dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

The ECJ ruling on the EU-US Privacy Shield and its Consequences

CAUTION: DATA PROTECTION

Avoid negligent Breaches when selecting Cloud Software Systems!

DR. JUR. ROBERT SELK, DR. MICHAEL TOEDT

dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

At least since the GDPR went into effect, data protection should be at the top of your agenda. However, when it comes to selecting cloud software systems, the applicable legislation is often negligently violated.

Data Transfer to a third Country

According to the GDPR, personal data may only be transferred to a third country if an adequate level of protection is ensured there (Article 44). However, data protection in the USA is not considered adequate. Therefore, in theory, no data may be transferred there. However, Article 45 GDPR provides that transfers to a third country are permissible if the European Commission has determined by an adequacy decision that the level of protection is sufficient.

(Source: datenschutz.org/privacy-shield/)

In case your Cloud Provider is located outside the EU

Today, every cloud provider is obliged to take sufficient technical and organizational measures with regard to data protection and data security.

This also includes regulations on any subcontractors, such as hosting providers or integrated software components. Both of these are part of the so-called Data Processing Agreement (DPA). However, experience has shown that these are rarely checked comprehensively by the contractor, e. g. the hotel, before they are concluded – with dangerous consequences. Since last year, there has been a very **significant court decision** that for all those cases in which either the cloud provider itself or one of its subcontractors is not based in the EU or EEA but outside. This applies to many large software providers, especially in the hotel industry.

dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

Background: Protection from US Authorities

In July 2020, **the European Court of Justice (ECJ)** declared the successor to the Safe Harbor Agreement, the so-called Privacy Shield Framework between the U.S. and the European Union, invalid. This means that personal data transferred to recipients in the USA on the basis of this **agreement may NOT be transferred there anymore. This affects cloud software providers as well as hosting companies in the USA**, as well as all subcontractors in the USA. Anyone who processes their guest data using a US cloud software provider or stores it in a hosting environment in the USA is therefore committing a data protection violation - insofar as this continues to take place against the background of the Privacy Shield - which can be punished with a fine of up to 4% of last year's global turnover.

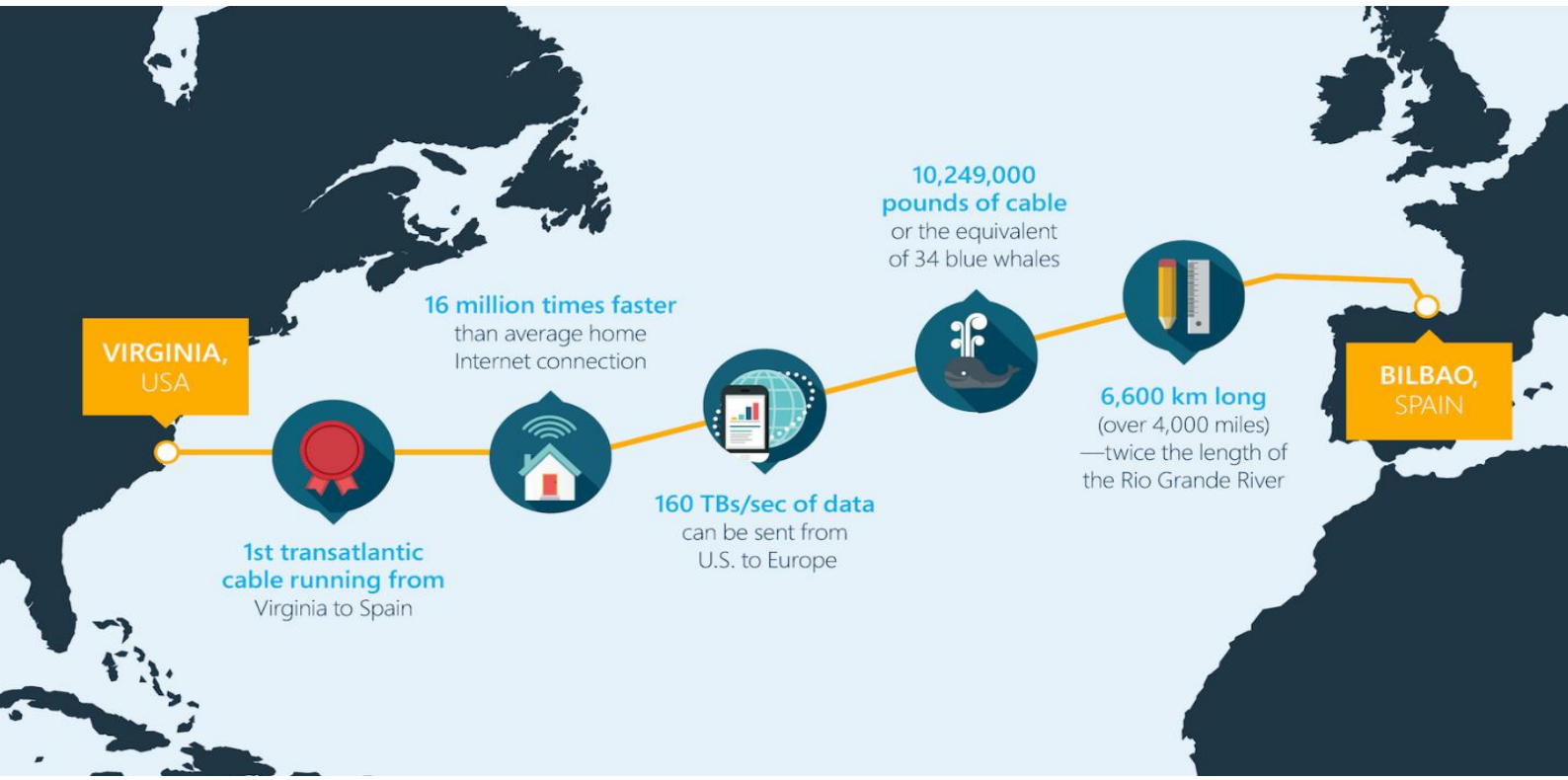
The reason for the court ruling is the fact that the Privacy Shield cannot provide sufficient protection for data stored by US

According to the GDPR, personal data may only be transferred outside the EU if a certain level of protection can be guaranteed (GDPR Article 44, General principles of data transfer)

companies against access by US authorities, as it binds US companies but not government investigating authorities in the USA. The EU court, which a few years earlier had also overturned the Safe Harbor agreement as a predecessor regulation, sees this as a serious violation of the high European data protection standards for the protection of the data subjects, in the hotel sector primarily the hotel guests.

The Privacy of Hotel Guests

This legal opinion is quite understandable and has a **great significance especially for the hotel industry**. On the one hand, hotels try everything to protect their guests and their privacy. On the other hand, however, the guests' data is often transferred to a country outside the EU, such as the USA, without their knowledge or consent and thus made accessible to the authorities there. Especially some guests of luxury hotels would



Overseas data cable from the USA to Europe (Source: Microsoft/ RUN Studios)

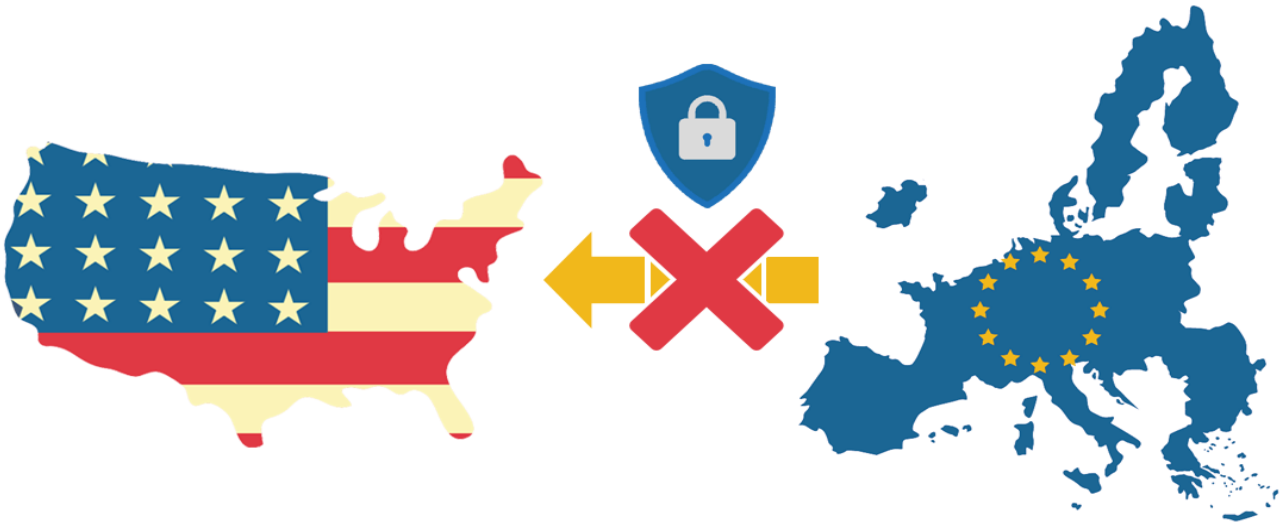
probably have their hair stand on end if they knew this.

As an alternative to the Privacy Shield, it has so far been possible to enter into standard data protection **agreements specified by the EU, the so-called EU standard data protection agreements**. These were not the subject of the ECJ proceedings, so that the ECJ was not allowed to rule on them. However, since contracts can never bind a national intelligence service or investigative authorities, but only the two contracting parties - for example, the hotel and a U.S. cloud provider - from a legal perspective, the considerations of the ECJ can also be applied in large part to this solution variant, i.e., the EU standard contracts. In the opinion of the EU data protection authorities in the form of the European Data Protection Committee, the conclusion of such EU standard data protection contracts is no longer sufficient, especially for the USA, unless the data can be stored so strictly and securely encrypted with the US provider that it can no longer be accessed by investigating authorities and intelligence services.

"The Privacy Shield does not provide sufficient protection against access by U.S. authorities."

Data Protection with Pitfalls

Such strict encryption is certainly conceivable. However, up to now this has largely only been possible for data in hosting context. With regard to cloud-based SaaS software solutions or other typical cloud applications that do not only consist of pure hosting of data, but also involve genuine software functionalities, this has hardly been possible in practice to date. Even the major U.S. companies do not offer any technical solutions in which, even in SaaS or cloud applications, the data is encrypted end-to-end and thus even the cloud providers themselves no longer have access but can still offer the functionalities. Although there are **a few minor exceptions from a legal point of view**, these do not yet play a role for the large mass of cases such as the use of US cloud applications in mass business. In fact, the current view of the data protection authorities in the EU is



Look for European solutions for your cloud software! (Image: datenschutz-generator.de)

tantamount to a far-reaching ban on the use of US cloud software.

The problem has now reached at least the major US software companies. As a result of the ruling, they have begun to install their **own data centers and instances in the EU** and to physically host the data in the EU. However, the issue is more complicated and hosting within the EU is not a sustainable solution as long as the actual administration of the data is carried out from the USA and US authorities can still access the data via this detour. This means that subsidiaries of U.S. corporations, for example, which are thus subject to instructions from the U.S., should also be viewed critically. Especially since even the support from the USA counts as unauthorized data transfer.

Get out of the Dilemma

But what is the solution? One solution is the aforementioned secure technical encryption of the data transferred or stored in a cloud application to such an extent that it can no longer be read by foreign authorities. However, this may not be possible for US companies or may not

even be technically feasible for cloud-based application software.

What options do hotels now have in the EU, or who must comprehensively observe the GDPR? Before signing a software contract with a U.S. provider (or an EU provider that uses U.S. subcontractors), it needs to be reviewed specifically with regard to the above issues in terms of data protection law. A detailed data protection review of software contracts by a specialist lawyer can cost a lot of money. In addition, it is currently unlikely that the result of the review in the cases discussed here will result in an endorsement of the conclusion of a contract.

The legally safest way

The legally safest way is to bypass the described data protection problems of non-EU transfers and service providers and to use a software provider based in the EU or EEA who also only uses subcontractors based in the EU/EEA. This is because all companies involved are then directly obligated to the GDPR and thus to the high level of data protection there, unlike companies outside the EU/EEA. In this context, it should be mentioned that the penalties of the GDPR initially affect the companies, such as the hotel, and not directly their legal representatives, such as managing directors or board members. However, according to national regulations, there may still be personal liability of the management - for example in Germany under the aspect of organizational culpability.

Those who want to sleep soundly should try to stay on the safe side in terms of data protection law when signing a contract for cloud software, i. e. within the borders of the EU/EEA.

dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

About dailypoint™ - Software made by Toedt, Dr. Selk & Coll. GmbH

dailypoint™ is the leading Data Management and CRM platform for sophisticated individual hotels and hotel groups. dailypoint™ collects data from all relevant sources such as PMS, POS, website, newsletter or WiFi and automatically creates a central and consolidated guest profile. In 350 steps, the data is processed and enriched by means of artificial intelligence (AI) to create a guest profile never seen before. The cloud-based SAAS solution consists of 16 modules and is complemented by the dailypoint™ Marketplace with more than 160 solution partners. dailypoint™ not only offers measurable marketing, but also covers the entire customer journey and thus supports all departments within a hotel. The integrated Privacy Dashboard is also the central element for the technical implementation of the GDPR.

dailypoint™ is headquartered in Munich, Germany and is sold and supported worldwide directly or through its distribution partners D-EDGE and XNProtel. dailypoint™ is the leading Data Management and CRM platform for sophisticated individual hotels and hotel groups. dailypoint™ collects data from all relevant sources such as PMS, POS, website, newsletter or WiFi and automatically creates a central and consolidated guest profile. In 350 steps, the data is processed and enriched by means of artificial intelligence to create a guest profile never seen before. For more information, visit **www.dailypoint.com**.

About Dr. Michael Toedt

Dr. Michael Toedt is Managing Partner of Toedt, Dr. Selk & Coll. GmbH in Munich. His professional life to date is bipartite: Growing up in his parents' hotel business, it was initially his goal to take over their business. After two professional apprenticeships and experience in the hotel business, he studied business administration with a focus on the hotel industry at the University of Applied Sciences in Munich. In 2000, he started his second professional life in the field of CRM at the Schörghuber group of companies. In 2005, he founded Toedt, Dr. Selk & Coll. GmbH. TS&C, today known as dailypoint™, has since made a name for itself as a software company and think tank for data-driven management. In addition to his work at Toedt, Dr. Selk & Coll., Michael Toedt is, among other things, a lecturer at the University of Applied Sciences in Munich on the topic of "CRM in Tourism" as well as a lecturer at Hotellerie Suisse in the NDS Management Program. He regularly publishes specialist articles aboutf Big Data and digitalization. Amongs othes, his book "Big Data" published by Deutscher Fachverlag. In 2015 and he completed his doctorate at the University of Latvia on the topic "Influence of communication on repurchase behavior in the hotel industry".

About Dr. jur. Robert Selk

Dr. jur. Robert Selk, a lawyer specializing in IT law, is a partner at SSH Rechtsanwälte in Munich. He received his doctorate in 2002 in the field of Internet and data protection law. The focus of his parallel master's postgraduate studies was European and international business law (Master of Law, LL.M.). For many years, his practice has involved computer, Internet and data protection law as well as trademark, copyright and competition law. Dr. Selk is also appointed as an external data protection officer in various internationally active companies, works extensively as a speaker on IT and data protection law, and is a member of, among other things, the legislative committee on IT law of the German Bar Association and co-chairman of the "Data Protection" specialist committee of the German Society for Law and Information Technology. In addition, he regularly publishes legal articles.

For more information: michael.toedt@dailypoint.net

www.dailypoint.com