The Second SWIFT Agreement Between the European Union and the United States of America – An Overview

By Valentin Pfisterer [*]

A. Introduction

The United States and other nations have taken numerous military, police and intelligence measures in order to counter terrorists' threats in response to the September 11 attacks on the World Trade Center in New York City and the Pentagon in Virginia as well as the attempted attack on a target in Washington, D. C.

Among these measures, the Terrorist Finance Tracking Program (TFTP) stands out.[1] The US Treasury Department launched this ambitious program aimed at tracking terrorist finance shortly after the September 11 attacks. It included the issuance of administrative subpoenas to access data bases of financial service providers.[2] In 2006, serious tensions between the United States and the EU as well as certain EU Member States arose when it became generally known that US authorities, in the course of the program, had approached SWIFT.[3] The United States and the EU took advantage of the tense situation and began to examine the opportunities for a broader cooperation in this context.[4] For

[*] Research Fellow at the Max Planck Institute for Comparative Public Law and International Law, Heidelberg (Prof. Dr. Armin von Bogdandy), and Doctoral Candidate at the Law Faculty of the University of Leipzig (Prof. Dr. Markus Kotzur, LL.M. (Duke Univ.)). Email: vpfister@mpil.de.

[1] The program is also known as "SWIFT Program." *See* Patrick Connorton, *Tracking Terrorist Finance through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide*, 76 FORDHAM L. REV. 283 (2007); as to the details of the program, see *id.*, 288; furthermore, see U.S. Treasury Department, TFTP Fact Sheet, available at: http://www.ustreas.gov/offices/enforcement/tftp.shtml (last visited Oct. 24, 2010).

[2] *See* Connorton, *supra,* note 1, at 283, 288.

[3] *See id.* at 284, 291.

[4] The first result of this cooperation was a compromise of June 27, 2007. See *id.* at 294. Then, in 2009, the (first) SWIFT Agreement was concluded: Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 8) 11.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

now, the most advanced result of this cooperation is the second so-called SWIFT-Agreement (hereinafter SWIFT-II Agreement).[5]

This contribution will outline the SWIFT saga focusing on the process of the creations of the two SWIFT Agreements and cursorily presenting the contents of both.

Hence, this paper will depict the specific political conditions while introducing the involved institutions and characterizing the difficulties that arose during the process leading to the conclusion of both of the Agreements. Subsequently, the contribution will outline the contents of the first SWIFT Agreement (hereinafter SWIFT-I Agreement) to further highlight the innovations of the SWIFT-II Agreement on this basis. The innovations will, finally, be summarized and briefly evaluated.

B. Political Process and Institutional Framework

I. General Political Background

The general political background of the process is determined by the phenomenon of international terrorism which reached its climax with regard to its public effect, at least preliminarily, by the September 11 attacks in 2001. The anti-terrorism measures taken by many governments in the wake of those events moved the fundamental political, legal and philosophical debate about the tension between liberty and security once more to the center of many contemporary controversies.[6] This situation has gained additional explosiveness for the fact that, during the last few years, an increased awareness of issues such as legal protection against (erroneous) actions of counter-terrorism[7] and data

[5] (Second) Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 195) 5.

[6] From a (German) jurisdictional perspective, the following cases recently decided by the *Bundesverfassungsgericht* (Federal Constitutional Court) are paradigmatic: *Air Security Law Case*, Bundesverfassungsgericht [BVerfG - Federal Constitutional Court], Case No. 1 BvR 357/05, Feb. 15, 2006, 115 BVerfGE 118 (on the constitutionality of a law authorizing the destruction of a hijacked airplane); *Data Retention Case*, BVerfG, Case No. 1 BvR 256/08, 1 BvR 263/08 and 1 BvR 586/08, March 2, 2010, 2010 NJW 833 (on the constitutionality of a law obliging telecommunication service providers to store customer data).

[7] From a (European) jurisdictional perspective, the different *Kadi* cases decided recently by the General Court (formerly Court of First Instance) and the European Court of Justice respectively give a stunning insight into this issue: Case T-315/01, Kadi v. Council and Commission, 2005 E.C.R. II-03649 on the legality of the EU practice of listing in accordance to a UN Security Council Resolution; set aside by Case C-402/05 P and C-415/05 P, Kadi et al. v. Council and Parliament, 2008, E.C.R. I-06351; most recently Case T-85/09, Kadi v. Commission, 2010 (available at: http://eur-lex.europa.eu).

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

protection and data security[8] has emerged not only in professional circles but also in the general public.

II. Relevant Institutions and Political Process Towards the First SWIFT Agreement

Subject matter of the SWIFT-I Agreement was the international financial services cooperative SWIFT. The major institutions involved in the political process leading to the conclusion of the Agreement were, for the United States, the US Department of the Treasury and, for the European Union, the Council and the Commission.

1. SWIFT

The acronym SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. SWIFT is a member-owned Belgium-based international cooperative of financial institutions. Linking more than 9,000 financial institutions, it is in charge of their telecommunications and allows for the automated and standardized execution of financial transactions.[9] For the turn of the year 2009/10, SWIFT planned to transfer a central server concerned with wire transfers in Europe from the United States to the Netherlands. Thus, the cooperative would have eluded the jurisdiction of the United States making it necessary for US authorities to attain access to its data via complex procedures of international legal assistance in the future.[10] This expectation provided for the impetus for the conclusion of the SWIFT-I Agreement between the United States and the European Union in 2009.[11] As SWIFT finally realized the transfer, the United States and the European Union were prepared accordingly (see below).

[8] See the current controversy in Germany about so-called web mapping services such as *Google Street View* and so-called social networks such as *Facebook* and the related privacy concerns; see, furthermore, some prominent recent decisions in the very same area, among these are: *Online Search Case*, BVerfG, Case No. 1 BvR 370/07 and 1 BvR 595/07, 120 BVerfGE 274 in which the Court develops the basic right to the guarantee of confidentiality and the integrity of information technological systems as well as the *Data Retention Case*, *supra,* note 6.

[9] As to detailed background information about SWIFT, see Connorton *supra* note 1, at 283, 287; furthermore, see the official website of SWIFT (www.swift.com); anyway, the SWIFT-Code should be commonly known in the context of, at least international, wire transfers.

[10] *See, e. g.,* Agreement on Mutual Legal Assistance Between the European Union and the United States of America, 2003 O.J. (L 181) 34.

[11] For a brief outline of this part of the SWIFT saga, see the article EU-Parlament kippt SWIFT-Abkommen, Spiegel online, Feb. 11, 2010, available at: http://www.spiegel.de/politik/ausland/0,1518,677232,00.html (last visited Oct. 24, 2010).

2. US Department of the Treasury, the Terrorist Tracking Finance Program and EU-US Controversies

In response to the September 11 attacks in 2001, the US Department of the Treasury, under the then Secretary of the Treasury Paul O'Neill, introduced the Terrorist Finance Tracking Program (TFTP).[12] The program is based on statutory mandates and Executive Orders.[13] Among the latter is the Executive Order 13224 of 23 September 2001 on measures to combat terrorist financing issued by the then US President George W. Bush.[14] The Order directs all United States government agencies, under the guidance of the Treasury, to take all appropriate measures to implement the arrangement established by the Order.[15] The goal of the TFTP is to collect data on financial flows, to analyze them and to cull those financial transactions intended to finance terrorist activities thereby enabling US authorities to identify, to track and to pursue potential terrorists and their supporters.[16] To this end, financial service providers residing or active in the United States can be required to submit relevant data to the Treasury through administrative subpoenas.[17] In cases that lack the mentioned link to the United States, US authorities, however, cannot apply this method without help. They rather have to initiate the much more complicated and protracted process provided for by agreements of international legal assistance.[18] SWIFT, though, was based in Europe and active in the United States at the same time. Hence, the cooperative was subject to the obligations generated by the administrative subpoenas issued by US authorities as well as European laws, especially privacy laws. Therefore, it ended up in an unenviable position in the midst of conflicting obligations.[19] The controversy arising between the United States and the European Union in this respect[20], finally, not only led to a compromise on the concrete subject matter[21] but also led to a broader cooperation between both parties. They entered into negotiations on

[12] For general information about the TFTP, see Connorton, *supra,* note 1, 288 as well as the corresponding TFTP Fact Sheet, *supra,* note 1.

[13] TFTP Fact Sheet, *supra,* note 1.

[14] Exec. Order No. 13224. 66 Fed. Reg. 49079 (Sept. 23, 2001), georgewbush-whitehouse.archives.gov.

[15] *Id.* at Section 7.

[16] TFTP Fact Sheet, *supra,* note 1.

[17] *Id.*; see also Connorton, *supra,* note 1, 283, 288.

[18] *See, e. g.,* Mutual Assistance Agreement, *supra,* note 10.

[19] Connorton, *supra,* note 1, at 284.

[20] For an outline of this part of the SWIFT saga, see *id.* at 290.

[21] *See, supra,* note 4.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

an international agreement[22] when they learned the cooperative's plans that implied the transfer of the central server.[23]

3. EU Institutions and Inter-Institutional Controversies

By means of exchange of information, the EU Member States had benefited a lot from the TFTP's investigation results.[24] Accordingly, the European Union had a specific interest in the continuation of a close cooperation with US authorities, even once SWIFT had moved its data processing activities from the United States to Europe. Hence, it was no surprise that the European Union welcomed negotiations on a special agreement on the issue of data collection, transmission and analysis related to the activities of SWIFT in 2009. To this end, the Council authorized the Presidency on 27 July 2009 to engage in negotiations, assisted by the Commission, on an "Agreement on the processing and messaging of financial data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program" pursuant to Articles 24 (1)[1] and 38 TEU.[25] Negotiations were completed not later than in November 2009, so that the Agreement could be concluded on 30 November 2009, only one day before the coming into effect of the Treaty of Lisbon.[26] The procedure established by the then effective Treaty of Nice only presupposed the approval of the Council for the conclusion of such agreements whereas the consent of the European Parliament was not required. The Parliament, on its part, had always been critical about the Agreement, its concrete arrangements and the procedure of the Agreement's adoption.[27] The Parliament criticized, amongst others, the lack of sensitivity to aspects of data protection and data security; furthermore, the procedure was conceived as dishonorable vis-à-vis the Parliament, first and foremost, because of the approval of the Agreement by the Council only one day before the coming into effect of the Treaty of Lisbon which would have required the consent of the Parliament (see Article 218 (6)[2]a)

[22] SWIFT-I Agreement, *supra,* note 4.

[23] The corresponding authorization of the Department of the Treasury can be found in Executive Order 13224, *supra,* note 14, Section 6.

[24] Explicitly acknowledged by the Preambles of both Agreements; *see id.*, paragraphs 4 and 5 respectively.

[25] Council Decision on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 8) 9, Preamble paragraph 1.

[26] *Id*.

[27] *See, e.g.*, the critical Recommendation of the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, EUR. PARL. DOC. 0178 (2010), available at: http://www.europarl.europa.eu.

TFEU).[28] Nevertheless, on 11 February 2010 the Parliament had the opportunity to vote on the Agreement. In the course of this vote, the Parliament rejected the Agreement by 378 to 196 votes (31 abstentions). The vote could be conceived as evidence of a rising self-confidence of the Parliament under the Treaty of Lisbon. As a result, the SWIFT-I Agreement was suspended.

III. Political Process Towards the SWIFT-II Agreement

After the failure of the SWIFT-I Agreement due to its rejection by the Parliament, its members, on 5 May 2010, agreed on a resolution officially communicating their concerns and preferences to the other EU organs involved.[29] Six days later, the Council authorized the Commission to engage in new negotiations with the competent organs of the United States.[30] In this respect, it shall be noted that under the Lisbon Treaty it is the Commission that is in charge of the negotiation process rather than the Presidency of the Council that was competent under the Treaty of Nice (see Article 218 (2) and (3) TFEU). When negotiations finished in mid-June, a draft Council Decision was provided for as initial legislative document on 22 June 2010.[31] Six days later, the Agreement was signed[32] and, on 8 July 2010, approved by the Parliament[33] following the recommendation[34] of the

[28] A valuable overview of the concerns and the related criticism is provided by the European Parliament Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorize the opening of negotiations for an Agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing, EUR. PARL. DOC. 0129 (2010), available at: http://www.europarl.europa.eu.

[29] *Id*.

[30] *See* Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 195) 3, Preamble paragraph 1.

[31] *See* (Draft) Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, available at: http://register.consilium.europa.eu/pdf/en/10/st11/st11222.en10.pdf.

[32] Council Decision on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 195) 1.

[33] European Parliament legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, EUR. PARL. DOC. 0279 (2010), available at: http://www.europarl.europa.eu.

[34] Recommendation of the Committee on Civil Liberties, Justice and Home Affairs on the draft Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the

Committee on Civil Liberties, Justice and Home Affairs. By means of a Council Decision, the Agreement was approved on 13 July 2010 (see Article 218 (2) and (6)[1] TFEU).[35] On 1 August 2010, it came into effect pursuant to the first paragraph of its Article 23.

C. The SWIFT-I Agreement

The SWIFT-II Agreement can be traced back to the preceding Agreement of November 2009 (see above). It is, therefore, particularly instructive to analyze the contents of the SWIFT-II Agreement by way of comparison with the contents of the SWIFT-I Agreement. Accordingly, the contents of the SWIFT-I Agreement will be presented shortly.

I. Legal Basis

The SWIFT-I Agreement was an international agreement between the European Union and the United States regulating US authorities' access to SWIFT financial transaction data. The material competence of the European Union resulted from the provisions on police cooperation and Europol, in particular on measures such as the "collection, storage, processing, analysis and exchange of relevant information" (Article 30 (1)b) TEU). With respect to the procedure of concluding the Agreement, the provisions of Articles 24 (1) and 38 TEU provided the necessary rules.[36] Accordingly, the Council could conclude agreements with one or more States or international organizations in the area of implementation of the Title on Police and Judicial Cooperation (title six TEU).

II. Objective

The objective of the Agreement was discussed in the first Article of the Agreement. According to this provision, the Agreement should ensure that "(a) financial payment messaging and related data stored in the territory of the European Union by providers of international financial payment messaging services (…) are made available upon request by the U.S. Treasury Department for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; and (b) relevant information obtained through the TFTP is made available to law enforcement, public security, or counter terrorism authorities of Member States, or Europol or Eurojust, for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing." The corresponding data "may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national

purposes of the Terrorist Finance Tracking Program, EUR. PARL. DOC., 0224 (2010), available at: http://www.europarl.europa.eu.

[35] *See* Council Decision, *supra,* note 30.

[36] *See* Council Decision, *supra,* note 25, Preamble.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

identification number, and other personal data related to financial messages" (Article 4 (2) SWIFT-I).

III. Outline of the Contents

The Agreement consisted of a preamble and 15 articles. A separate declaration was attached according to which the Member States obliged themselves to apply the Agreement temporarily as from 1 February 2010 until its definitive coming into effect (also see Article 15 (2) SWIFT-I).[37]

1. Preamble

The preamble made reference to the TFTP and the joint efforts of the two parties in the struggle against terrorism and alluded to the UN Security Council Resolution 1373 (2001) on the financing of terrorism.[38] It explicitly recognized the importance of the relevant fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, the European Convention on the Protection of Human Rights and Fundamental Freedoms as well as other applicable human rights provisions and necessary procedures of legal protection.[39]

2. Operative Part

In its operative part, the Agreement established a complex system of mutual messaging between EU Member States and the United States (Articles 4, 7 and 8 SWIFT-I). The system was built on the already existing mechanisms of the Agreement on Mutual Legal Assistance between the European Union and the United States of America of 25 June 2003[40] and the related bilateral mutual legal assistance instruments between the EU Member States and the United States (see Article 4 (1) SWIFT-I). Notwithstanding certain simplifications, the procedure envisaged in the SWIFT-I Agreement worked as follows:

Pursuant to Article 4 (1) SWIFT-I, the process was to be initiated by means of an official request issued by the Treasury according to Article 8 of the Mutual Legal Assistance Agreement. The request had to be directed to a central authority in the EU Member State in which the financial service provider concerned (so-called "Designated Providers") was either based or where it stored the requested data. The central authority, then, was to verify the accordance of the request with both the SWIFT-I Agreement and the

[37] Furthermore, see *id.*, Article 3.

[38] SWIFT-I Agreement, *supra,* note 4, Preamble, paras. 3, 4, 5.

[39] *Id.* at para. 6.

[40] *See* Mutual Assistance Agreement*, supra,* note 10.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

requirements of the applicable bilateral mutual legal assistance instrument. Once the accordance was confirmed, the request was to be transmitted to the competent authority of the same Member State for execution. As soon as provided for by the Designated Providers, the competent authority was to transfer the relevant data to the United States (Article 4 (3), (5) and (7) SWIFT-I).

The Agreement contained multiple guarantees and safeguard mechanisms to ensure the interests and the legal status of the citizens. Among those, the following formal and material requirements and restrictions stand out:

First, the elements of those actions labeled terrorism financing by the Agreement, the permissible purposes of data collection and processing as well as the type of data concerned were precisely defined (Article 2, Articles 1 (1) and 5 (2)a) as well as Article 4 (2) SWIFT-I). Second, a request was to be based upon "pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing" (Article 5 (2)b) SWIFT-I), it was to be substantiated correspondingly and, in any case, to be "tailored as narrowly as possible" (Article 4 (2) and Article 5 (2)c) SWIFT-I). Third, each search was to be logged (Article 5 (2)c) SWIFT-I). Fourth, there were several explicit prohibitions such as the ban on data mining, copying and editing of the data (Article 5 (2) and (2)f) and g) SWIFT-I). Furthermore, the data had to be maintained in a secure physical environment and protected from unauthorized access; it was, in fact, to be made available to a narrowly defined group of experts only (Article 5 (2)d) and e) SWIFT-I). Finally, the Agreement established precise requirements concerning the deletion and its logging (Article 5 (2)i) to l) SWIFT-I).

The compliance with the above mentioned guarantees and safeguard mechanisms were subject to a joint review which was to be carried out no later than after a period of six months. In this context, "a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing" was to be realized (Article 10 (1)[1] and [2] SWIFT-I).

Finally, concerned citizens were given right to "obtain (…) confirmation from his or her data protection authority whether all necessary verifications have taken place within the European Union to ensure that his or her data protection rights have been respected in compliance with this Agreement, and, in particular, whether any processing of his or her personal data has taken place in breach of this Agreement. Such right may be subject to necessary and proportionate measures applicable under national law, including for the protection of public security or national security or to avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences, with due regard for the legitimate interest of the person concerned" (Article 11 (1) SWIFT-I). Moreover, a citizen was "entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively" in

case he or she considered "his or her personal data to have been processed in breach of this Agreement" (Article 11 (3) SWIFT-I).

3. Criticism

The criticism of the Agreement covered several aspects. Among other things, it was alleged that the requested data might lack any reference to the United States and a messaging, therefore, would not be justified. Furthermore, it was pointed to the large amount of data that could possibly be requested and consequently transferred. Lastly, there were complaints about the data being withdrawn from any EU influence and its high standards of data protection once transferred to the United States.[41]

D. The SWIFT-II Agreement

The SWIFT-II Agreement has been binding the institutions of the EU and its Member States since 1 August 2010 as obligatory law (Article 216 (2) TFEU). It can be traced back to the SWIFT-I Agreement and substitutes it. At the same time, it contains numerous changes in detail intended to accommodate SWIFT-I's criticisms.

I. Legal Basis

Just like the SWIFT-I Agreement, the SWIFT-II Agreement is an international agreement between the European Union and the United States. The material competence of the Union can be found in the provisions of Articles 87 and 88 TFEU on measures concerning the collection, storage, processing, analysis and exchange of information by Member State police authorities (Article 87 (2)a) TFEU) and on Europol (Article 88 (2) TFEU). The rules on the procedure follow from the provision of Article 218 TFEU in conjunction with the substantive provisions in the area of police cooperation.[42] In the very case, the Counsel had to adopt its decision on the conclusion of the Agreement on a proposal by the negotiator and after obtaining the consent of the Parliament (Article 218 (5) and (6)[2]a) TFEU).

II. Objective

The objective of the Agreement, determined in its first Article, is virtually identical to the first Agreement's objective as only minor conceptual changes can be found.

[41] For a valuable overview on the relevant concerns and criticism, see Recommendation of the Committee on Civil Liberties, Justice and Home Affairs, *supra,* note 27; furthermore, see European Parliament Resolution, *supra,* note 28.

[42] *See* Council Decision, *supra,* note 30, Preamble.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

III. Outline of the Contents

The SWIFT-II Agreement consists of a preamble and 23 articles. Pursuant to paragraphs five and six of the preamble of the Council Decision and due to Protocols 21 and 22 to the TEU and the TFEU as introduced by the Treaty of Lisbon, the Agreement does, at least for the time being, not apply to Ireland and Denmark.[43] The SWIFT-II Agreement no longer provides for provisional application as was the case in the SWIFT-I Agreement (see Article 15 (2) SWIFT-I); rather it was to come into effect on the first day of the month after the date on which the Parties have exchanged the necessary notifications (Article 23 (1) SWIFT-II).

1. Preamble

The preamble of the SWIFT-II Agreement is longer and more elaborate than that of the SWIFT-I Agreement. The importance and the achievements of the TFTP are being recognized more extensively as well as the important role of data protection and security and the corresponding procedures and safeguard mechanisms.[44] Furthermore, it is noteworthy that paragraph six of the Preamble makes elaborate reference to data protection related to human rights provisions such as "the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 (2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms, the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union".[45] The referral to Article 6 (2) TEU made in the same paragraph, however, appears to be a wrong citation. The cited provision, as amended by the Treaty of Lisbon, authorizes the European Union to accede to the European Convention on the Protection of Human Rights and Fundamental Freedoms whereas the first and the third paragraph of the very provision address substantive questions of human rights.

[43] *Id.* at paras. 6 and 7.

[44] SWIFT-II Agreement, *supra,* note 5, Preamble, para. 3.

[45] *Id.* at para. 6.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

2. Operative Part

In its operative part, the Agreement establishes – just as its predecessor did – a system of mutual messaging between EU Member States and the United States (Article 4, 9 and 10 SWIFT-II).
An examination in detail, however, quarries many differences between the SWIFT-I and SWIFT-II Agreement including the procedural structure and the legal technique, the guarantees and safeguard mechanisms, the rules on the onward transfer of data as well as, finally, the issues of transparency and legal protection.

First, the procedural structure (request and corresponding data transfer) has been completely altered. In this context, an absolutely different legal technique has been applied concerning the obligation of the Designated Provider to provide the relevant data. Notwithstanding certain simplifications, the procedure envisaged in the SWIFT-II Agreement works as follows:

Just like in the SWIFT-I Agreement, the process is to be initiated by means of an official request issued by the US Department of the Treasury (Article 4 (1) SWIFT-II). Unlike the SWIFT-I Agreement, however, the request is to be served directly upon the Designated Provider. Only a copy is to be provided to Europol, none to any EU Member State authority. Europol, then, verifies the accordance of the request with certain requirements established in the Agreement and, in case of a successful verification, notifies the Designated Provider. As a consequence, the Designated Provider is "authorized and required to provide the data to the U.S. Treasury Department" (Article 4 (1), (3), (4) and (5) SWIFT-II).

There are several issues that are striking about the newly established procedural structure: First, the linkage between the Agreement at hand and the Agreement on Mutual Legal Assistance of 2003[46] is abandoned (see Article 4 (1) SWIFT-I); instead, a separate structure is implemented. Second, the U.S. Department of the Treasury is granted the competence to approach the Designated Providers directly and, thus, without having to make a detour to EU or Member State authorities (see Article 4 (1) SWIFT-II compared to 4 (1) SWIFT-I); in this way, the national authorities have almost lost their role in the messaging process in favor of Europol. Third, the legal obligation of the Designated Provider contains an interesting particularity. Stating that the request "shall have binding legal effect as provided under U.S. law, within the European Union as well as the United States", the provision of Article 4 (5) SWIFT-II grants US law full applicability within the territory of the European Union. This novelty is accompanied by a corresponding provision concerning the legal protection against the request: according to the provision of Article 4 (8) SWIFT-II, the Designated Provider "shall have all administrative and judicial redress available under U.S. law to recipients of Treasury Department Requests."

[46] *See, supra,* note 10.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

Second, the guarantees and safeguard mechanisms of the SWIFT-II Agreement go far beyond what was laid down in the SWIFT-I Agreement.

In this respect, virtually all guarantees and safeguard mechanisms of the SWIFT-I Agreement are contained in the SWIFT-II Agreement – mostly extended and strengthened; among those provisions are the precise definition of the elements of those actions labeled as terrorism financing by the Agreement, the type of data concerned and the permissible purposes of data collection and processing, the requirement of a "cause for suspicion" and a corresponding substantiation of the request, logging requirements, explicit prohibitions such as the ban on data mining, copying or editing of the data, physical security requirements, the protection from unauthorized access as well as, finally, deletion requirements and deadlines (see above). In addition, the SWIFT-II Agreement has introduced the requirement of a precise request also with regard to the data category (Article 4 (2)a) SWIFT-II). Furthermore, data relating to the Single European Payment Area has been excluded from the scope of the data to be requested by or produced to the Treasury, and the interconnection of relevant data with other databases has been explicitly prohibited (Article 4 (2)d) and Article 5 (4)b) SWIFT-II). Moreover, the deletion requirements and deadlines have been rendered more stringent (Article 6 SWIFT-II). Finally, the requirements of necessity and proportionality of data collection and processing have been highlighted more articulately and the principle of non-discrimination with respect to nationality and country of residence as well as other distinctive features has been introduced as an additional safeguard mechanism (Article 5 (1), (5), (6) and (7) SWIFT-II).

Third, the monitoring of the above mentioned guarantees and safeguard mechanisms and the joint review play a more significant role in the Agreement.

Thus, the Agreement establishes, first, a permanent oversight mechanism whose subject is the "strict counter terrorism purpose limitation and the other safeguards set out in Articles 5 and 6" (Article 12 (1)[1] SWIFT-II). In this context, independent overseers, including a person appointed by the European Commission, are being assigned to verify the compliance of the above mentioned guarantees and safeguard mechanisms. According to the provision of Article 12 (2) SWIFT-II, this oversight mechanism including its independency is itself subject of regular monitoring as envisaged by the provision of Article 13 SWIFT-II. This provision establishes a joint review mechanism for the entirety of the safeguards, controls, and reciprocity provisions envisaged in the Agreement.

Fourth, the onward transfer of data by the Treasury is subject of a separate article in the SWIFT-II Agreement (Article 7 SWIFT-II, see Article 5 (2)h) SWIFT-I) and, thus, set out in more detail.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

The safeguard clause contained in the SWIFT-I Agreement ("Only terrorist leads obtained through the TFTP under this Agreement shall be shared with (…) third States to be used for the purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing", Article 5 (2)h) SWIFT-I) has basically been transposed, complemented by additional guarantees and restructured (Article 7 a) to f) SWIFT-II). Among these changes are the categorical requirement of the prior consent of the relevant Member State in cases involving EU citizens or residents (Article 7 d) SWIFT-II), the obligation of the United States to request that the information be deleted by the third State when no longer required (Article 7 e) SWIFT-II), as well as a logging requirement (Article 7 f) SWIFT-II).

Fifth, the SWIFT-II Agreement places particular emphasis on the issues of transparency and legal protection (Articles 14 to 18 SWIFT-II). These issues obviously constitute a major priority of the Agreement.

With regard to the issue of transparency, the provision of Article 14 requires that the Treasury provides detailed information about the TFTP and its purposes as well as the procedures available for the exercise of the rights set out in the Agreement on its public website.

These above mentioned rights and procedures are contained in the Articles 15 to 18 SWIFT-II that arrange for a legal protection mechanism completely different to that of the SWIFT-I Agreement. Thus, the right to information (Article 15 (1) SWIFT-II, see Article 11 (1) SWIFT-I) has been complemented by a corresponding administrative procedure in due form (Article 15 (3) SWIFT-II). Another novelty is the right to rectification, erasure, or blocking in Article 16 (1) SWIFT-II. It is, just like the right to information, supplemented by a corresponding administrative procedure in due form (Article 16 (2) SWIFT-II). These subjective rights are to be conceived together with or in the light of the provision of Article 17 SWIFT-II (see Article 11 (2) SWIFT-I). This provision establishes an objective obligation of the parties to take all appropriate measures including supplementation, deletion, or correction of inaccurate or unreliable data in case one of them becomes aware of such a deficiency. The second paragraph of the provision ensures that corresponding indications are being shared between the parties. In addition, the provision of Article 18 (2) SWIFT-II entitles "any person who considers his or her personal data to have been processed in breach of this Agreement (…) to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively."

Finally, the Agreement offers some minor changes in addition to the major changes mentioned above. Among these are the introduction of an additional element of an action labeled as terrorism financing by the Agreement expanding, thus, the scope of application of the Agreement (Article 2 c) SWIFT-II). Moreover, unlike the SWIFT-I Agreement, the SWIFT-II Agreement contains an Annex which concretely identifies the Designated Providers being subject to the arrangements of the Agreement; this Annex currently

includes no other entity than SWIFT. The Annex, however, may be updated by the exchange of diplomatic notes. The update, thereafter, has to be duly published in the Official Journal of the European Union.

E. Brief Evaluation

I. General Remarks

Without any doubt, the SWIFT-II Agreement constitutes a substantial development compared to the SWIFT-I Agreement. The demands of the Parliament and other actors have obviously been given serious consideration and have, at least partly, found their way into the text of the Agreement.

In general, the SWIFT-II Agreement is characterized by a more cooperative style which conceives of messaging rather as a cooperation of coequal nature than as a service of the European Union and its Member States to the United States. Furthermore, it enhances coherence, clarity, and comprehensibility by means of its clear and stringent language and structure.

With regard to the contents, the SWIFT-II Agreement contains major developments in comparison to the SWIFT-I Agreement: The Treasury is granted direct access to the Designated Providers, thus, increasing the pace of the messaging procedure as well as its efficiency – both, of course, in favor of Europol and at the expense of the EU Member State authorities. The protection of the interests and the legal status of the citizens go far beyond what was set out in the SWIFT-I Agreement. Not only have the existing guarantees and safeguard mechanisms, the rules on the joint review as well as the rules on the onward transfer of data been amplified, advanced and restructured; they have also been complemented by detailed rules on transparency, legal protection and redress. Legal protection and redress, especially, have been strongly enhanced.

Some issues, however, remain unclear, problematic or dissatisfactory, at least from a European citizen's point of view.

Among these, the bold legal technique applied with regard to the legal effects of the request stands out. The fact that US law is to govern the legal effects of the request in the United States as well as in the European Union (Article 4 (5) SWIFT-II) might provoke serious questions and uncertainties concerning the relation between EU and EU Member State law on the one hand and US law on the other hand. These concerns might be aggravated by the fact that the corresponding administrative and legal redress is also dependent on US law (Article 4 (8) SWIFT-II). At least from a European perspective, this dominance of US law might be dissatisfactory as well as the mere fact that, under the newly established regime, EU citizens might (still) have to appeal to US courts in most cases.

Further questions and uncertainties could arise in view of the equal-treatment clause in Article 18 (2) SWIFT-II. It cannot be assured that this provision will stand up to the US Privacy Act which determines that US citizenship or permanent residence in the United States is a prerequisite for a request for information.

Finally, it is not clear whether the significantly expanded citizen's rights in the second Agreement will really be made available to the citizens at the end of the day. The provision of Article 20 (1) SWIFT-II (also see Article 13 SWIFT-I), stating that the Agreement "shall not create or confer any right or benefit on any person or entity, private or public", at least provokes doubts in this regard.

II. Focusing Data Protection

At this point, it cannot be determined whether the Agreement meets the substantive requirements of the basic rights enshrined in the Charter of the Fundamental Rights of the European Union (Article 6 (1) TEU) and those constituting general principles of EU law according to Article 6 (3) TEU.

Possible violations of Articles 7 and 8 CFREU in conjunction with Article 6 (1) TEU as well as of Article 8 ECHR in conjunction with Article 6 TEU (3) TEU as well as other possible violations will, at any rate, be subject of further discussion. As often, as the decisive question might turn out the question whether the provisions laid down in the Agreement meet the requirements of the proportionality test applied in human rights matters.[47] And once more, the European Court of Justice might have the ultimate say here.[48]

From a German point of view, the question arises if the provisions laid down in the Agreement meet the requirements of the German Basic Law. Once again, a detailed analysis cannot be provided at this point. At any rate, it will be necessary to approach this question with due regard to the decision of the Federal Constitutional Court on data retention of 2 March 2010.[49] Herein, the Court holds that "the principle of proportionality requires that the legal arrangement of such data storage has to duly accommodate the specific intensity of the interference associated with the storage. There shall be sufficiently sophisticated and clear regulations regarding data protection, use of the data,

[47] See the Opinion of Advocate General Léger in the *Passenger Name Record Case*, C-317/04, European Parliament v. Council and Commission, 2006, E.C.R. I-04721. Herein, Léger advocates for a reduction of the intensity of the judicial review with regard to the proportionality test in the context of security matters.

[48] The reaction of the European Court of Justice to Léger's proposal can be seen, among others, in Case C-402/05 P and C-415/05 P, *supra,* note 7, where the Court basically rejects this conception.

[49] *Data Retention Case*, *supra,* note 6.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

transparency and legal protection."[50] Given the strict and detailed requirements the Court sets out in its decision and assuming their transferability, there is serious reason to fear—or hope?—that the SWIFT-II Agreement does not meet these requirements.

[50] *Id.* at 833.

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press

https://doi.org/10.1017/S2071832200020174 Published online by Cambridge University Press