De iurisprudentia et iure publico
JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT
JOURNAL OF LEGAL AND POLITICAL SCIENCES
HU ISSN 1789-0446
Kiadja:
Magyar Jog- és Államtudományi Társaság
Hungarian Association of Legal and Political Sciences

Mészáros, János PhD Student,
University of Szeged Faculty of Law and Political Sciences
Department of Political Science

IX. évfolyam | Vol. IX
2015/1. szám | No. 1/2015
Tanulmány | Article
www.dieip.hu

Two different approaches of the data protection law: the European Union and the United States

I. The meanings of privacy and the different approaches of data protection

It is difficult to describe what "privacy" is, because the meaning of "private" differs in society and it constantly changes through the ages. There were public restrooms at Ephesus[1] two thousand years ago, and these days it would be invasion of privacy if someone watched our living room through the windows[2].

Historically the "private person" was who didn't participate in the public life which meant pejoratively that the person didn't want to participate or he had a lack of capacity to do it.

It was rude to guard one's "private" life from the public until the twentieth century and only just a few people could do that. In the 20th century our life retreated from squares into offices, houses and institutions, thus privacy became a protected right.

In the last decade this private life in our home and workplace was changed because of the digital age: although our modern life no longer takes place in the public eye, but the participation in the digital world made us exposed virtually. There is no choice about participating in the digital life: we have to apply to our courses online at the university, receive our messages via email and working on a computer which is usually a part of a network in our workplace. Even a big part of our communication with friends and classmates goes through to the internet especially when our friends or we are abroad and this tendency forces us to voluntarily disclose information about our life: the place we visit, the movies we watch and the people who are our friends. The desire to invade our privacy comes no longer only from the governments these days but also from the companies and their goal is to be better than their competition by learning the consumer's habits and desires.

There is a big difference in the interpretation of privacy between Europe and the United States which led to a different legal environment about data privacy. These differences made much more problems than just a cultural misunderstanding: it led to transatlantic legal and trade conflicts (the significant parts of these conflicts were solved by the Safe Harbor Agreement in 2000).

The different approaches of privacy resulted different regulations, thus there are two general approaches to regulate privacy in the countries of the world:[3]

---

[1] Ephesus (Turkish: Efes) was an ancient Greek city, and later a major Roman city, on the coast of Ionia, near present-day Selçuk, İzmir Province, Turkey.

[2] Whitman, James Q.: *The Two Western Cultures of Privacy: Dignity versus Liberty*. The Yale Journal, Faculty Scholarship Series, 2004. p. 1154.

[3] Lothar Determann: *Determann's Field Guide to International Data Privacy Law Compliance*. Edvard Elgar Publishing Limited, 2012. p. 8.

1. **The omnibus regulation**: a comprehensive approach which means that a single law protects personal data in all industries and most contexts. The single omnibus data protection statue can cover the private and public sector both. This is the concept of the European Union.
2. **Sectoral approach**: it means that the data protection is regulated on a sector-by-sector basis. Different industries have different regulation and some areas are not regulated at all. The public and the private sectors are regulated by different statues.[4] The best example for this approach is the United States.

II. Worldwide privacy rules and guidelines

The **Universal Declaration of Human Rights** was adopted in 1948 by the United Nations General Assembly. It is legally not binding but numerous parts of the Declaration protect privacy, especially the Article 12 which does it explicitly:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The **OECD Guidelines** established eight fundamental principles for the protection of personal information in 1980: *collection limitation, data quality, purpose specification, limitation of using the data, security safeguards, openness, individual participation, accountability*.[5]

The **United Nations Guidelines for the Regulation of Computerized Personal Data Files**, adopted by General Assembly resolution 45/95 of 14 December 1990, contains recommendations for national legislatives about data privacy principles. Thees recommendations are principle of lawfulness and fairness, principle of accuracy, principle of the purpose-specification, principle of interested-person access, principle of non-discrimination, power to make exceptions, principle of security, supervision and sanctions, transborder data flows, field of application.[6]

III. The European Union

Privacy is a highly respected value in the European Union. It is protected in the constitutions of the Member States and in the constitutional documents of the European Union.

The core of the European privacy is the protection of the right to respect and the personal dignity. The most important areas of privacy are the rights to someone's image, name, reputation and the right to "self-determination" which is the ability to control the information that is disclosed about ourselves.[7] The base of these rights is the personal control one's public image.

The EU data protection laws affect most companies of the world because their direct or indirect business partners have to comply with the EU regulation.

The **European Convention on Human Rights** is an international treaty to protect human rights and fundamental freedoms in Europe. Drafted in 1950 by the newly formed Council of Europe, the convention entered into force in 1953. Each member states are part of the Convention and new members are expected to ratify it.

---

[4] Daniel J. Solove & Paul M. Schwartz: *Privacy Law Fundamentals*. International Association of Privacy Professionals, 2011. p. 165.

[5] Péterfalvi Attila: *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC Lap- Könyvkiadó Kft., Budapest, 2012. p. 37.

[6] United Nations Guidelines for the Regulation of Computerized Personal Data Files, http://www.refworld.org/pdfid/3ddcafaac.pdf (2014. augusztus 25.)

[7] Whitman, James Q.: i. m. p. 1161.

The Convention protects the privacy in the Article 8 which provides the right to respect one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society":

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

As a part of the EU constitutional law, the **Charter of Fundamental Rights of the European Union**[8] regulates privacy:

Article 8, Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

The **Treaty on the Functioning of the European Union**[9] specifically lays down a legal basis for action:

Article 16

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

The European integration both increased the sharing of data among Member States and generated new demands for personal data within separate Member States.

The **Data Protection Directive**[10] contains the fundamentals of the EU data protection, which came into force in 1995. The Directive was necessary because of the differences in the statutory protections of the countries. The goals of the Directive are to provide the free flow of personal data and to protect the individual's rights regarding their personal data. These objectives can be seen as two opposite interests between the companies and the individuals thus the Directive establishes obligations for the processors of personal data and provides rights for the individuals.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protect personal data and privacy and promoting good practice in the EU

[8] The Charter of Fundamental Rights of the European Union brings together in a single document the fundamental rights protected in the EU. Proclaimed in 2000, the Charter has become legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009.

[9] The two principal treaties on which the EU is based are the Treaty on European Union (TEU; Maastricht Treaty, effective since 1993) and the Treaty on the Functioning of the European Union (TFEU; Treaty of Rome, effective since 1958). These main treaties (plus their attached protocols and declarations) have been altered by amending treaties at least once a decade since they each came into force, the latest being the Treaty of Lisbon which came into force in 2009.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

institutions and bodies. The position was established by the Regulation No 45/2001.[11] The Supervisors main tasks are monitoring the processing of personal data by the EU administration (supervision), advising on policies and legislation that affect privacy (consulting), and cooperating with similar authorities to ensure consistent data protection (cooperation). He also monitors new technologies that might have impact to the data protection.

Peter Hustinx and Giovanni Buttarelli were appointed as European Data Protection Supervisor (EDPS) and Assistant Supervisor by a joint decision of the European Parliament and the Council. Assigned for a five-year term, they took office in January 2009.

The most important task of the Supervisor is to supervise personal data processed by EU institutions and bodies.[12] He makes "prior checking" when EU institutions and bodies carry out operations processing personal data with specific risks.

The EDPS can make inquires when he gets a complaint from EU staff members or from other people about mishandling their personal data by EU institution or body. He can also inquire by his own initiative. The Supervisor consults with the EU legislatives about proposals for new legislation and soft law instruments that can affect the personal data protection.

The cooperation covers specific issues such as the interpretation of the EU Data Protection Directive, as well as more structural collaboration together with other data protection authorities.

The EDPS can also intervene in cases before the Court of Justice, the Court of First Instance and the Civil Service Tribuna.[13]

It is important that the EDPS is not the supervisor of the national data protection agencies or any national institutions, bodies and organizations.

The **Article 29 Working Party** is an independent European working party that deals with issues relating to the protection of privacy and personal data. It was created by the Article 29 of the Directive 95/46/EC ("Data Protection" directive) and the Directive 2002/58/EC ("Electronic communications" directive).[14]

The data protection authorities of the EU Member States are members of the Working Party. Apart from them, the European Data Protection Supervisor and the representative of the Commission also participate in the Working Group's activities. The member states of the European Economic Area have the status of observer in this group, as well as a number of candidate Member States. The "Data Protection" section of the Directorate-General for Justice, Freedom and Security of the European Commission is in charge of the Working Party's administration and clerical tasks.

The Article 29 Working Party's missions comprise all issues related to the application of national provisions that were adopted in implementation of the Directive 95/46/EC and the Directive 2002/58/EC.

The Article 29 Working Party regularly issues opinions, publishes working documents and resolutions related to the protection of privacy and personal data, aiming towards a harmonized application of these directives in the EU Member States. The Article 29 Working Party is also in charge of providing expert opinions to the European Commission and on codes of conduct at Community level.

---

[11] Regulation (EC) No 45/2001 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2000. 12. 18.)

[12] Gombos Katalin: *Az Európai Unió jogának alapjai*. Complex Kiadó jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2012. p. 88.

[13] Osztovits András (szerk): *EU-jog* , HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2012. p. 163.

[14] Commission for the Protection of Privacy, www.privacycommission.be

IV. The United States

The core of privacy in the United States is the "sanctuary of home". The freedom from the intervention of the government, entities and other person is a fundamental right which plays a big role in the meaning of privacy in the American liberal society.

In 2013, the United States had more than 20 federal sectoral laws concerned privacy (e. g. Bank Secrecy Act, Cable Communications Policy Act) and hundreds of such laws on state level (e. g. California Breach Notification Statue).

The sectoral regulation means that different industries have different regulations if they are regulated at all (e. g. the Children's Online Privacy Protection Act provides protection for the children under 13 years old but there is no such law that generally regulates privacy for adults on the Web).

There is no official Data Protection Authority in the United States but the Federal Trade Commission[15] (FTC) forces companies against unfair and deceptive trade practices.

The FTC uses this authority to pursue companies when they fail to implement minimal data security measures or they don't follow these rules. The FTC enforces privacy regulations also in specific areas (e. g. children's privacy, spamming, health data).

The USA Attorney General[16] and the State Attorneys General have the power to enforce privacy regulations. For example, they can bring civil actions on behalf of state residents for violations of the Health Information Privacy and Security Rules.[17]

IV.1. Federal constitutional law

The United States Constitution doesn't protect privacy explicitly but several Amendments do it from different aspects of privacy: The First Amendment's right to speak anonymously; The Third Amendment's protection of the home from quartering of troops; The Fourth Amendment's protection against unreasonable searches and seizures; The Fifth Amendment's privilege against self-incrimination.

IV.2. Federal Statutory Law

There are more than 20 sectoral statues providing privacy protection. The most important statues are:

The CAN-SPAM Act (2003) which provides penalties for the transmission of unsolicited mail.

The Gramm-Leach-Bliley Act (1999) requires privacy notices and provides opt-out rights when financial institutions seek to disclose personal data to other companies.

The Children's Online Privacy Protection Act (1998) restricts the use of information which was gathered from children under age 13.

The Health Insurance Portability and Accountability Act (1996) gives the Department of Health and Human Services the authority to promulgate regulations governing the privacy of medical records.[18]

---

[15] The Federal Trade Commission (FTC) is an independent agency of the United States Government, established in 1914 by the Federal Trade Commission Act. Its principal mission is the promotion of consumer protection and the elimination and prevention of anti-competitive business practices.

[16] The United States Attorney General is the head of the United States Department of Justice. He is responsible for legal affairs and he is the chief law enforcement officer of the United States government. The attorney general is considered to be the chief lawyer of the U.S. government.

[17] The Health Information Technology for Clinical and Economic Health (HITECH) Act

[18] Other Acts with the purpose of the protection of privacy: Fair Credit Reporting Act (1970), Bank Secrecy Act (1970), Privacy Act (1974), Family Educational Rights and Privacy Act (1974), Right to Financial Privacy Act

IV.3. Decisions of the Supreme Court

The Supreme Court has an important role in the United States' legal system because it can interpret the law or make it out of effect. The Court has a lot of important decisions about privacy and these days there are more cases concerned privacy because of the digital age.

Some important cases about privacy: Reno v. Condon, Kyllo v. USA, City of Indianapolis v. Edmond, Board of Education v. Earls, Connecticut Dept. of Public Safety v. Doe, Lawrence v. Texas, Doe v. Chao, Brendlin v. California, Illinois v. Cabelles, Hiibel v. Sixth Judicial District Court.

IV.4. State Constitutional Law

Ten States protect privacy directly in their constitution: Alaska (article I, § 22), Arizona (article II, § 8), California (article I. § 1), Florida (article I, § 23), Hawaii (article I, § 6), Illinois (article I, § 12), Los Angeles (article I, § 12), Montana (article II, § 10), South Carolina (article I, § 10), Washington (article I, § 27).

IV.5. State Statutory Law

The biggest part of the privacy law in the United States can be found in state law and most of the federal statues permit state laws to exceed them. Privacy tort and data breach notification rules are state law.

V. Collision between the European Union and the United States

It is a basic rule in the data protection regulation of the European Union that the transfer of personal data outside the EU is prohibited except certain conditions. The reason of this restriction is the fear of losing data protection standards in third countries.

EU Data Protection Directive[19], Chapter IV, Article 25:

1. The Member States shall provide that the **transfer to a third country of personal data which** are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question **ensures an adequate level of protection**.

The paragraph 2 lists the criteria should be taken into consideration about adequacy:

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

(1978), Foreign Intelligence Surveillance Act (1978), Privacy Protection Act (1980), Cable Communications Policy Act (1984), Electronic Communications Privacy Act (1986), Computer Matching and Privacy Protection Act (1988), Video Privacy Protection Act (1988), Telephone Consumer Protection Act (1991), Driver's Privacy Protection Act (1994), Communications Assistance for Law Enforcement (1994), Personal Responsibility and Work Opportunity Reconciliation Act (1996), Identity Theft and Assumption Deterrence Act (1998), USA-PATRIOT Act (2001), Video Voyeurism Prevention Act (2004).

[19] Directive 95/46/EC of the European Parliament and of the Council

These are the criteria which should to be evaluated by the Article 29 Working Party in its opinion regard to the adequacy of a third country.[20] The Working Party gave an opinion about the level of data protection in the United States in 1999:

"Privacy and data protection in the United States is found in a complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation."

"Nevertheless, the Working Party takes the view that the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[21]

The decision of the Working Party affects companies with headquarters in the United States directly because their subsidiaries in the EEA are not allowed to share personal data of the employees, contractors and customers. The regulation also indirectly affects all companies that have business partners and suppliers in Europe because they are prohibited to send personal data.[22] The headquarters of the multinational companies would like to be in control over worldwide operations by centralizing decision-making and data processing because it is easier, faster and cost effective.

There are plenty of options and solutions to send personal data to companies residing in third countries that are not adequate from the point of view of the EU data protection law:

a) Data subject's consent
b) Necessity under contract
c) Interest of the data subject
d) Necessity under statues
e) Safe Harbor
f) Binding corporate rules
g) Data transfer agreement
h) Other methods

V.1 The data subject's consent

The Data Protection Directive permits[23] the transfer of personal data to the third country which does not ensure adequate level of protection if the data subject gives his consent unambiguously to the proposed transfer. In practice, the consent is valid only if it is prior the data transfer, freely given, specific, written and the data subject was informed properly.

The prior consent has to be a positive act which is given in advance the data transfer (opt-in) thus it is not acceptable if the data subject can object against to the transfer only after it occurred (opt out).

Any doubt as to whether the consent has really been given in advance would make it inapplicable.[24] (e. g. the Working Party recommended[25] the use of boxes on Internet sites to be ticked by the data subject as an indication of his prior consent, thus using preticked boxes fails to fulfil the condition that consent must be a clear and unambiguous indication of wishes.)

---

[20] The countries that were found adequate by the Working Party: Switzerland, Argentina, Canada, the Bailiwicks of Guernsey and Jersey, Isle of Man and Israel.

[21] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *OPINION 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp15en.pdf (2013. 02. 18.)

[22] Lothar Determann: i. m. p. 26.

[23] Directive 95/46/EC, Article 26. 1§ (a)

[24] Article 29 Working Party: *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC*, 1995. p. 6.

[25] Article 29 Working Party: *Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC*, WP 90, of 27 February 2004. point 3.2.

The consent which is freely given means a real choice for the data subject thus it is unacceptable when the data subject hasn't other option (e. g. passenger data has to be sent before the departure of the airplane)[26]

V.2. Necessity under contract

The transfer of data is allowed if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request.[27]

In this case the contractual obligations which are desired to be fulfilled by the data subject cannot be carried out without the data transfer (e. g. travel agencies have to send the personal data of the traveller to hotels and airlines, data has to be sent for shipment of packages via post) thus it is necessary.

V.3. Interest of the data subject

Under this option the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and the third party.[28]

This case is similar to the "necessity under contract" because it has to pass the "necessity test" which means that there has to be a close and substantial connection between the data subject's interest and the purposes of the contract. (e. g. international groups manage stock option schemes for certain categories of their employees, thus they have to conclude contract with financial service providers for the interest of the beneficiary data subject)

V.4. Necessity under statues

Data transfers can be required by European laws but this is a rare case (e. g. arrangements for cross-border employee secondments where employers have to share data with each other and authorities in both countries).

V.5. Safe Harbour

The United States Department of Commerce and the EU Commission negotiated the Safe Harbor Agreement because the regulation of data protection in the USA wasn't found adequate by the EU.

The Safe Harbor Agreement regulates the onward transfers of personal data from the EU to the USA and from the USA to elsewhere. The agreement doesn't cover direct data transfers from the EU to any other country than USA.[29]

Companies in the United States can voluntary adhere to the Safe Harbor Principles through self-certification and after that these organizations will be able to provide adequate level of protection from the European Union's point of view.[30]

Only those companies can join the SH program that are under the jurisdiction of the Federal Trade Commission (FTC). US air carriers and ticket agencies can join if they are under the jurisdiction of the Department of Transportation.

---

[26] Article 29 Working Party: *Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States. 2002.* p. 7.
[27] Directive 95/46/EC, Article 26. 1§ (b)
[28] Directive 95/46/EC, Article 26. 1§ (c)
[29] Lothar Determann: i. m. p. 31.
[30] Daniel J. Solove & Paul M. Schwartz: i. m. p. 174.

The onward data transfer from the Safe Harbor participant to other data controller requires the notice and\or the consent of the data subject: notice and providing choices (opt out) are enough in general but opt in is necessary when sensitive data is transferred and there is no exception for intra-group transfers. Data transfer agreement is not required but the recipient data controller has to be a Safe Harbor member or otherwise a subject of the EU data protection law.

V.6. Binding Corporate Rules (BCR)

"Binding Corporate Rules are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define a global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection."[31]

The BCR were developed by the Article 29 Working Party which can permit intra-group transfers of personal data for multinational corporations and international organizations.

The BCR form a stringent, intra-corporate global privacy policy or code in practice which reflect and safeguard the EU data protection rules in a group of companies. The Binding Corporate Rules don't legitimize data transfers outside the organization thus it is not possible to transfer data to customers, suppliers, business partners, government agencies and other entities.

There are no official pre-approved templates of the Binding Corporate Rules but the Article 29 Working Party has issued a guideline on what topics need to be addressed in the BCR and how they can be negotiated and approved by the national authorities.

BCR must contain in particular: privacy principles (transparency, data quality, security, etc.), tools of effectiveness (audit, training, complaint handling system, etc.) and an element proving that BCR are binding (the BCR has to be enforceable by the "data subject" and the BCR must indicate a clear duty of cooperation with data protection authorities in the EU).

The problem with the Binding Corporate Rules is that the approval has to be acquired from each data protection authority in each of the countries from where the personal data would be transferred. The Working Party wanted to make this approval process easier by developing the "standard application" which means that just one single copy of a form should be submitted to one data protection authority ("lead data protection authority").[32]

V.7. Data Transfer Agreement (standard contractual clauses)

The data transfer agreement is concluded between the data exporter (within the EEA) and the importer (outside the EEA) which can be an adequate safeguard with the approval of the competent authority.

The standard contractual clauses (SCC) are templates of the data transfer agreements that were promulgated by the European Commission. There are two types of SCC: the first types of agreements were made for data transfers to data controllers and the second types were made for transfers to data processors.[33]

The parties of the SCC are under the force of the EU data protection law thus they have to follow its rules and it is important that the contractual obligations can be enforced by the data

[31] Overview on Binding Corporate rules http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (2015. 01. 10.)

[32] Article 29 Data Protection Working Party: *Explanatory Document on the Processor Binding Corporate Rules*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation /files/2013/wp204_en.pdf (2012. 04. 19.)

[33] Lothar Determann: i. m. p. 30.

subject as a third-party beneficial against either party in a local court under local law. The parties are permitted to modify the SCC or make their own agreement.

Companies are allowed to implement the SCC in a wider contract and add other clauses if the modification won't contradict it or derogate the fundamental rights or freedoms of the data subjects.[34]

It is possible that the parties add more safeguards and rights of the data subject but these additional clauses are not covered by the third party beneficiary rights thus the data subjects are not able to enforce them.[35]

The problems with the companies own (or modified) data transfer agreements and the modified SCC are that these documents have to be approved by local authorities which can be time and money consuming and they will be under the scope of the supervising of the EU and local authorities.

The SCC made for transferring data to data processors outside the EU have to be signed by the contractors (subprocessors, e. g. payroll provider) of the data processor which is difficult or nearly impossible in a lot of cases (e. g. a financial service provider would have to make the contract signed with its credit card provider, internet service and financial background provider).

The advantages and the disadvantages of the compliance methods

	advantages	**disadvantages**
Consent	-both can be suited by the interest of the parties -cheap and fast	-there are situations where the consent cannot be applied (e. g. the consent of the employee does not count freely given)
Necessity under contract		-the "necessity" can be scrutinized by the data protection authorities
Binding Corporate Rules	-in a certain organization the BCR are suitable to send any type of data to anywhere on the world	-data can be sent only inside of the organization -there are no official templates -BCR have to be approved by the Data Protection authorities -the process is time consuming and expensive
Standard Contractual Clauses	-the SCC are suitable to send any type of data to anywhere on the world -there are templates	-onward data transfers require the recipient to sign the data transfer agreement
Safe Harbor	-the application process is easy, cheap and fast	-geographically restricted: data can be sent directly only into the United States

***Table 1*:** the advantages and the disadvantages of the compliance methods

[34] Article 29 Data Protection Working Party: *Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp38en.pdf (2012. 05. 22.)

[35] European Commission: *Standard contractual clauses for the transfer of personal data to third countries - Frequently asked questions,* http://europa.eu/rapid/press-release_MEMO-05-3_en.htm (2001. 01. 26.)

VI. The future: the proposed EU regulation and the United Nations resolution

"I will include easier access to one's own data in the new rules. People must be able to easily take their data to another provider or have it deleted if they no longer want it to be used."
- EU Justice Commissioner Viviane Reding (January 2012)

VI.1. The Proposed EU regulation

The European Commission revealed a draft legislative package to establish a unified European data protection law on 25 January 2012. The package includes a draft "General Data Protection Regulation" (the "Regulation") that will be directly applicable in all Member States of the European Union replacing the different data protection laws currently in force in the different Member States.[36]

The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for US companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 2 % of worldwide turnover.[37]

The biggest proposed changes of the EU data protection law:

a) The proposed EU data protection regulation will be applied for all non-EU companies without any establishment in the EU, provided that the processing of data is directed at EU residents. This may force for example US companies not only to comply with EU law, but also to establish a data protection management, for example by appointing a "European" data protection officer.

b) As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data (opt-in), other than in cases in which the data protection regime explicitly allows the processing of personal data.

c) The Regulation will make a safe transfer of data outside of the EU (including the procession of data in clouds) easier in the event that the parties involved commit themselves to binding corporate rules.

d) New privacy rights, including data subject's "right of portability" and the "right to be forgotten", will be established in the EU. The "right of portability" will allow a transfer of all data from one provider to another upon request, for example transfer of a social media profile or email, whereas the "right to be forgotten" will allow people to wipe the history clean.

e) The processing of data of individuals under the age of 13 will require parental consent in general which will make it more difficult for companies to conduct business which is aiming at minors.

f) All companies will be required to notify EU data protection authorities and individuals whose data are concerned by any breaches of data protection without undue delay that is within 24 hours.

g) A strict sanction regime will be established in case of breach of the EU data protection law allowing data protection authorities to impose penalties of up to 2 % of a company's worldwide turnover in the case of severe data protection breaches.

[36] M Law Group, http://www.mlawgroup.de (2014. 12. 20.)

[37] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (2014. 05. 7.)

The Data Protection Directive of 1995 stuck in the lawmaking process for more than two years. It is expected therefore that the Regulation to come into force in medium term only, which gives to all lobby groups enough time to try to engage lawmakers to change or amend the draft Regulation.

VI.2. The proposed United Nations resolution

The future of the data protection law depends on a lot of circumstances but the most important thing is that the USA has the "hegemony of the web": the most dominant web companies (e. g. Facebook, Google, Microsoft, Twitter, even Apple with its web services) have been incorporated in the USA and their headquarters are there.

Even the Internet Corporation for Assigned Names and Numbers (ICANN) is based in the States which is a non-profit organization that is "assigning domain names and establishing common web standards"[38]

This hegemony was not a problem until the NSA[39] scandal: Edward Showden, who was an employee of the National Security Agency, revealed that the agency is able to access information stored by major US technology companies, often without individual warrants, as well as mass-intercepting data from the fibre-optic cables which is the backbone of the global phone and internet networks.

The agency has also worked to undermine the security standards upon which the internet, commerce and banking rely.[40] A lot of politicians and leaders were under the NSA surveillance (e. g.: Angela Merkel) which growth the scandal bigger and made the leaders angry.

Germany and Brazil proposed United Nations resolution calling for stronger internet privacy protection, echoing an impassioned speech that Brazilian president Dilma Rousseff delivered to the organization in September, after it was reported that the NSA conducted surveillance in her office. The UN General Assembly resolutions are not legally binding but they reflect the opinion of the world and carry moral and political weight. The draft resolution proposes expanding the protection guaranteed in a key global human rights treaty, the International Covenant on Civil and Political Rights, to electronic communications and privacy.[41]

German Ambassador Peter Witting asked, while introducing the jointly sponsored German-Brazilian resolution to the UN General Assembly committee that deals with human rights:

"Today, there seem to be hardly any technical limitations for accessing, storing or combining personal data. But should everything that is technical feasible also be allowed? Where do we draw the line between legitimate security concerns and the individual right to privacy? And how do we ensure that human rights are effectively protected both offline and online?"

[38] Amar Tooron: *Will the global NSA backlash break the internet?*. http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization (2013. 11. 8.)

[39] The National Security Agency (NSA) is the USA's signals intelligence agency which focuses on overseas, rather than domestic, surveillance. It is the phone and internet interception specialist of the USA, and is also responsible for code breaking.

[40] The Guardian: *The NSA Files*, http://www.theguardian.com/world/the-nsa-files (2014. 11. 25.)

[41] Peter James Spielmann: *Brazil, Germany debut on web privacy resolution*. http://bigstory.ap.org/article/brazil-germany-debut-un-web-privacy-resolution (2013. 11. 7.)