CLOUD COMPUTING AND IT-LAW

Sabine Proßnegg / Johannes Feiner

Sabine Proßnegg, Associate Professor (FH), FH JOANNEUM, Institute for Software Design and Security
Werk-VI-Straße 46, 8605 Kapfenberg, AT
Sabine.Prossnegg@fh-joanneum.at; https://www.fh-joanneum.at

Johannes Feiner, Senior Lecturer (FH), FH JOANNEUM, Institute for Software Design and Security
Werk-VI-Straße 46, 8605 Kapfenberg, AT
Johannes.Feiner@fh-joanneum.at; https://www.fh-joanneum.at

Keywords: ***cloud computing, data protection, data transfer to third countries***

Abstract: *The outsourcing of IT services is a widespread trend. Cloud solutions offer advantages such as simple scalability, access, and an up-to-date service. Large US providers are unrivaled market leaders. But are these US companies really a good choice? Do the providers‘ terms hold what they promise? European authorities and courts are critical of this, and a brief survey through contract and data protection law makes it clear why. This paper shows the growing gap between legal requirements European companies have to adhere to while at the same time their negotiating power diminishes. We argue that European interests cannot be implemented without European providers or at least new solutions.*

1. Cloud computing from a technical perspective

The outsourcing of IT services such as data storage, computing power, or application software is a trend in both the private and the business sectors.[1] Looking at the terminology, it is worth noting that it has not been possible to establish a universally valid definition of cloud computing, yet. The definition of the U.S. standardization body NIST (National Institute of Standards and Technology), which is also used by ENISA, the European Network and Information Security Agency, reads as follows: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […].” Serverless computing with Function as a Service (FaaS) and Backend as a Service (BaaS) have been added in recent years to better support microservices in cloud computing. Demands for separation of services and packaging single services into containers drive virtualisation. This can be provided by Container as a Service (CaaS).[2]

The use of cloud services is in many respects similar to classic outsourcing, but there are some differences. For economic reasons, several users share a common infrastructure in a cloud. Cloud services are dynamic and can be scaled up and down in a short time. The technologies used in cloud computing make it possible to distribute IT services dynamically across several locations, which can be widely scattered geographically. Country borders do not play a role here. The customer can easily administer the services and the resources used via web interfaces, without the need of a lot of interaction with the provider.[3]

[1] Mell/Grance, The NIST Definition of Cloud Computing (Technical report), National Institute of Standards and Technology: U.S. Department of Commerce, doi:10.6028/NIST.SP.800-145, 2011.

[2] NIST FN. 1, see also BSI, BSI – Grundlagen – Cloud Computing Grundlagen (www.bsi.bund.de), Accessed: 17.3.2022.

[3] BSI – Grundlagen – Cloud Computing Grundlagen (www.bsi.bund.de), 17.3.2022.

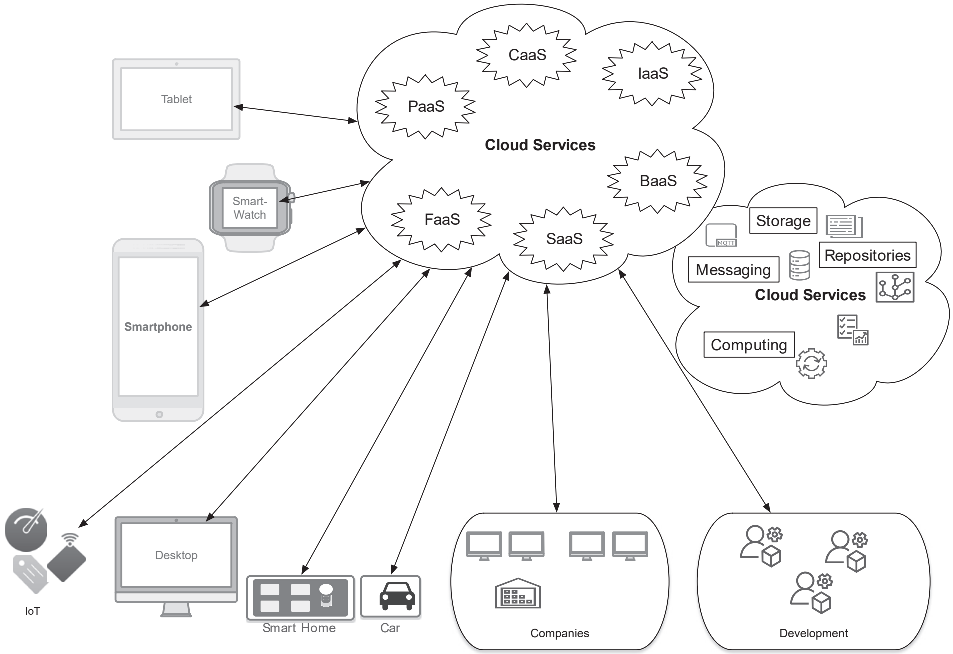

Figure 1 Feiner, Johannes, Services provided in the Cloud.

From a security perspective, it is an advantage to host services by cloud providers, because they are responsible for using firewalls, backup, and always updated software. In general, outage time is shorter and recovery after hacks can be faster. For most of the services the software is based on open source operating systems, applications and frameworks. Open Source Software (OSS) can be inspected and updated (patched) by anyone at any time, which enhances transparency, security, and cost-efficiency. Concerning the performance, cloud providers might distribute data using Content Delivery Networks (CDN) with worldwide caches. This results in fast loading times of web applications independent of the users' location.[4]

Scaling services for more users or more computing power is easy, but the costs increase not proportionally depending on the pricing scheme. Companies might run into problems when migrating from one provider to another, because the tool chains or storage formats used are often vendor-specific, the locked-in syndrome. Clients use not only web based apps in the browser, but native apps running on Google and Apple mobile operating systems. The software is maintained by those American companies and partly protected by copyright. Additionally, applications work best in combination with cloud services provided on Google and Apple servers. Hence, mobile app users are largely dependent on US infrastructure and software for backup, photos, music, maps, contacts, video messaging, notifications and the like.[5] App stores, synching data between devices, and home automation are further examples where the dependency on U.S. cloud services is substantial Data of the Synergy Research Group shows[6] in seven cloud services and cloud infrastructure market segments, operator and vendor revenues surpassed the $150 billion mark in the first half of 2019, growing 24% over the first half of 2018. Among cloud service segments, IaaS and PaaS business models showed the highest growth rate at 44%, followed by Enterprise SaaS at 27%. Spending on hardware and software for public, pri-

[4] Heise, Die Vorteile und Nachteile des Cloud-Computing (www.heise.de), 24.3.2022, Accessed: 15.11.2022.

[5] A list of cloud services provided by Apple: https://www.apple.com/support/systemstatus/, 15.11.2022.

[6] Reno, NV, Sept. 19, 2019, Half-Yearly Review Shows $150 billion Spent on Cloud Services and Infrastructure, Synergy Research Group (srgresearch.com), 15.11.2022.

vate and hybrid infrastructure grew by just over 10%. Across the cloud ecosystem, Microsoft, Amazon/AWS, Dell EMC, Cisco, HPE and Google were among the market leaders.

2. Advantages and disadvantages of a cloud

The main advantage of cloud computing is that cloud users do not need their own hardware resources to store data or use application software. The user‘s own hardware and software do not have to be adapted and upgraded, because most cloud services are used via a web browser or a client. This saves personnel costs and does not tie up any capital. The costs are easy to predict thanks to monthly invoices. Storage space, computing power and the software package can be adjusted and adapted to actual requirements at any time. Another advantage is the easy access at any time with different devices, stationary or mobile. In addition, data such as images, documents, music or videos can be exchanged, shared and jointly edited with others. Company branches or locations can be connected to the IT infrastructure at low cost. Access to the resources by a company‘s employees is usually controlled by the cloud provider‘s administration. The same applies to access protection to computer systems.[7]

Disadvantages of using cloud services are privacy and data protection. The computer systems of cloud service providers must be maintained and secured at great technical and financial expense. In most cases, it is essential to store account and login data such as name, address, e-mail, telephone number and payment information in order to use cloud services. This kind of data, as well as metadata such as device number, the browser used, IP address, location, language settings and log data, is stored. Furthermore, in some cases, the data is not only stored, copied, modified, analysed, and logged by the provider itself, but also transferred to third parties.[8] Very often data is stored in its unencrypted form, or encrypted in a way that the provider can still access the data, especially if the provider possesses a global decryption key. From a legal perspective, the Austrian Information Security Handbook cites the following areas of particular importance in the context of cloud computing: data protection law, IT contract law, public procurement law, criminal procedure law.[9] We want to look at two of the named areas: contract law and data protection.[10]

3. Cloud and contracts

The contracts in IT outsourcing are usually called service agreements (SA). Contract law for cloud services is complex and comprises documents such as general terms and conditions (GTC), service level agreements (SLA), usage and customer license agreements. Sometimes, in addition, there are documents about “side issues” like fair use and compliance. Since the Austrian General Civil Code, the ABGB, does not cite such contracts, they are usually seen as a mixture of known instruments like rent, lease, service and work contracts. In case of doubt, the interpretation is made according to the regime that prevails in the opinion of the judge. In order to avoid this supplementary interpretation of the ABGB, the parties, in particular the cloud provider, tends to regulate all possible issues in as much detail as possible. As a consequence, the landscape of legal documents concerning cloud services becomes complex. On top, the documents are sometimes difficult to find and they reference each other, so that it is difficult to have an overview of all of them. They are not easy to read, often provided in English only, or at least the English version is the legally binding one.[11]

As outlined above, Cloud business models use the principle of scalability, the underlying processes have to be standardized and designed to be customer-neutral. This applies not only to the technical processes, but also to the contracts. Providers of cloud services are particularly interested in using uniform contractual conditions.[12]

[7] Minnich, https://www.heise.de/download/blog/Die-Vorteile-und-Nachteile-des-Cloud-Computing-3713041, 15.11.2022.

[8] Ibid.

[9] A-SIT, BKA, Österreichisches Informationssicherheitshandbuch, Cloud Computing, 15.11.2022.

[10] Blaha et al, Rechtsfragen des Cloud Computing (2011).

[11] Manhardt, Der “Software as a Service”_Vertrag (2012).

[12] Bomhard/Baum, Cybersecurity in outsourcing and cloud computing, 27.04.2021, online: Cybersecurity in outsourcing and cloud computing, 15.11.2022.

Companies, on the other hand, that depend on cloud providers are highly diverse. As a rule, especially SMEs concentrate on their core business, their IT knowledge is scarce, and there is little time to deal with digitization and its consequences. So, it makes sense to them to use services that are easy to access, user-friendly and inexpensive or even free of charge. However, European companies are not only forced to fulfil certain minimum requirements in the area of their IT due to the GDPR (see later), but also due to sector-specific regulations such as health or energy. In areas of critical infrastructure the requirements for technology and processes become really complex, which must be reflected in the contracts in order to be compliant.[13]

The Austrian handbook for IT Security Standards states that contractual arrangements with the cloud service provider should in principle always be tailored to the individual needs. This is followed by a list of points that should be part of a contractual agreement such as compliance with data protection laws, especially information about data breaches, access for the data controller to carry out a risk assessment, processing agreements, details about the service, liability and warranty claims.[14]

European companies are thus faced with a dilemma: on the one hand, the few U.S. providers who have their standardized set of contracts which are used by the majority, on the other hand European companies who are subject to very specific European and national legal requirements. The argument is that this growing tension between the contractual standards of these large U.S. IT service providers and the requirements of European companies must be resolved by well designed contracts. Each requirement must be adequately taken into account and like in software development, the industry-specific and country-specific standards would have to be „programmed" into the contracts.[15] But is this realistic at all, given the different markets of the two sides? In practice, SMEs have little or no negotiating power on their side. On the contrary, even with existing contracts, companies are often at the mercy of short-term changes without alternative. Cloud operators can terminate existing cloud accesses completely, for example by changing the access authorizations, legally and also physically at any time.

The EU acknowledges the problem and points out that leading markets such as the U.S. and China have asymmetric (public) procurement policies that favour their local cloud service providers and disadvantage European counterparts in global competition. The EU will intervene to level the playing field, mainly by regulating the digital gatekeepers through the Digital Markets (DMS) and the Data Act, but also by implementing a cloud industrial policy based on a level playing field, software sovereignty and a new Buy European Tech Act.[16] However, due to the need for standardization of the cloud services and due to unequal market power as well as the high market concentration of the providers, the contract design is unilaterally distributed, which clearly limits the possibilities, both when concluding and when changing a contract.

4. Cloud and data protection

IT outsourcing usually comprises the processing of personal data in the sense of Art. 4 GDPR. Data protection law is closely related to fundamental and human rights since it is about the protection of personality, dignity and individuality. In Austria, the Data Protection Act (DSG) is relevant, in particular § 1 DSG, paragraph 1 providing for secrecy, information, correction and deletion. As part of a set of fundamental rights with third-party effect, see also Art. 8 of the Human Rights Convention and Art. 8 of the European Charta of Fundamental Rights, data protection helps to ensure the rights and freedoms of natural persons, pillars of a free and democratic society. That is why these rights are specially protected and there is a rigorous examination necessary before they can be restricted. The least restrictive means to achieve a goal in public interest must be chosen, the means have to be necessary, objectively justifiable and proportionate.[17]

[13] Ibid.

[14] A-SIT, BKA, Österreichisches Informationssicherheitshandbuch, 22.4.2022.

[15] Ibid.

[16] Digital Business Cloud, Cloud-Architektur: Die 11 wichtigsten Trends für 2022 (digitalbusiness-cloud.de), 15.11.2022.

[17] Knyrim (Hg), Der DatKomm (2018); Pöschl, „Grundrechtseingriffe müssen durch ein öffentliches Interesse geboten, zur Zielerreichung geeignet, dieser adäquat […] und auch sonst sachlich zu rechtfertigen [sein.]", https://staatsrecht.univie.at.at/fileadmin/user_

Cloud computing is usually data processing on behalf of a controller. In terms of Art. 28 GDPR, a processor agreement must therefore be concluded, which binds the processor, i.e. the cloud provider, to the controller, in our case a European company. The subject and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller are specified. The cloud service provider must provide sufficient guarantees that appropriate technical and organizational measures (TOMs) are implemented in such a way that the data processing is carried out in compliance with the requirements of the GDPR and the protection of the rights and freedoms of the data subjects are ensured. The required level of detail of these measures is determined by the risks of the data subject resulting from the data processing. The risk will depend on both the type of data and the scope of the processing. The clients should therefore conduct their own supplementary risk assessment and evaluate the measures submitted by the processor with regard to the required scope. Subsequently, the concrete technical and organizational measures can then be attached to the order processing contract.[18]

Usually, it is in the customer‘s interest to contractually oblige the cloud service provider to comply with certain TOMs including documentation, compliance with which the customer can monitor and prove to the data protection authority. Cloud providers usually reserve the right to continuously adapt the TOMs to technical developments to which there is no objection. It is good practice to define specific TOMs dynamically, but to prescribe certain minimum requirements based on the respective state of the art, as well as documentation obligations; standards of a European, international or national organization are often used for this purpose.[19] Further norms can be used provided that they are transparent and accepted.[20] Although technical standards are in principle not sources of law, there are nevertheless regulatory techniques that break this principle, namely when a legal provision, law or contract, refers to such a standard. While this was viewed critically at the beginning, it is now generally accepted in the case of references to technical rules.[21]

Since the cloud market is dominated by a few U.S. companies, the issue of transfer to third countries as defined in Art. 44 ff GDPR adds up to the general obligations of the GDPR. There are only three possibilities here: the existence of an adequacy decision by the European Commission, the existence of suitable guarantees, or the fulfillment of an exception. After the end of the adequacy decisions Safe Habour and its successor Privacy Shield, see ECJ judgments Schrems I and Schrems II[22], only the appropriate safeguards and the exceptions remain. Appropriate safeguards are, above all, the standard contractual clauses, which do not provide an appropriate solution themselves, even less with sensitive data, since they cannot be enforced against authorities (esp. NSA, FBI).[23]

5. U.S. American law like CCPA, Cloud Act, FISA and NSL

Comparing privacy legislation in the U.S. and in Europe, there are similarities as well as differences. The California Consumer Privacy Act (CCPA) is California’s data privacy law enacted in 2018 and taking effect on January 1, 2020. The CCPA protects personal information of “consumers or households” worldwide.[24]

upload/i_staatsrecht/Poescl/Publikationen/1997_UEber_Gleichheit_und_Verhältnismäßigkeit.pdf, 07.11.2022; VfSlg 13.739/1994; 13.955/1994 uvm.

[18] Bomhard/Baum, Cybersecurity in outsourcing and cloud computing, 27.04.2021, 15.11.2022; see also Knyrim (Hg), Der DatKomm (2018).

[19] Harmonisierte Norm, erstellt aufgrund des Auftrags der Kommission und im Amtsblatt veröffentlicht; EU-Organisationen: CEN, Cenelec, ETSI (Anhang I VO (EU) 2012/1025), Int. Organisationen: ISO, IEC, ITU (Art. 2 Z 9 VO (EU) 2012/1025).

[20] Frässdorf, Rechtsfragen des Zusammentreffens gewerblicher Schutzrechte, technischer Standards und technischer Standardisierung (2009) 16.

[21] Die koordinativen Regelungen haben für diese Arbeit weniger Bedeutung, siehe Bauer, Das Recht des Technischen Produkts (2018) 166–167.

[22] ECJ C-362/14 of 6.10.2015 (Schrems I); ECJ C-311/18 of 16.7.2020 (Schrems II).

[23] Knyrim (Hg) DatKomm, Art. 44 DSGVO.

[24] https://www.lexology.com, 15.11.2022; An explanation to the CCPA states: “[…] the GDPR regime […] may well have enthused non-EU countries to put a new emphasis on their own data privacy regimes. Non-EU companies are likely to need to be GDPR

The CCPA has similarities with the GDPR but differs in scope and content. It focuses on consumers' rights and is only applicable to companies of a certain size. Consumers have a right to know what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information. They have a right to deletion of personal information held by businesses and extension or a business's service provider. Consumers have the right to opt-out of sale of their personal information and can force businesses to sell their personal data. Children are specially protected under the CCPA.[25]

Cloud Act is the abbreviation for Clarifying Lawful Overseas Use of Data Act.[26] This is essentially a statutory data protection regulation of the U.S. law enforcement. The goal is to collect evidence related to U.S. persons in criminal cases. It authorizes U.S. authorities to access all corporate and customer data of cloud and communications providers, provided the company is based in the U.S. or is subject to U.S. law. There is a ban on „fishing expeditions", but the skepticism is broad and justified which we know due to the revelations of Edward Snowden.[27] The Cloud Act also means that those affected have no way of defending themselves against access, only the U.S. Internet Service Providers can lodge an objection.[28]

The National Security Letters (NSL) requests for a user's information considered relevant to issues of national security issued by the Federal Bureau of Investigation (FBI) and FISA, the Foreign Intelligence Surveillance Act, originally enacted in 1978 to govern how the US government collects foreign intelligence for national security, can be relevant, too. FISA also created the Foreign Intelligence Surveillance Court and the Foreign Intelligence Court of Review, who have the power to require companies or other private organizations to hand over information in foreign intelligence investigations.[29] The FISA Amendments Act, passed in 2008, authorizes the government to require U.S. companies to provide information and the content of communications associated with the accounts of non-U.S. citizens or non-lawful permanent residents who are located outside the United States. Telecommunication services also have to abide to the Communications Assistance for Law Enforcement Act. All companies like Microsoft and Google publish transparency reports about such requests.[30] To summarize, U.S. intelligence agencies and courts have very extensive access to data, worldwide. Consumers in most U.S. states have legal remedies against this if they find out about it, in contrast to Europeans.

6. How to be compliant

As we have seen, mere legal remedies are not enough. They are important but have to be combined with technical measures. When agreeing on TOMs, one important technical measure is the anonymization[31] of data as far as possible before it leaves the user/client. With aggregation and polls, the possibilities for analysis are intentionally limited. Randomization, synthesis and suppression are transformation or perturbation techniques that are selected to preserve as much of the statistics as possible. Multi-party computation and enterprise security guarantee ownership and control enforcement. Audit logs and accountability systems ensure a certain process.[32] The general idea of homomorphic encryption is to provide a way to conduct calculations on encrypted data.[33] A practical application example would be to perform searches on encrypted data stored centrally in the

complaint anyway. The US appears to be focusing heavily upon data privacy, particularly following the 2018 Facebook/Cambridge Analytica data scandal."

[25] See CCPA fact sheet, California Lawyers Association, https://calawyer.org, 15.22.2022.

[26] Der lange Arm der USA – Neues Cloud-Gesetz in Kraft (cloudcomputing-insider.de), 30.3.2022; ICTLC Italy, What's new in Personal Data Transfers from the EU to the USA? – ICTLC, 15.11.2022.

[27] Greenwald/MacAskill, Edward Snowden: the whistleblower behind the NSA surveillance revelations, The NSA files, The Guardian (2013) 15.11.2022.

[28] Der lange Arm der USA – Neues Cloud-Gesetz in Kraft (cloudcomputing-insider.de), 30.3.2022.

[29] United States National Security Requests FAQs – Transparency Report Help Center (google.com), 16.3.2022.

[30] For Google see Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht, 16.3.2022.

[31] For anonymization one might use Differential Privacy: ZHAO/CHEN, A Survey on Differential Privacy for Unstructured Data Content (2022) https://doi.org/10.1145/3490237.

[32] Zeadally/Badra, Privacy in a Digital, Networked World (2015) 46f.

[33] Al Badawi et al. „OpenFHE: Open-source fully homomorphic encryption library" Cryptology ePrint Archive (2022), https://ia.cr/2022/915, 15.11.2022.

cloud. In such an environment, clients can send encrypted search queries to a server. The server subsequently conducts the search and sends the result back to the user without being able to decrypt the original plain text itself. This anonymization of data is technically difficult and is currently at least very rare.[34]

In general, we advise to give preference to European cloud services, such as GaiaX,[35], Scalingo,[36] and Outscale,[37] which must comply to European Law and the GDPR.

7. Conclusion

Today, many companies use cloud offerings from Google, Amazon or Microsoft for areas such as CRM, CMS, project management, security or data storage. However, an acceptable balance must be struck between the advantages and disadvantages, with particular emphasis on the protection of personal rights as fundamental rights of our society.

The problems with data protection issues regarding data transfer in the US are well known[38] and are, failing not only an adequacy decision but a real change in U.S. laws, difficult to solve. Encryption is only useful if the cloud service providers do not have the key to decrypt the data. Moreover, it is not possible to check from the outside whether data has been decrypted, so uncertainty remains, especially after the NSA scandal, and one must be aware of the fact that one‘s own data on foreign servers may be viewed. Anonymization usually takes place too late and is not always implemented in a technically form. This makes it clear that a high data protection standard in Europe also needs strong European companies that offer real alternatives to the leading (U.S.) companies. Ideally, only private clouds located in Europe and run by European companies should be used.[39]

Apart from contract law and data protection issues, Europe is losing out on technology, innovation and know-how. As is currently evident with Europe’s dependence on Russian gas and energy, this heavy dependence on one partner is generally not advisable. Particularly in view of the massive digitization efforts in Europe, this must be accompanied by sensible risk management and resilient European systems. The distribution injustice refers not only to the economic value of the data directly, but also to the economic value of the BigData and, above all, its possible (future) analysis. European companies must have access to this data. On top of that we will have to start a general debate about what should be allowed and where we need borders for the data economy. It is high time that Europe starts to act.

“*Technology is a useful servant, but a dangerous master*.” Christian Lous Lange

8. Literature

Al Badawi, Ahmad et al, „OpenFHE: Open-source fully homomorphic encryption library“ Cryptology ePrint Archive (2022), https://ia.cr/2022/915, 15.11.2022.

A-SIT, BKA, Österreichisches Informationssicherheitshandbuch, Cloud Computing, 15.11.2022.

Bauer, Matthias, Das Recht des Technischen Produkts, Springer, (2018) Wiesbaden.

Blaha, Ralf/Marko, Roland/Zellhofer, Andreas/Liebel, Helmut, Rechtsfragen des Cloud Computing Vertragsrecht – Datenschutz – Risiken und Haftungen, Medien und Recht Verlag (2011) Wien.

[34] GENTRY, Fully Homomorphic Encryption Using Ideal Lattices (2009), 444-gentry.dvi (cmu.edu), 15.11.2022.

[35] https://gaia-x.eu, 15.11.2022.

[36] https://scalingo.com, 15.11.2022.

[37] https://en.outscale.com, 15.11.2022.

[38] See especially ECJ C-311/18 of 16.7.2020 (Schrems II); also DSB GZ D155.027, 2021-0.586.257; NOYB: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk.pdf, 15.11.2022; CNIL Entscheidung Anfang 2022: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply, 15.11.2022; https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf, 15.11.2022; LG München, 3 O 17493/20 „google fonts“.

[39] Papenfuss, Die 10 besten Cloudspeicher, 7.3.22, Die 10 besten Cloud-Speicher, heise Download, 15.3.2022.

Bomhard, David/Baum, Andreas, Cybersecurity in outsourcing and cloud computing: a growing challenge for contract drafting, 27.4.2021, online: Cybersecurity in outsourcing and cloud computing: a growing challenge for contract drafting, SpringerLink (fh-joanneum.at), 15.11.2022.

BSI, BSI – Grundlagen – Cloud Computing Grundlagen (bund.de), 17.3.2022.

California Lawyers Association, https://calawyer.org, 15.22.2022.

CCPA Facsheet, https://oag.ca.gc/system/fines/attachments/press_releases/CCPA, 15.11.2022.

Cloudcomputing Insider, Der lange Arm der USA – Neues Cloud-Gesetz in Kraft (cloudcomputing-insider.de), 30.3.2022.

CNIL Entscheidung Anfang 2022: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply, 15.11.2022; https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf, 15.11.2022.

Digital Business Cloud, Cloud-Architektur: Die 11 wichtigsten Trends für 2022 (digitalbusiness-cloud.de), 15.11.2022.

DSB GZ D155.027, 2021-0.586.257.

ENISA's PETs Maturity Assessment Repository, Nov. 2018, https://www.enisa.europa.eu/publications/pets-maturity-tool.

ECJ C-362/14 of 06.10.2015 (Schrems I); ECJ C-311/18 of 16.07.2020 (Schrems II).

Edpb.europa.eu: dk_sa_standard_contractual_clauses_january_2020_en.pdf (europa.eu), 15.11.2022.

EU: Questions & Answers: EU-U.S. Data Privacy Framework (europa.eu), 15.11.2022.

EU Clouds: https://gaia-x.eu, https://scalingo.com, https://en.outscale.com, 15.22.2022.

Frässdorf, Henning, Rechtsfragen des Zusammentreffens gewerblicher Schutzrechte, technischer Standards und technischer Standardisierung, Gabler (2009) Hamburg.

Gentry, Craig, Fully Homomorphic Encryption Using Ideal Lattices, Standford University and IBM Watson (2009), 444-gentry.dvi (cmu.edu), 15.11.2022.

Greenwald, Glenn/MacAskill, Ewen/Poitras, Laura: Edward Snowden: the whistleblower behind the NSA surveillance revelations (2013), Edward Snowden: the whistleblower behind the NSA surveillance revelations, The NSA files, The Guardian, 15.11.2022.

Heise.de, Die Vorteile und Nachteile des Cloud-Computing, heise Download, 15.11.2022.

ICTLC Italy, What's new in Personal Data Transfers from the EU to the USA?, What's new in Personal Data Transfers from the EU to the USA? – ICTLC, 15.11.2022.

Knyrim, Rainer (Hg), Der DatKomm, Praxiskommentar zum Datenschutzrecht – DSGVO und DSG, 12. Lfg, Art. 44–50, Manz'sche Verlags- und Universitätsbuchhandlung (2018) Wien.

LG München, 3 O 17493/20 „google fonts".

Manhardt, SANDRA, Der „Software as a Service"-Vertrag, LexisNexis, (2012) Wien.

Mell, Peter/Grance, Timothy (September 2011) The NIST Definition of Cloud Computing (Technical report), National Institute of Standards and Technology: U.S. Department of Commerce, doi:10.6028/NIST.SP.800-145.

Minnich, Sebastian, https://www.heise.de/download/blog/Die-Vorteile-und-Nachteile-des-Cloud-Computing-3713041, 15.11.2022.

NOYB: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk.pdf, 15.11.2022; New US Executive Order unlikely to satisfy EU law (noyb.eu), 15.11.2022.

Papenfuss, Florian, die 10 besten Cloudspeicher, 7.3.22, Die 10 besten Cloud-Speicher, heise Download, 15.3.2022.

Pöschl, Magdalena, https://staatsrecht.univie.at.at/fileadmin/user_upload/i_staatsrecht/Poescl/Publikationen/1997_UEber_Gleichheit_und_Verhältnismäßigkeit.pdf, 7.11.2022.

RENO, NV, September 19, 2019, Half-Yearly Review Shows $150 billion Spent on Cloud Services and Infrastructure | Synergy Research Group (srgresearch.com), 15.11.2022.

The White House, Fact Sheet: EO to Implement the EU-U.S. Data Privacy Framework, 7.10.2022.

Zeadally, Sherali/Badra, Mohamad, Privacy in a Digital, Networked World, Springer, (2015).

Zhao, Ying/Chen, Jinjun, A Survey on Differential Privacy for Unstructured Data Content, ACM Comput. Surv. 54, Article 207 (January 2022).