%), increased productivity (54%), superior storage capacity (47%), and lower costs (46%)
- The cloud service providers US IT decision makers most trust are in the US, followed by Canada and England, while those in India, Singapore and Iceland are among the least trusted. German IT decision makers rely on German and Dutch cloud service providers and distrust US-based suppliers. UK IT decision makers tend to choose the US, the UK and Germany
- Data that decision makers would never move outside the company include information about clients and employees, research data about new products and financial information.
- In-house infrastructures were often favored for allowing greater company control than with external solutions

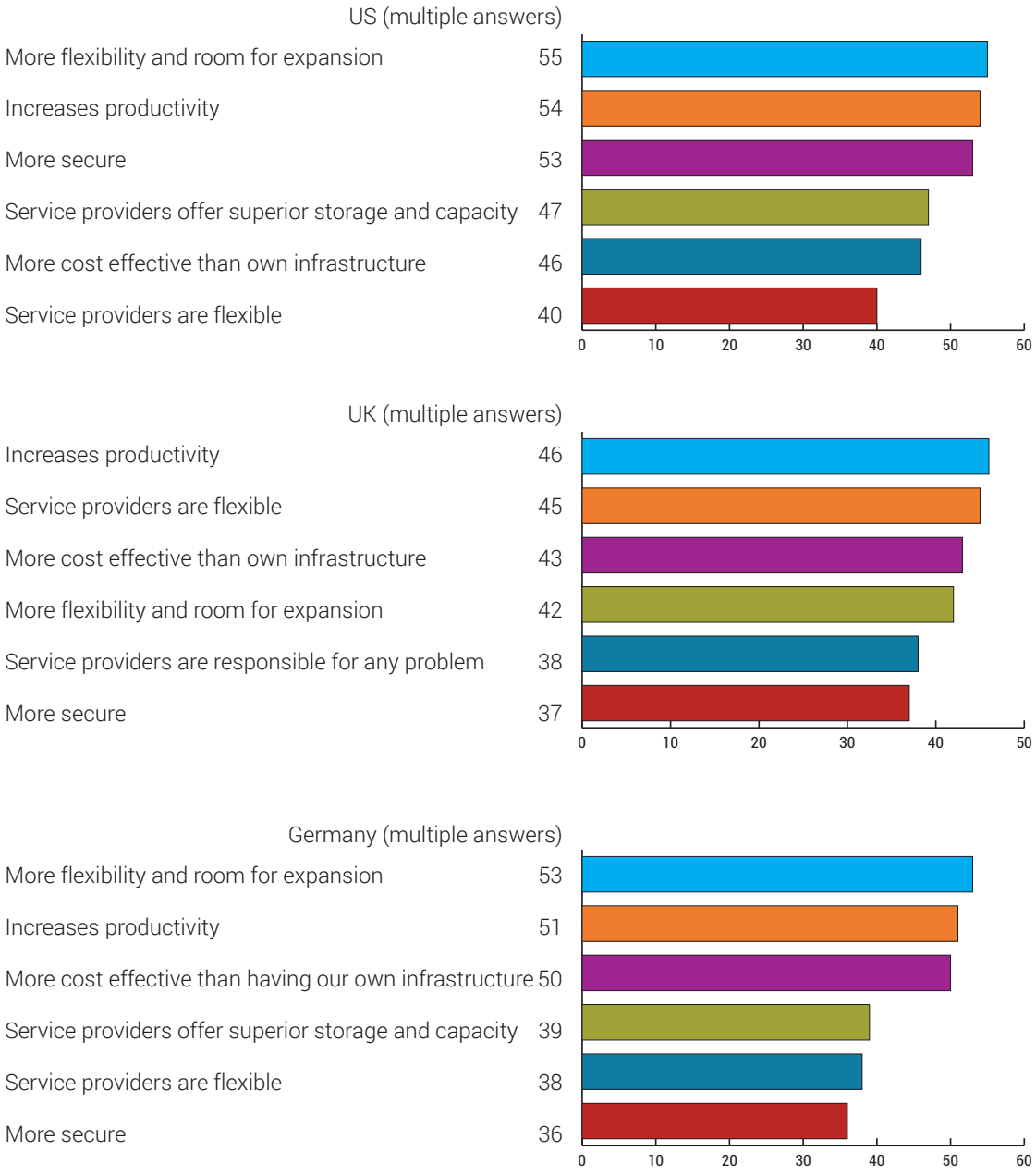
By 2025, some 80% of corporate data centers will disappear as the cloud becomes the primary deployment for information technology, according to recent predictions. The hybrid approach of blending the cloud and the data center has already become a reality. According to researcher MarketsandMarkets, the hybrid cloud market is growing far faster than the overall IT market and will achieve compound annual growth of 27% until 2019. The market is expected to surpass $50-billion this year, double the $25 billion registered in 2014. Analysts expect the hybrid cloud market to reach $85 billion in 2019.[1]

According to advisory company Gartner, by 2019, more than 30 percent of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only.

Companies that have heavily invested in their own private data centers are the first to embrace the hybrid approach. A Bitdefender report published in December, 2016 shows most companies have experienced cloud security incidents such as lack of visibility (51%), a lack of policies (41%) and potential access by unauthorized devices (34%). Gartner recently predicted that the cloud will most commonly be used in a hybrid manner by 2020, and emphasized that purely off-cloud operations will largely disappear by the end of the decade. The advisory company estimates that, by 2019, new software investments of more than 30 of the 100 largest vendors will have shifted from cloud-first to cloud-only.

However, companies choose to virtualize more hardware by substituting it with less expensive and more versatile software, as shown in a Bitdefender survey of more than 500 IT decision makers. US IT decision makers say hybrid environments allow more flexibility and room for expansion, while they also increase productivity and security. Most US respondents even place security as their third-most important argument for migrating to the cloud (53%), far more than Germans (36%) and Britons (37%). Cost-effectiveness is one of the top three reasons mentioned by IT decision makers from enterprises in the UK and Germany.

Why companies made the switch to hybrid infrastructures (%)



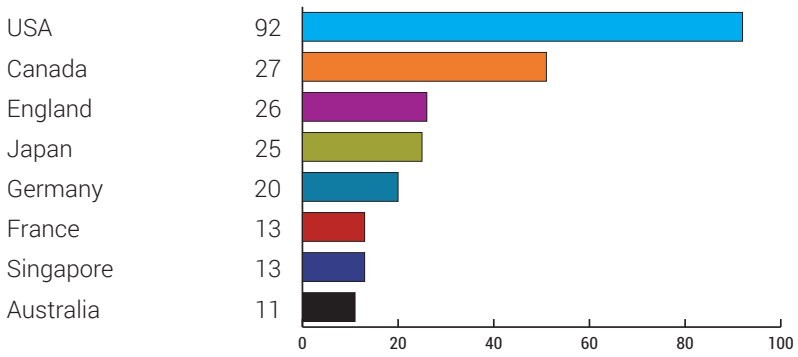
Bitdefender's survey also shows that trust is vital when companies choose a cloud provider. Most respondents place greater trust in suppliers from their own country.

An overwhelming majority of US IT decision makers still have the most confidence in storing data in their own country. After the US, the main countries US IT decision makers favor for data storage are Canada, the UK and Japan.

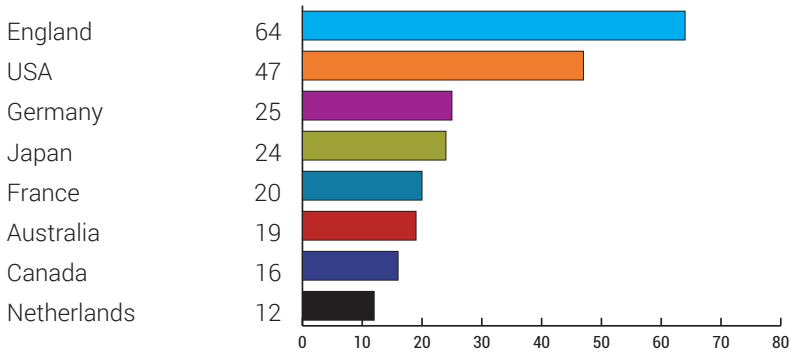
After the UK, UK IT decision makers trust the US, Germany, Japan and France, while only 5% of Germans would store their data in the US. Most German respondents place Germany first (89%), followed by the Netherlands, Japan and the UK.

Location of most-trusted cloud computing service providers (%)

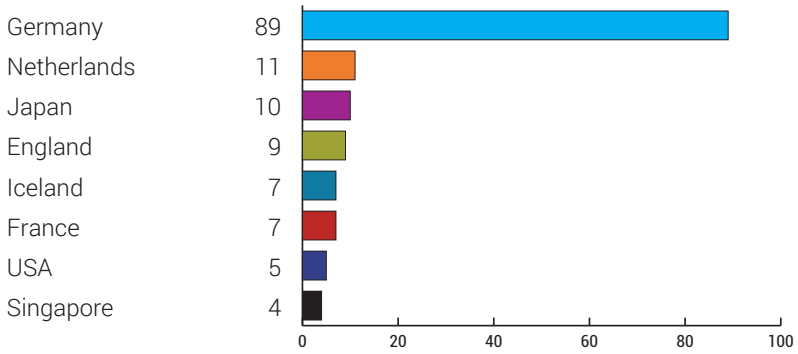
US IT decision makers (multiple answers)



UK IT decision makers (multiple answers)



German IT decision makers (multiple answers)



The least-trusted destination for data storage is India, mentioned by 44% of US respondents, 35% of UK respondents and 43% of German respondents. It's worth noting that IT decision makers did not mention Russia or China among the least trusted 10 countries, showing that they are not even taken into consideration as a viable option for data storage by respondents based in the US, UK, and Germany. They may have also been mentioned as others (by less than 3% of those surveyed).

"If businesses or governments think they might be spied on, they will have less reason to trust the cloud and it will be cloud providers who ultimately miss out," Neelie Kroes, former European Commission VP for digital affairs, said in a speech, as cited by The Guardian. "Why would you pay someone else to hold your commercial or other secrets, if you suspect or know they are being shared against your wishes? Front or back door – it doesn't matter – any smart person doesn't want the information shared at all. Customers will act rationally and providers will miss out on a great opportunity."

The European Data Protection Supervisor, EU's authority responsible for privacy and data protection, says information processed in the cloud usually flows through - and is stored in - various jurisdictions across the globe that might not offer an equivalent level of protection: "Cloud providers must, therefore, guarantee by way of a contract with the customer or in binding corporate rules, that all transfers of

information to non-EU jurisdictions will meet specific data protection requirements to provide adequate safeguards. (...) Ideally, they say, under the terms of the contract, customers should be informed about access requests from law enforcement agencies. Moreover, information should only be handed over to law enforcement bodies in accordance with clear procedures defined in international or bilateral agreements. "Such procedures are under discussion but in many cases are not yet official agreements."[2]

Bitdefender's survey confirms that the US is perceived as the least trusted destination by 54% of German IT decision makers, and by 14% of UK IT decision makers. Besides the aforementioned European regulations, one reason for this distrust might be that European companies distrust US suppliers and are concerned about data privacy, following the rescinding of the Safe Harbour data sharing agreement and the Edward Snowden leaks about potential mass-scale US snooping in the EU, as the BBC has noted.

Safe Harbour, an agreement between the EU and US that took effect in 2000, was designed to provide a "streamlined and cost-effective" way for 5,000 US firms to get data from Europe without breaking its rules. The EU forbids personal data from being transferred to and processed in parts of the world that do not provide "adequate" privacy protections. So, to make it easier for US firms - including the tech giants - to function, Safe Harbour was introduced to let them self-certify that they are carrying out the required steps. In 2013, whistleblower Edward Snowden leaked details about a surveillance scheme operated by the NSA called Prism. It was alleged the agency had gained access to data about Europeans and other foreign citizens stored by US tech giants. After privacy campaigners went to court, Safe Harbour was invalidated by the Court of Justice of the EU in October 2015.[3]

Today, Privacy Shield is the framework that replaces the Safe Harbour scheme. Since August 2016, it allows US businesses to self-certify compliance with a set of privacy principles and, as a result, transfer personal data from the EU to the US in line with EU data protection law requirements. However, the legitimacy of model contract clauses for EU-US data transfers are being tested as Irish authorities say EU-US data transfers "fail to provide for individuals' rights to privacy, the protection of their personal data and their rights to effective remedy as required under of the Charter of Fundamental Rights of the EU." [4]

Furthermore, after Donald Trump became president of the US, the European Commission expressed concern over the recent decision to eliminate privacy protection for non-US citizens and requested additional guarantees that Privacy Shield, a pact signed up by 1,500 companies over the past six months, won't be eliminated.

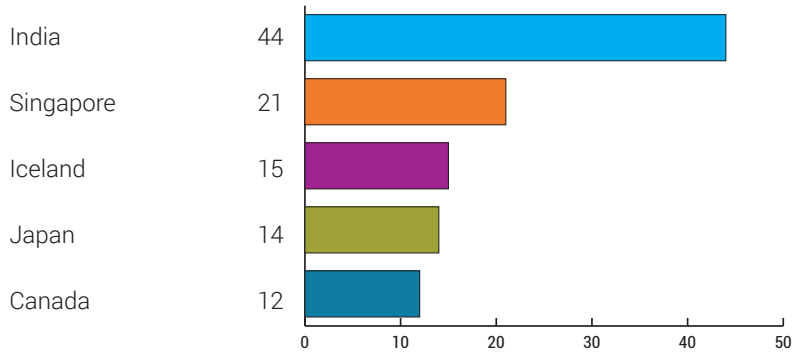
On a different note, Singapore was cited by 22% of respondents in the countries surveyed, on average, as the least trusted country for data storage, followed by Iceland, at an average of more than 10%.

Bitdefender security specialists advise that, when choosing a cloud service provider, it's vital that the datacenter physically reside in a region or country in which data handling and storing legislation is favorable to the company's business interests. A datacenter, regardless of the data it stores, falls under the data privacy and protection laws of the country it's built in. Consequently, it's vital that any company that plans to use a cloud service provider with datacenters outside its home country understand local data protection laws. Otherwise, the organization may risk judicial repercussions that could damage both finances and reputation.

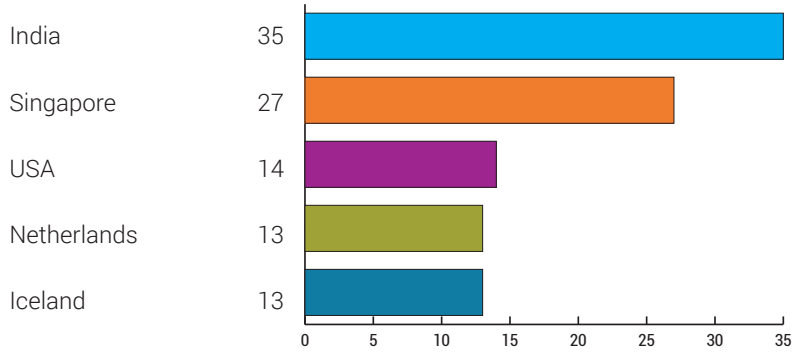
The EU's General Data Protection Regulation (GDPR), which takes effect April 2018, will bring cascading privacy demands that will require a renewed focus on data privacy for companies that offer goods and services to EU citizens. Businesses that do not comply with GDPR face fines of as high as 4% of the company's global annual revenue.[5]

Location of least-trusted cloud computing service providers (%)

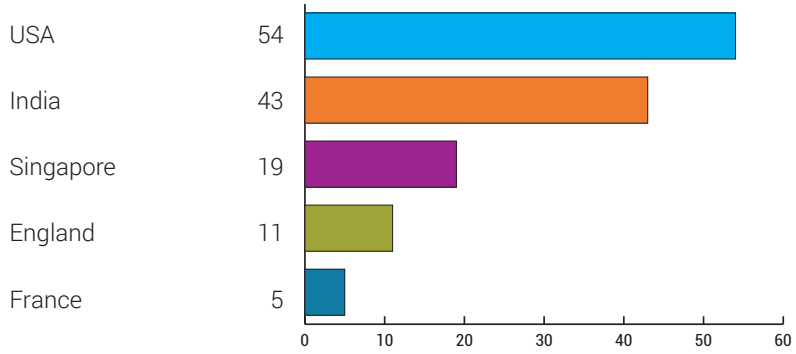
US IT decision makers (multiple answers)



UK IT decision makers (multiple answers)



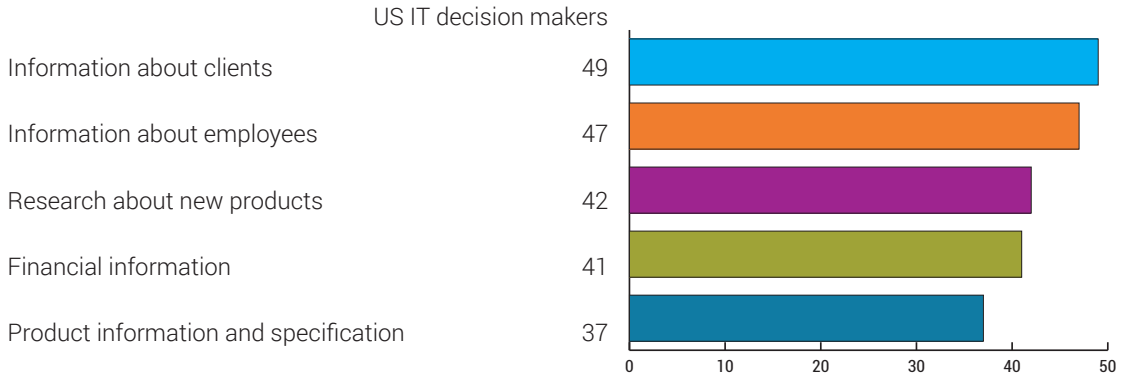
German IT decision makers (multiple answers)

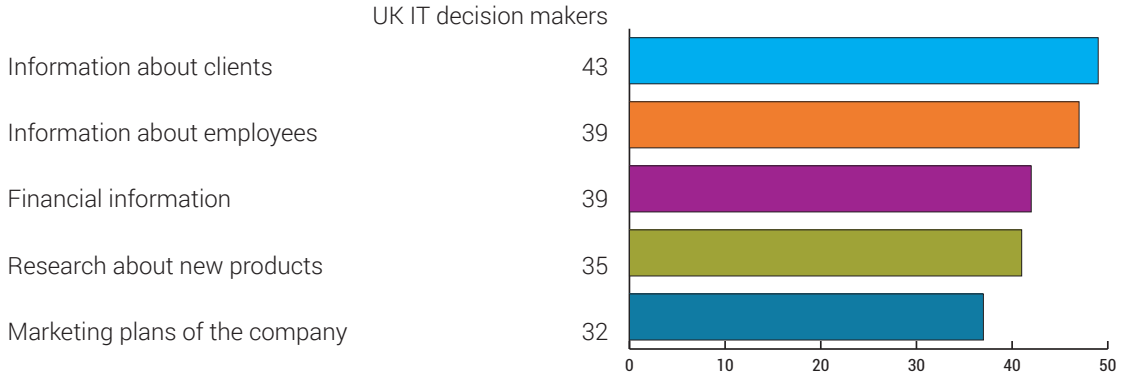


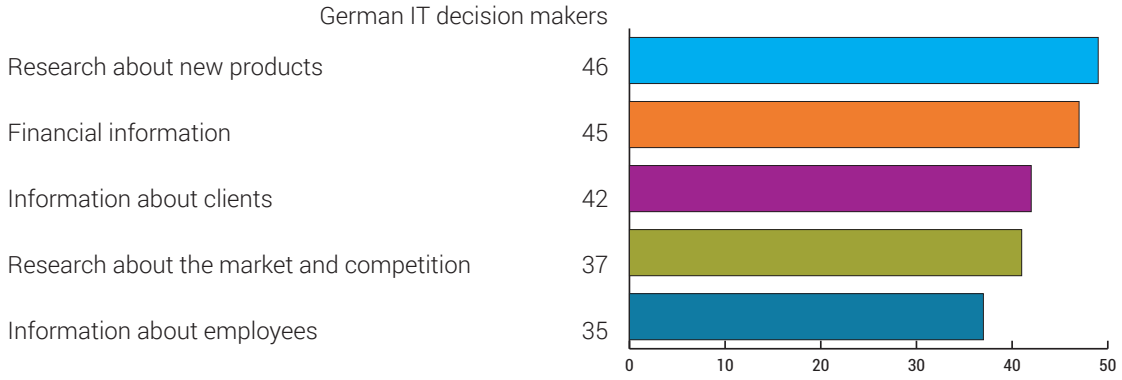
Companies care most about information related to clients (i.e. credit cards, demographics, contracts) and employees (i.e. income, salary, service fees, contact information, stakeholders), research data about new products and competition, and financial information. Most respondents in the surveyed countries perceive these types of data as sensitive and best to store on their own infrastructures. Organizations that handle sensitive or confidential data, or data related to intellectual property, need to ensure their private cloud infrastructure remains private. No one outside the local network should be able to access that data, and only authorized personnel should handle it. The private cloud needs complete isolation from public internet access to prevent attackers from exploiting vulnerabilities to remotely access the data.

The majority IT decision makers in the US that haven't yet adopted the hybrid mix (less than 20 percent of those surveyed in total) say management has more control over in-house solutions than over external ones, while those in the UK and Germany perceive them as more secure than the public cloud option.

Top 5 types of sensitive data companies would never move outside the company (%)







Methodology

This survey, conducted in October 2016 by iSense Solutions for Bitdefender, included 503 IT security purchase professionals from enterprises with 1,000+ PCs based in the US, the UK and Germany. Half of the respondents originate from the United States, while 153 are from the UK and 100 from Germany.

Some 62 percent of organizations surveyed in the US have over 3,000 employees, while 14 percent have between 2,000 and 2,999 and 24 percent employ between 1,000 and 1,999. Some 44 percent of the organizations surveyed in the UK have over 3,000 employees, while 21 percent have between 2,000 and 2,999 and 35 percent employ between 1,000 and 1,999. In Germany, almost half of the organizations surveyed have over 3,000 employees, while 6 percent have between 2,000 and 2,999 and 45 percent between 1,000 and 1,999.

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com/.

Author: Răzvan Mureșan

1 – SPECIAL REPORT: CIOs Say Hybrid Cloud Takes Off, WSJ, October 2015, http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/

2 - European Data Protection Supervisor, 10) CLOUD COMPUTING, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA10

3 – BBC, October 2015, Facebook data transfers threatened by Safe Harbour ruling, www.bbc.com/news/technology-34442618

4 - Legitimacy of model contract clauses for EU-US data transfers to be tested in Irish case, February 2017, http://www.out-law.com/en/articles/2017/february/legitimacy-of-model-contract-clauses-for-eu-us-data-transfers-to-be-tested-in-irish-case/

5 – PwC, Moving forward with cybersecurity and privacy, citing EU's General Data Protection Regulation, http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

BD-Business-Mar.23.2017-TK#: 70585