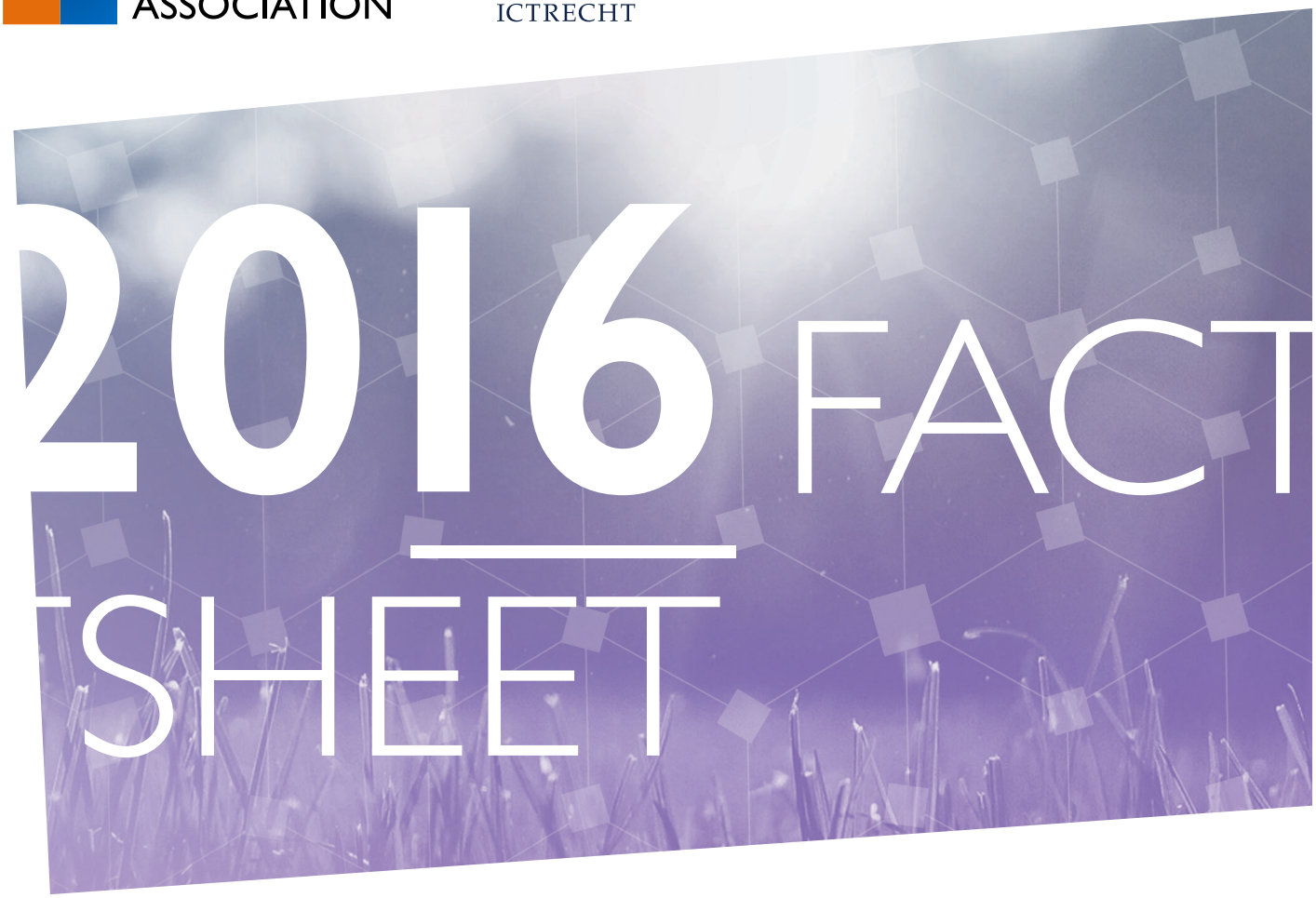
DUTCH DATACENTER ASSOCIATION

In collaboration with:

ICTRECHT



2016 FACT SHEET

SAFE HARBOR

The Netherlands thrives on international trade and logistics. With its many data centers, the Netherlands is an important landing and distribution point of data for numerous US companies. As major digital hub, the Digital Gateway to Europe, we now have a considerable size, are ranked higher and are growing faster than traditional hubs such as Schiphol Airport and the Port of Rotterdam.

Trust, through sound agreements and frameworks on how we handle data and specific personal information, forms the basis of trade and transit. That is why agreements on personal information are so essential.

To be able to pass on personal information to the United States, the European Commission signed an agreement with the US in 2000, called the Safe Harbor Agreement. American organizations which signed up to the Safe Harbor Framework were seen as organizations which handled European personal information in a secure manner.

On 6 October 2015 the European Court of Justice declared the Safe Harbor Agreement to be invalid. The Court took this decision in its ruling on a case between Austrian Max Schrems and Facebook. Since trade and logistics need continue as they always have done, a new agreement was put together, called Privacy Shield.

WHAT IS PRIVACY SHIELD

Personal information in the EU is protected by strict European legislation. Thanks to these strict laws, personal information cannot simply be passed on freely to countries outside the EU. The transit of personal information to other countries is only permitted if there is a legal basis for this, which means the protection of personal information is safeguarded.

For many years the Safe Harbor Agreement formed the basis for the transfer of personal information to the US. If American institutions satisfied the requirements of Safe Harbor, it was assumed that the European personal information was sufficiently protected. Although Safe Harbor wasn't the only basis for sending personal information from Europe to the US, it was for a long time the most used.

In October 2015 the European Court of Justice ruled that the Safe Harbor Agreement did not sufficiently guarantee the protection of European personal information. The Safe Harbor Agreement was subsequently nullified by the Court because the mass surveillance carried out by the US government constituted a major violation of the fundamental rights of European citizens.

Since October 2015 the search has been on to find a solution to the nullification of the Safe Harbor Agreement. This solution has now been found in the 'Privacy Shield'. The aim is for Privacy Shield to replace Safe Harbor and become the new basis for passing European personal information to the US.

CURRENT PROPOSAL

On 29 February 2016 the Privacy Shield was made public by the European Commission. Privacy Shield is to become the replacement for Safe Harbor and is supposed to prevent the problems inherent to Safe Harbor. However, one has to question whether Privacy Shield really can offer sufficient protection of the privacy of European citizens. In any case, more guarantees for Europeans' privacy have been incorporated into Privacy Shield.

For instance, stricter requirements have been set for American companies. There will be greater supervision and sanctions will be imposed on those not acting according to the laws and regulations. For several forms of personal information processing an opt-out must be offered to individuals, but this is in no way the case for all forms of processing.

People have the right to submit a complaint to companies which process personal information and companies must respond to such complaints within 45 days. If the complaint is not handled to the satisfaction of the complainant, attempts to reach a solution can be made via dispute resolution or via a Privacy Shield panel. European citizens can also direct their complaint to the national regulator. The national regulator can then, for example, decide to terminate all data traffic from a particular company to the US.

Furthermore, the rights and obligations of the US government are better stipulated. However, although the European Court ruled that Safe Harbor did not adequately guarantee privacy protection because of, among other things, the mass surveillance conducted by the US government, this can still occur under the Privacy Shield. There are, however, six possible grounds which must be met in order for mass surveillance by the US government to be permitted: the detection and combating of espionage by other countries, combating terrorism, combating the spread of weapons of mass destruction, cybersecurity, the detection of threats to the US or its allies and the detection of cross-border criminality.

These grounds for mass surveillance have already provoked a considerable response. The foundations are so broadly defined that mass surveillance would be permissible in almost any situation.

It is true that guarantees have been established that bind the US government to supervision, such as its promise to keep to the rules. The question is, though, who is going to check whether the US keeps its promise? An ombudsman will be appointed to deal with complaints, but how will this ombudsman obtain his/her powers? And to what extent will this ombudsman be impartial?

STATEMENT 13 APRIL

On 13 April the Article 29 Working Party, a collaboration of the national regulators of every EU country, announced its findings regarding Privacy Shield. The Working Party was satisfied with a number of improvements as compared with Safe Harbor, such as the appointment of an ombudsman, although the Working Party did question the impartiality of this ombudsman.

The working group is of the opinion that the privacy of European data is not sufficiently safeguarded by Privacy Shield. The Working Party has doubts, for example, as to whether Europeans can sufficiently exercise their rights and whether the process of raising a complaint is not too limited and complex.

In addition, the Working Party is concerned about the potential for US secret services to initiate surveillance, when mass surveillance by the US secret services was one of the reasons for invalidating Safe Harbor.

The Article 29 Working Party urges the European Commission to resolve these issues within Privacy Shield and to ensure the creation of a framework that truly guarantees the privacy of European citizens. The decision of the Working Group, however, serves only as advice for the European Commission. The European Commission can decide to disregard this advice.

NEXT STEPS

The findings of the Article 29 Working Party will be passed to the Article 31 Committee. The committee will then consider all the issues around Privacy Shield and take a position on it. Privacy Shield will also be discussed in the European Parliament. Once this has occurred, the European Commission can then make a definitive decision on Privacy Shield. We anticipate that Privacy Shield will in all likelihood be adopted by the European Commission, in view of the major consequences which would result from their rejecting it.

The following provisional timescale is anticipated for the implementation of Privacy Shield:

1 July 2016	*Full implementation Privacy Shield.*
Early 2017	*Start enforcement of Privacy Shield with associated checks.*
Mid 2017	*Joint EU/US evaluation of the agreement.*

Opinion Niels Dutij, legal adviser at ICTRecht.

It is crucial that an agreement is reached whereby the privacy of European citizens is safeguarded. We are particularly concerned about the possibility of mass surveillance by the US secret services. Safe Harbor was primarily invalidated due to the unlimited possibilities for mass surveillance. Yet under Privacy Shield mass surveillance by the US is still permitted, as long as there are sufficient grounds for it. However, the grounds are outlined so broadly that the US government would almost always be justified to do so.

We are pleased therefore that the Article 29 Working Party has taken a critical stance on Privacy Shield. The Working Party has not simply followed the European Commission's proposal, it has given a clear signal. The privacy of Europeans must be guaranteed and, in this regard, Privacy Shield is not currently fit for purpose. Our own criticism of Privacy Shield has been clearly reinforced by the Article 29 Working Party. We therefore hope that the European Commission takes this criticism seriously and makes the adjustments necessary to safeguard the privacy of Europeans.

ABOUT THE AUTHORS

David Snead

Co-founder and vice chair
Internet Infrastructure Coalition

David Snead is a legal expert in the US in the field of internet infrastructure and general legal adviser at cPanel. He is co-founder and vice chair of the Internet Infrastructure Coalition (I2Coalition) which was established in 2012. The I2Coalition represents the interests of the entire internet sector, both in the US and on the international stage, among others in the area of cyber security and privacy.

Stijn Grove

Director Dutch
Datacenter Association

Stijn Grove has more than 15 years' experience in the hosting, cloud and datacenter branches and is one of the driving forces behind promoting the importance and value of the Dutch digital infrastructure. He is director of the Dutch Datacenter Association, of which almost 30 market leading Dutch datacenters are members.

Niels Dutij

Legal adviser ICTRecht

Niels Dutij is legal adviser at legal advice bureau ICTRecht. In his work Niels focusses primarily on privacy. He completed his Masters in Criminal Law and Constitutional & Administrative Law at the University of Amsterdam. During his study he worked for a software company where he gained both legal and technical knowledge.

DUTCH DATACENTER ASSOCIATION

More information:
@DutchDatacenter
www.dutchdatacenters.nl