EU-USA PRIVACY PROTECTION LEGISLATION AND THE SWIFT BANK DATA TRANSFER REGULATION: A SHORT LOOK

by

RASTISLAV FUNTA*

Although the European Union (EU) and the United States (USA) share common values of democracy, rule of law and respect for human rights and fundamental freedoms, there is a critical importance of providing a high level of effective protection of personal data, in particular in the international financial transactions (SWIFT). In a globalizing economy a widespread increase in the availability and use of computers and computer networks creates threats to the privacy. To protect individuals against inappropriate uses of personal data and to ensure the economic benefits of trade liberalization, a more stringent protection of data privacy is needed. The aim should be here protection of personal data while processing and exchanging information for law enforcement purposes. European Commission's Communication from 10 June 2009 states that "Union must be a driving force for behind the development and promotion of international standards for personal data protection and in the conclusion of appropriate bilateral or multilateral instruments. The work on data protection conducted with the United States could serve as a basis for future Agreements."[1] The purpose of this paper is to examine and analyze the current legal framework on data protection in the EU and USA.

KEYWORDS

Data protection, EU Law, SWIFT, US Law

* JUDr. Rastislav Funta, LL.M. (Budapest) is a PhD Candidate on Faculty of Law at Charles University Prague.

1 COM (2009): An area of freedom, security and justice serving the citizen, 262/4, Brussels, pp. 8-9

1. INTRODUCTION: SWIFT AND PRIVACY

The functioning of the global banking community (GBC) in the 21th century is nearly unthinkable without the Society for Worldwide Interbank Financial Telecommunication (hereinafter SWIFT) system.[2] The SWIFT has revolutionized the international banking community by providing highly secure financial messaging services not only to banks, but brokers, dealers, as well as investment managers as well. In short words it can be described as a secure window to the financial industry. The core of SWIFT is to obtain visibility on cash across banks as well as better control and increase of security and reliability. The right to privacy is acknowledged in many international agreements, e.g. in Article 12 of the Universal Declaration of Human Rights[3] or in Article 17 of the *United Nations International Covenant on Civil and Political Rights*.[4] Both states that *"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."*

Nearly 100 years ago the UK Court of Appeal has decided in the case *Tournier v National Provincial and Union Bank of England*[5] that a bank must maintain the confidentiality of all information derived from the relationship between bank and customer, unless some conditions are met (e.g. disclosure is required by law or the customer has consented to disclosure).

According to Article 1 (1) of the Regulation No 45/2001, the purpose of that regulation is to *"protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."* Such provision can not be separated into two categories, namely a category in which a treatment is examined only on the basis of Article 8 of the ECHR[6] and the case-law of the European Court of Human Rights relating to this article and another category in which such processing is subject to the provisions of Regulation No 45/2001.[7] E.g. Section 3 (1) of the BDSG

---

2 Funta, R. (2010): 1000+ Questions and Answers about EU and EU Law, 2nd Edition, Tribun EU Publishing, Brno, p. 86

3 The Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly on 10 December 1948

4 The International Covenant on Civil and Political Rights (ICCPR) was adopted by the United Nations General Assembly on 16 December 1966

5 Case: Tournier v. National Provincial and Union Bank of England [1924] 1 K. B. 461

defines personal data as any information concerning the personal or material circumstances of an identified or identifiable individual.[8]

The US Supreme Court has recognized in the case *Whalen v. Roe* for the first time the right to privacy information as follows: *"One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."*[9]

2. EUROPEAN UNION PRIVACY PROTECTION LEGISLATION

It is important to mention that under the Lisbon Treaty, protection of personal data is recognized as a fundamental right.[10] Article 16 of the Treaty on the Functioning of the European Union (TFEU) states that: *"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."* Modern EU data protection[11] is guided, in particular, by the following regulations:

- The Charter of Fundamental Rights of the European Union,[12] which entered into force with the Lisbon Treaty, states in Chapter II (Freedoms) in Article 8 that everyone has the right to the protection of personal data concerning him or her. 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

---

6 The 1981 Convention on Data Protection was the first instrument where the right to data protection was explicitly provided. Article 8 ECHR provides that *"Everyone has the right to respect for his private and family life, his home and his correspondence*. and that *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."* But this instrument did not recognise data protection as a separate right.

7 ECJ Case C-28/08 P (Appeal – Access to the documents of the institutions – Document concerning a meeting held in the context of a procedure for failure to fulfill obligations –Protection of personal data – Regulation (EC) No. 45/2001 Regulation (EC) No 1049/2001), of 29 June 2010, point 61

8 Federal Data Protection Act of Germany (Bundesdatenschutzgesetz, BDSG)

9 Case: Whalen v. Roe, 429 U.S. Reports (February 22, 1977), para. 589-604

10 Svoboda, P. (2010): Úvod do evropského práva, 3. vydání, C-H-Beck Praha, p. 278

11 First law on data protection was enacted by the German Federal State of Hessen (07.10.1970)

12 The Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364/3)

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. According to this, the right is seen as an autonomous fundamental right;

- As it is stated in Article 1 of the 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,[13] the Directive shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Further Article 56 of the Directive states that adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;
- Regulation 45/2001/EC[14] shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal (processing of personal data by the Community institutions);
- Directive 2002/58/EC[15] concerns the right to privacy, with respect to the processing of personal data in the electronic communication sector. This general Data Protection Directive has been complemented by other legal instruments, such as the e-Privacy Directive for the communications sector;
- There are also specific rules for the protection of personal data e.g. in police and judicial cooperation in criminal matters (Decision 2008/977/JHA).[16]

---

[13] 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, Official Journal L 281

[14] Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 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, Official Journal of the European Communities L 8/1

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities L 201

[16] Council Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350

3. PRIVACY PROTECTION IN THE UNITED STATES

The U.S., in contrary to the EU, has no single data protection legislation. Also the U.S. Constitution does not contain the word privacy (the right to privacy is not guaranteed by the Constitution). We can divide the privacy rights in the United States into two categories (one part is regulated by the government and another one is under common law). The most important privacy protection legislation can be found in the:

- Fair Credit Reporting Act (the first federal information privacy law in the United States);[17]
- Privacy Act (regulates how U.S. federal government agencies collect, use, and disseminate personal information of citizens. According to the 5 U.S.C. § 552a (e) (1) of the Privacy Act of 1974 the U.S. federal system contains only *"information about an individual as is relevant and necessary to accomplish a purpose of the agency."*);[18]
- Computer Security Act (deals with personal information in federal record systems);[19]
- Computer Matching and Privacy Protection Act (regulates the use of computer matching by U.S. federal agencies);[20]
- Gramm-Leach Bliley Act (privacy rights in relation to information held by financial services institutions[21] like banks or insurance companies)[22] and
- Cybersecurity Act (aimed to secure the US nation's cuber infrastructure).[23]

---

[17] Fair Credit Reporting Act of 1970, 15 U.S.C. §§1681 et seq

[18] Privacy Act of 1974, 5 U.S.C. § 552a

[19] Computer Security Act of 1987, 40 USC Chapter 25 Section 1441, P.L. 100–235

[20] Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. 552a et seq

[21] In the U.S. Supreme Court's 1976 ruling in United States v. Miller the Court found that bank customers had no legal right to privacy in financial information held by financial institutions (see United States v. Miller, 307 U.S. 174 (1939)

[22] Gramm-Leach Bliley Act of 1999, 15 U.S.C. §§ 6801–6809 (The Act requires the Federal Trade Commission ("FTC"), along with the Federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission, to issue regulations to ensure that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually, and before disclosing any consumer's personal financial information to a non-affiliated third party, must give notice and an opportunity for that consumer to "opt-out" from such disclosure. The Act also limits the sharing of account number information for marketing purposes.

[23] The Cybersecurity Enhancement Act of 2010, H.R. 4061

In America, states are able to enact stronger rules and even where the U.S. Congress has created such rules and states are usually allowed to enhance them. As Rotenberg stressed *"we should reject the proposition that police agencies can investigate people and compel disclosure of private information - absent a reasonable indication of criminal activity. The Fourth Amendment of the US Constitution requirements of probable cause of a crime, supported by the judicial issuance of a warrant, is a bedrock principle of the American system of justice. Unless the government can demonstrate that it has a criminal predicate - evidenced by a court order or a grand jury subpoena - the government should not be given access to sensitive or private information about individuals even if that information is maintained by third parties."* [24] The main aim of the protection is to confront global terrorism because secret banking system might be used by terrorists for their illegal operations.

4. WHY IS THE DATA PROTECTION SO IMPORTANT?

Why was it important to the USA to conclude an agreement quickly with the EU? There are several reasons regarding the importance of data protection. This agreement has been highlighted as an important step that should protect personal privacy (in particular by minimizing financial losses). Without a doubt, cooperation with the US should be a priority for the EU in the fight against terrorism. Intelligence operations or security checks are some of the tools which can be used by fighting terrorism.[25] There is a need for money which are used by terrorists to carry out attacks, hence this should be seen as the main point by defending the data protection agreement between EU and USA.

5. A BATTLE ABOUT SWIFT AGREEMENT

After the attacks of 11th September the U.S. government has adopted the U.S. Patriot Act which has expanded the government power regarding money laundering, share of information, etc. The section 215 of the Patriot Act gives the government the power to obtain all business records from the

[24] Rotenberg, M. (2010): Data Protection in a Transatlantic Perspective: Future EU-US international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters, EPIC, Brussels, p. 3

[25] Funta, R. (2010): Common foreign and security policy in terms of the Lisbon Treaty and suppression of international terrorism, International Conference „The Milestones of law in the area of the Central Europe." 18.-20. March, Bratislava

Foreign Intelligence Surveillance Court. The U.S. responses to these attacks were made e.g. through the Terrorist Finance Tracking Program which future goes hands in hands with the EU/U.S. SWIFT agreement.[26] In February 2010, 378 MEPs voted against and 196 in favour, the MEPs rejected the SWIFT interim agreement. There were many arguments against the SWIFT agreement mainly that the US Privacy Act does not protect European citizens and is contrary to the EU law. After a long battle, on July 2010, the European Parliament approved the new SWIFT II-Agreement on bank data transfers to fight against terrorist financing.[27] José Manuel Barroso, president of the European Commission, welcomed the approval with the words that Brussels has *"created a balance between the need to guarantee the security of citizens against the threat of terrorism and the need to guarantee their fundamental rights."*[28] In contrast to the previous version, the definition of terrorism in the new agreement corresponds to the one in the Framework Decision 2002/474/JHA on combating terrorism.[29] The SWIFT II agreement has incorporated new conditions of deleting data after the investigation, the maximum duration[30] of the data transfer which is limited to 5 years (Article 6), only data transfers to countries outside Europe will be checked (Article 7) or the Europol should first check whether a terror suspect is justified (Article 4). European Commissioner Viviane Reding made her statement to the battle as follows *"I remain to be convinced that all these SWIFT transfers are necessary, proportionate and effective to fight terrorism."*[31]

5.1. HOW IT IS RUNNING IN THE PRACTICE?

E.g. Mr X from Munich (Germany) is suspected of terrorism. The United States ask from SWIFT the bank account details of Mr X. Swift sent to the

[26] See more in Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 24 October 2001, 2001HR 3162 RDS, 107th CONGRESS, 1st Session, H. R. 3162

[27] MEPs voted by 484 in favour, 109 against and 12 abstentions

[28] Statement by President José Manuel Barroso on the European Parliament's approval of the agreement on the Terrorist Financing Tracking Programme (TFTP), MEMO/10/309

[29] Terrorism constitutes one of the most serious violations of such principles like the principle of democracy and the principle of the rule of law, principles which are common to the Member States. See Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, *OJ* L 164, 22.6.2002.

[30] As it was decided in the case *Kennedy* "the retention of unused data for an unspecified period is acceptable, as long as this retention matches one of the legitimate purposes for which the data was obtained." See Case: Kennedy v. United Kingdom 26839/05 [2010] ECHR 682, paras. 32 and 42

[31] Viviane Reding, Member of the European Commission responsible for Information Society and Media Privacy: The challenges ahead for the European Union Keynote Speech at the Data Protection Day 2010, European Parliament, Brussels, SPEECH/ 10/16

United States complete data packets from the country or region in which the person is suspected. This means that in the case of Mr X, names of all similar account holders from Bavaria may fall in hands of U.S. investigators, if they have paid money on a given day in a country outside the EU. Also unsuspecting citizens may find themselves targeted by the secret services.

6. FINAL REMARKS

As Aaron wrote: *"privacy protection is an obligation of the state towards its citizens. In America, we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot."*[32] But the view of typical Americans, regarding privacy, did not fully correspond with the statement. Americans do not see it as a fundamental right but rather as a product. Coming from a different historical background or having different ways of getting things done did not solve the problem. The EU-US data protection agreement must respond to the latest technological developments, provide legal certainty and a set of clearly defined rights for EU citizens.[33] Such framework should ensure appropriate data protection and prevent the data from being used for purposes other than counter-terrorism. According to my opinion, several privacy protection questions may be posed before the European Court (until now, many remain unanswered)[34], namely: is the transfer of data in accordance with the principle of proportionality? Has the EU sufficient power to exercise effective supervision of data transfers by Europol? A question, if such an agreement represents a clear violation of EU legislation on data protection should be also answered individually. There is still much work to be done in creating best standards of data and information privacy. Because internet and e-commerce become significant, differences must be reconciled for both economies. The SWIFT agreement, as the first important test of new transatlantic cooperation in the post-Lisbon Treaty, will show us if both sides have chosen the right way for the fight against terrorism.

---

[32] Aaron, D. L. (2001): The EU Data Protection Directive: Implications for the U.S. Privacy Debate. The House Committee on Energy and Commerce, Washington D.C., p. 42

[33] COM (2010): Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A comprehensive strategy on the data protection in the European Union, XXX Final, Brussels, p. 16

[34] See C-54/08 Commission v. Germany; A European Court of Justice (ECJ) decision in the case of the European Commission vs. Germany rules that the Data Protection Authorities (DPAs) needs to be completely independent. The Court ruled that *"the supervisory authorities are the guardians of fundamental rights and freedoms."*

ABBREVIATONS

BDSG Bundesdatenschutzgesetz
DPA Data Protection Authorities
ECHR European Court of Human Rights
ECJ European Court of Justice
EU European Union
FTC Federal Trade Commission
GBC Global banking community
ICCPR International Covenant on Civil and Political Rights
MEPs Members of the European Parliament
SWIFT Society for Worldwide Interbank Financial Telecommunication
TEU Treaty on the European Union
TFEU Treaty on the Functioning of the European Union
UDHR Universal Declaration of Human Rights
UK United Kingdom
US United States
U.S.C. United States Code

REFERENCES

[1] COM (2009): An area of freedom, security and justice serving the citizen, 262/4, Brussels, pp. 8-9

[2] Funta, R. (2010): 1000+ Questions and Answers about EU and EU Law, 2nd Edition, Tribun EU Publishing, Brno, p. 86

[3] The Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly on 10 December 1948

[4] The International Covenant on Civil and Political Rights (ICCPR) was adopted by the United Nations General Assembly on 16 December 1966

[5] Case: Tournier v. National Provincial and Union Bank of England [1924] 1 K. B. 461

[6] The 1981 Convention on Data Protection was the first instrument where the right to data protection was explicitly provided. Article 8 ECHR provides that *"Everyone has the right to respect for his private and family life, his home and his correspondence*." and that *"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."* But this instrument did not recognize data protection as a separate right.

[7] ECJ Case C-28/08 P (Appeal – Access to the documents of the institutions, Document concerning a meeting held in the context of a procedure for failure to fulfill obligations –Protection of personal data – Regulation (EC) No. 45/2001 Regulation (EC) No 1049/2001), of 29 June 2010, point 61

[8] Federal Data Protection Act of Germany (Bundesdatenschutzgesetz, BDSG)

[9] Case: Whalen v. Roe, 429 U.S. Reports (February 22, 1977), para. 589-604

[10] Svoboda, P. (2010): Úvod do evropského práva, 3. vydání, C-H-Beck Praha, p. 278

[11] First law on data protection was enacted by the German Federal State of Hessen (07.10.1970)

[12] The Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364/3)

[13] 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, Official Journal L 281

[14] Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 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, Official Journal of the European Communities L 8/1

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities L 201

[16] Council Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350,

[17] Fair Credit Reporting Act of 1970, 15 U.S.C. §§1681 et seq

[18] Privacy Act of 1974, 5 U.S.C. § 552a

[19] Computer Security Act of 1987, 40 USC Chapter 25 Section 1441, P.L. 100–235

[20] Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. 552a et seq

[21] In he U.S. Supreme Court's 1976 ruling in United States v. Miller the Court found that bank customers had no legal right to privacy in financial information held by financial institutions (see United States v. Miller, 307 U.S. 174 (1939)

[22] Gramm-Leach Bliley Act of 1999, 15 U.S.C. §§ 6801–6809 (The Act requires the Federal Trade Commission ("FTC"), along with the Federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission, to issue regulations to ensure that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually, and before disclosing any consumer's personal financial information to a non-affiliated third party, must give notice and an opportunity for that consumer to "opt out" from such disclosure. The Act also limits the sharing of account number information for marketing purposes.

[23] The Cybersecurity Enhancement Act of 2010, H.R. 4061

[24] Rotenberg, M. (2010): Data Protection in a Transatlantic Perspective: Future EU-US international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial co-operation in criminal matters, EPIC, Brussels, p. 3

[25] Funta, R. (2010): Common foreign and security policy in terms of the Lisbon Treaty and suppression of international terrorism, International Conference „The Milestones of law in the area of the Central Europe." 18.-20. March, Bratislava

[26] See more in Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 24 October 2001, 2001HR 3162 RDS, 107th CONGRESS, 1st Session, H. R. 3162

[27] MEPs voted by 484 in favour, 109 against and 12 abstentions

[28] Statement by President José Manuel Barroso on the European Parliament's approval of the agreement on the Terrorist Financing Tracking Programme (TFTP), MEMO/10/309

[29] Terrorism constitutes one of the most serious violations of such principles like the principle of democracy and the principle of the rule of law, principles which are common to the Member States. See Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, *OJ* L 164, 22.6.2002.

[30] As it was decided in the case *Kennedy* "the retention of unused data for an unspecified period is acceptable, as long as this retention matches one of the legitimate purposes for which the data was obtained." See Case: Kennedy v. United Kingdom 26839/05 [2010] ECHR 682, paras. 32 and 42

[31] Viviane Reding, Member of the European Commission responsible for Information Society and Media Privacy: The challenges ahead for the European Union Keynote Speech at the Data Protection Day 2010, European Parliament, Brussels, SPEECH/ 10/16

[32] Aaron, D. L. (2001): The EU Data Protection Directive: Implications for the U.S. Privacy Debate. The House Committee on Energy and Commerce, Washington D.C., p. 42

[33] COM (2010): Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A comprehensive strategy on the data protection in the European Union, XXX Final, Brussels, p. 16

[34] See C-54/08 Commission v. Germany; A European Court of Justice (ECJ) decision in the case of the European Commission vs. Germany rules that the Data Protection Authorities (DPAs) needs to be completely independent. The Court ruled that *"the supervisory authorities are the guardians of fundamental rights and freedoms."*