the SPANISH YEARBOOK of INTERNATIONAL LAW

The Standards for Protection of Financial Information Gathered Within EU-US Cooperation in Criminal Matters. An Outline of the Existing Legal Framework and New Initiatives in Personal Data Protection

Martyna KUSAK*

Abstract: The article aims to outline an existing legal framework for the gathering of financial information within ES-US cooperation in criminal matters in light of personal data protection. The study deals both with current instruments and new initiatives in personal data protection and EU and EU-US cooperation.

Keywords: transnational cooperation in criminal matters – data protection – gathering of financial information – SWIFT – Umbrella Agreement

INTRODUCTION

It is commonly acknowledged that financial information is highly sensitive and thus requires strict data protection rules. However, the fight against crime has increased the motivation for states to gather and use citizens' financial information for the purposes of criminal proceedings, including those carried out in trans-border and transatlantic contexts. The standards for protection of information gathered and processed within EU-US activities is of great interest, particularly in light of the recent European Court of Justice judgment in case C-362/14[1], as well as of the finalisation of the negotiations on the Umbrella Agreement[2].

Accordingly, this paper aims to provide a brief overview of the existing legal framework for the gathering of financial information within ES-US cooperation in criminal matters in the light of personal data protection. Firstly, the EU approach to gathering and protecting financial information will be outlined. Secondly, instruments governing the gathering of financial information within EU-US cooperation will be briefly presented. This part of the study will also examine whether the European standard of data protection still applies when it comes to transatlantic cooperation. The concluding remarks will sketch new initiatives to ensure an adequate level of protection of European citizens' financial information in the context of EU-US cooperation in criminal matters.

* PhD Researcher, Adam Mickiewicz University in Poznań, e-mail: m.kusak@amu.edu.pl

[1] The case relates to transferring personal data of the EU citizen gathered by Facebook to the United States.

[2] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offence, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf, access: 1 December 2015.

 DOI: 10.17103/sybil.19.15

GATHERING OF FINANCIAL INFORMATION AND PERSONAL DATA PROTECTION IN THE EU

(1) The 2001 EU MLA Protocol

(a) *Gathering of financial information*

Until now, the main instrument for allowing member states to collect financial information in the EU is the 2001 EU MLA Protocol[3] (hereafter: Protocol). According to its provisions, authorities are entitled to:

- issue a request for information on bank accounts (art. 1 of the Protocol).
- issue a request for information on banking transactions (art. 2 of the Protocol); and
- issue a request for the monitoring of banking transactions (art. 3 of the Protocol).

Art. 1 of the Protocol allows member states to trace bank accounts throughout the territory of the requested member state. However, in order to do so, member states must comply with certain requirements. Firstly, a person (natural or legal) whose banking information is to be gathered has to be the subject of a criminal investigation. Secondly, this article applies only if the investigation at issue concerns certain offences[4]. Moreover, the issuing authority shall justify why it considers that the requested information is likely to be of substantial value for the purpose of the investigation[5]. The requested member state, however, is not obliged to execute a request and may make it dependent on the same conditions as they apply in respect of requests for search and seizure, what allows the member states to require dual criminality[6].

Two following articles of the Protocol apply where the requesting state has already identified the bank account and seeks information on transactions.

A request for information on banking transactions (art. 2 of the Protocol), unlike the previous measure, does neither make any references to bank accounts linked to a person that is the subject of criminal investigation, nor to the proceedings concerning certain offences[7]. Consequently, member states are obliged to assist also in respect of accounts held by third persons[8], however, the requesting authority is bounded by paragraph 3 which obliges the requesting member state to indicate in its

---

[3] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326, 21.11.2001, at. 2–8.

[4] According to art. 1.3 of the Protocol those offences are as follows: *an offence punishable by a penalty involving deprivation of liberty or a detention order of a maximum period of at least four years in the requesting State and at least two years in the requested State, or an offence referred to in Article 2 of the 1995 Convention on the Establishment of a European Police Office (Europol Convention), or in the Annex to that Convention, as amended, or to the extent that it may not be covered by the Europol Convention, an offence referred to in the 1995 Convention on the Protection of the European Communities' Financial Interests, the 1996 Protocol thereto, or the 1997 Second Protocol thereto.*

[5] Art. 1.4 of the Protocol.

[6] Art. 1.5 of the Protocol, see also: Explanatory report to the Protocol to the 2000 Convention on mutual assistance in criminal matters between the Member States of the European Union, OJ C 257/1, 24.10.2002 (hereafter: Explanatory report), at. 4.

[7] Consequently, this article applies in respect of the same proceedings as those referred to in art. 1 of the 1959 European Mutual Assistance Convention and art. 3 of the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, see more elaborately Explanatory report, at. 5.

[8] See also: Explanatory report, at. 5.

request why it considers the requested bank information relevant for the purpose of the investigation. It is noteworthy that, as in the previous article, the execution of a request may be dependent on the same conditions as they apply in respect of requests for search and seizure[9]. Art. 3 of the Protocol obliges member states to ensure that, at the request of another member state, it is able to monitor the banking operations. The only one requirement here is to indicate why the requesting member state considers the requested information relevant for the purpose of the investigation[10].

(b) *Data protection*

Restrictions on the use of data gathered using the Protocol are ensured in art. 23 of the 2000 EU MLA Convention (hereafter: Convention)[11] which clarifies the conditions in which the personal data may be used. It is noteworthy that the Convention is the first instrument on judicial cooperation in criminal matters, which has incorporated rules on protecting personal data exchanged between member states[12]. In general, the member state to which such data have been sent may use them *without* the prior consent of the member state which forwarded only in three cases:

- for the purposes of proceedings to which the Convention applies, or
- for other judicial and administrative proceedings directly related to proceedings referred to under the previous point, or
- for preventing an immediate and serious threat to public security.

For any other purpose the consent of the data subject or the consent of the communicating member state is required[13].

(2) The EIO Directive

(a) *Gathering of financial information*

Briefly speaking, the EIO Directive[14] is an instrument based on mutual recognition, designed to replace the existing framework of mutual legal assistance in the EU and to cover the whole area of gathering of evidence. With regard to financial information, the EIO Directive is broadly based on the 2001 EU MLA Protocol[15] and, consequently, allows:

- gathering of information on bank and other financial accounts (art. 26);
- gathering of information on banking and other financial operations (art. 27);
- the monitoring of banking or other financial operations (art. 28).

As in the case of the Protocol, the EIO Directive places restrictions on the gathering of bank

9 Art. 2.3 of the Protocol.

10 Art. 3.3 of the Protocol.

11 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C 197, 12.7.2000.

12 See: Explanatory Report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 379/7, at. 26.

13 See more elaborately: E. De Busser, *Data Protection in EU and US Criminal Cooperation*, (Maklu 2009), at. 148 *et seq.*

14 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36; transposition deadline passes on 22 May 2017.

15 Proposal for a Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters- Explanatory Memorandum, 2010/0817 (COD), at. 23.

information, which concern, *inter alia*, *ratione personae* and *ratione materiae* issues[16].

(b) *Data protection*

Pursuant to art. 20 of the EIO Directive, all personal data (including financial information) gathered using the EIO are protected and may only be processed in accordance with the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereafter: the PPDP FD)[17]. The PPDP FD provides, *inter alia*, restrictions on the use and processing of personal data; rules concerning rectification, erasure and blocking; time limits for erasure and review, as well as right to access and right to compensation for the damage applicable to any person who has suffered damage as a result of an unlawful processing operation.

(c) *New approach to data protection in the EU*

It is noteworthy that, at the EU level, personal data protection is guaranteed by the Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights of the EU. Accordingly, art. 16 (1) of the TFEU establishes the principle that everyone has the right to the protection of personal data. Art. 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right.

Due to the specific nature of the criminal proceedings, it was acknowledged that the present 'state of play', governed by the PPDP FD and art. 23 of the Convention, is not satisfactory and specific, common rules on the protection of personal data in the EU may prove necessary[18]. This conclusion follows from the fact that both acts have a limited scope of use and apply only to cross-border data processing, not to gathering and processing activities at purely national level. Hence, the Commission is considering extending the application of these rules to data exchanged at national level[19].

---

[16] See: art. 26.1 of the EIO Directive and art. 11.1 (g) of the EIO Directive.

[17] Council Framework 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, OJ L 350, 30.12.2008. It is noteworthy, that this provision was incorporated after the intervention of the European Data Protection Supervisor, see: Opinion of the European Data Protection Supervisor on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order and on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters, avalable on: https://secure.edps.europa.eu.

[18] Due to the fact that data gathered and used nationally, upon a national initiative, are not protected neither by art. 23 of the Convention nor by the PPDP FD.

[19] See: Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.1.2012, COM (2012)10 final.

GATHERING OF FINANCIAL INFORMATION AND PERSONAL DATA PROTECTION IN EU-US COOPERATION

(1) 2003 EU-USA MLA Agreement

(a) *Gathering of financial information*

The US's right to request the financial information of EU citizens is possible upon art. 4 of the EU-USA MLA Agreement (hereafter: Agreement)[20]. This provision is inspired by art. 2 of the Protocol, so the requirements for obtaining the requested information will in many cases be identical to those for requests within the European Union[21]. However, the Agreement only allows access to financial data where a person *suspected of* or *charged with a criminal offence* is the holder of a bank account. Moreover, the request has to comply with certain requirements, as identification of the natural or legal person relevant to locating such accounts or transactions and justify the natural or legal person concerned is engaged in a criminal offence and that the information sought relates to the criminal investigation or proceedings[22].

(b) *Data protection*

The general limitations on the use and protection of personal data, which also apply to financial information, are laid down in art. 9 of the Agreement, which is inspired by art. 23 of the Convention[23]. According to its provisions, gathered data may be used solely:

- for the purpose of criminal investigation and proceedings,
- for preventing an immediate and serious threat to public security;
- for purposes laid down in art. 9.1(c)- (d) of the Agreement.

If used for any other purpose, the prior consent of the requested state is required.

(2) SWIFT Agreement

(a) *Gathering of financial information*

The so-called 'Transatlantic SWIFT Saga'[24] started after the 9/11 attacks, when the US Treasury Department introduced a secret programme allowing it access to European citizens' financial data through administrative subpoenas. After the disclosure of that fact and the serious tensions which consequently arose between the EU and the US[25], negotiations on the scope of US access to European banking information were started and, as a matter of fact, remain ongoing until now.

---

[20] Agreement June 25, 2003 on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003.

[21] Council of the European Union, Handbook on the practical application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements, 25.3.2011, 8024/11, at. 21-22, hereafter: Handbook.

[22] See art. 4. 2 of the Agreement.

[23] Handbook, at. 31-32.

[24] J. Monar, *The Rejection of the US-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications*, European Foreign Affairs Review 15 (2010), at. 143.

[25] See more elaborately: P. M. Connorton, *Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide*, 76 Fordham Law Review 283 (2007).

After a rejection of the first agreement (which was unsatisfactory to the EU in the field of data protection)[26], a second draft, the so-called the Second SWIFT Agreement[27] (hereafter: SWIFT), was adopted which, until now, constitutes the basis for the exchange of financial information between the EU and the US in cases concerning terrorism[28]. Briefly speaking, this document gives the US wide powers to collect European information, including the obtaining and use of financial payment messaging and related data with a view to the prevention, investigation, detection, or prosecution of conduct pertaining to terrorism or terrorist financing[29]. In other words, the collected data may be used by US authorities to prevent terrorist actions. What is striking is that this information may be collected regardless of whether criminal proceedings have been carried out or whether a person whose financial data is to be collected is a subject of criminal proceedings. In this light, one may assume that the US's powers to collect financial data in the EU go beyond the framework established not only in the Agreement, but also within the EU's internal framework.

(b) *Data protection*

It is hoped that the wide margins of SWIFT's application are balanced by restrictions on the use of the gathered data concerning, *inter alia*:

- rules for processing of the data (art. 5);
- requirements for the principle of necessity and proportionality (art. 5.5);
- the involvement of Europol (art. 2. 4-5);
- the role of a person appointed by the European Commission (art. 12).

However, it has to be stressed that despite of all efforts and good intentions, standard for data protection ensured in SWIFT is not satisfactory. Firstly, it has to be stressed that the conditions for gathering and use of bank information do not meet the guarantees demanded by EU law, like data retention limitation or purpose limitation. Moreover, the right to legal remedies in case of unlawful processing of financial information is not guaranteed at the same level as under the EU law, cause EU citizens – non-resident in the US- are unable to obtain redress in US courts[30].

DISCUSSION: THE EU-US DATA PROTECTION "UMBRELLA AGREEMENT"

With regard to the overview presented above, one may notice that all efforts to ensure data protection

[26] See more elaborately: V. Pfisterer, *The Second SWIFT Agreement Between the European Union and the United States of America – An Overview*, German Law Journal, Vol. 11, No.10.

[27] 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, OJ L 195/5, 27.7.2010.

[28] See also: J. Santos Vara, *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, CLEER WORKING PAPERS 2013/2, p. 17-20.

[29] See art. 2 of the SWIFT.

[30] In this respect see Article 29 Data Protection Working Party & Working Party on Police and Justice, Press Release on EU-US TFTP agreement; Staff Working Document Joint Review Report of the implementation 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, COM (2014) 513 final.

within the EU, and within EU-US cooperation in criminal matters, fail miserably when it comes to SWIFT[31]. SWIFT, unlike all previously mentioned instruments, allows data collection even in cases where a criminal investigation has not yet been carried out. Moreover, there are neither strict *ratione personae*, nor *ratione materiae* requirements for data gathering. Finally, the practice shows that the various SWIFT safeguards, intended to ensure data protection, are unsatisfactory.

Hence, since March 2011, the EU has been negotiating a new approach to personal data protection with the USA, which also covers financial information gathered through SWIFT[32]. The main EU goal was a revision of the current data protection legal framework and a clarification of the procedure. In contrast, on the US side, the main objective was to maintain the smooth delivery of personal data from the EU[33]. These sharply different wishes were seriously hampering the negotiations and, as a consequence, the US approach still dominates in terms of the exchange of European citizens' financial information[34]. The negotiations were finalized on September 2015. It is believed that the Umbrella agreement will provide high-level data protection framework for EU-US law enforcement cooperation, ensuring *inter alia*:

- clear limitations on data use,
- onward transfer,
- retention periods,
- right to access and rectification,
- judicial redress and enforceability of rights[35].

Although the Umbrella Agreement may been considered as is a turning point in current standards for protection of financial information gathered within EU-US cooperation in criminal matters, the act has been already criticised due to the fact that in some aspects it is likely to lead to violations of the TFEU and the EU Charter of Fundamental Rights[36].

It is argued, *inter alia*, that the Umbrella Agreement in many respects fails to meet important substantive requirements of EU data protection law and fails to meet important requirements of EU data protection law in terms of data subject rights and data subjects' access to real and effective remedies. Moreover, it is said that in terms of transparency and oversight, the Umbrella Agreement falls significantly short of fundamental European data protection and human rights requirements. A big objection is also the fact that the Agreement does not provide for equal rights and remedies for EU - and US nationals in the USA. Furthermore, non-EU citizens living in EU Member States are

[31] See also: M. Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement*, Institute for European Integration Research Working Paper 2011/4, p. 27-28.

[32] So-called 'Data Protection Umbrella Agreement', see more elaborately: Factsheet EU-US negotiations on data protection: http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf

[33] E. De Busser, *The Adequacy of an EU-US Partnership*, in S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet (eds.) *European Data Protection: In Good Health?* (Springer Dordrecht Heidelberg London New York 2012, in particular at.185-187.

[34] See more elaborately: A. Ripolli Servent, A. MacKenzie, *The European Parliament as a 'Norm Taker'? EU-US Relations after the SWIFT Agreement*, European Foreign Affairs Review 17, Special Issue (2012).

[35] See more elaborately: European Commission Fact Sheet, Questions and Answers on the EU-US data protection "Umbrella agreement", 8 September 2015.

[36] D. Korff, *EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff*, http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/, access: 1 December 2015.

completely denied judicial redress in the USA under the Umbrella Agreement[37].

It also has to be highlighted that the Umbrella Agreement does not make any reference to financial information, which would require a special treatment of this data. Confronting the SWIFT main weaknesses one may notice that the Agreement supplements the current loophole concerning data retention limitation (art. 12 of the Agreement) and purpose and use limitations (art. 6 of the Agreement). However, the right of legal remedies in case of unlawful processing of information is still not guaranteed at the same level for EU citizens and citizens living in the EU one the one side, and the US citizens on the other side.

[37] D. Korff, *EU-US Umbrella...*

 DOI: 10.17103/sybil.19.15