EDPS DECISION
of 19 December 2019
relating to the technical administration of FIU.net by Europol

1. INTRODUCTION

1.1. This decision concerns the technical administration of the Financial Intelligence Unit Network ("FIU.net") network by Europol.

1.2. This decision is addressed to Europol. Under Article 43 of Regulation (EU) 2016/794 of 11 May 2016 ("the Europol Regulation")[1], the EDPS is responsible for monitoring and ensuring the application of the provisions of the Europol Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol.

2. BACKGROUND

2.1. On 15 June 2018, the EDPS received a letter from Europol seeking the opinion of the competent data protection supervisory authority at EU level in relation to data protection and information security concerns expressed by several Financial Intelligence Units ("FIU") regarding the foreseen embedment of FIU.net into SIENA. The letter contained the opinion of Europol on the matter, a letter from FIU.net Advisory Group with a list of questions, a document compiling the different concerns expressed by FIUs and an overview of the FIU Solution Roadmap. In addition, Europol provided the EDPS with further clarifications on the envisaged solution during the bi-monthly meeting held on 9 July 2018.

2.2. On 20 July 2018, the EDPS issued an Opinion on the compliance of the planned embedding of FIU.net into SIENA with the Europol Regulation. The EDPS considered that Article 18(2)(d) of the Europol Regulation, interpreted together with Annex II.B(1), did not allow Europol to process data related to data subjects who did not class as 'suspects' of money-laundering or terrorist financing activities under the applicable national criminal law. These articles apply both to Europol acting as controller and as service provider, as the Europol Regulation does not make any distinction. Considering the fact that FIUs activities do not fall under the applicable national criminal laws, the EDPS considered that Europol did not have sufficient legal basis to embed FIU.net into SIENA.

2.3. In that Opinion, the EDPS also stressed that this finding had implications for the current technical administration of FIU.net by Europol.

2.4. On 8 July 2018, the FIU.net Advisory Group referred a series of questions regarding the embedding of FIU.net into SIENA to the Europol Cooperation Board ("ECB").

2.5. Between September 2018 and January 2019, as follow-up to the Opinion, the EDPS engaged in discussions with Europol in order to assess the feasibility of a technical

[1] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 200/934/JHA, 2009/935/JHA, 200/936/JHA and 2009/968/JHA.

solution that would exclude the processing of personal data by Europol for the purpose of the technical administration of FIU.net.

2.6. On 25 January 2019, the EDPS and Europol visited the Belgian Financial Intelligence Unit ("FIU") in order to obtain a practical understanding of the personal data processing activities involved in FIUs' tasks.

2.7. In letters of 6 February and 23 April 2019, Europol argued that the concept of suspect within the meaning of the Europol Regulation should not be interpreted only in relation to criminal procedural law but should also take into account other laws such as the ones implementing Directive (EU) 2015/849[2] (the "Anti-Money Laundering Directive") and the nature of the work done by FIUs, which is "not based on value thresholds but on strong and in depth investigations which are being shared with the FIUs as competent authorities", and of FIUs which "analyse and prioritise these data".

2.8. In a letter of 30 April 2019, the EDPS informed Europol that the technical solution explored, end-to-end encryption, would not allow Europol to perform the technical administration of FIU.net without processing personal data. According to Article 3(6) of Regulation (EU) 2018/1725[3], such processing activity would qualify as processing of pseudonymous data. In this letter the EDPS also informed Europol that he had decided to refer the matter of the interpretation of the concept of "suspect" to the ECB, in line with Article 44(1) of the Europol Regulation which mandates the EDPS to act in close cooperation with the national supervisory authorities on issues requiring national involvement, and Article 45(3)(b) of the Europol Regulation, according to which the ECB is competent to examine the difficulties of interpretation or application of the Europol Regulation.

2.9. On 11 September 2019, the ECB provided an answer to the questions raised by the FIU.net Advisory Group, and took position on the interpretation of the concept of "suspect" within the meaning of the Europol Regulation. In its Opinion, the ECB notes that there is no harmonised status or legal definition of the term 'suspect' under EU and national laws. It concludes that it is not possible to ascertain that all information and personal data to be processed under the envisioned solution, would fall within the remit of Europol's competence. The ECB therefore rules out the legal competence for Europol to process data exchanged through FIU.net.

2.10. On 1 October 2019, Europol Data Protection Function (DPF) consulted the EDPS in relation to a request of the Swedish FIU made to Europol to delete all information processed in FIU.net and older than five years. The DPF inquired whether they were legally authorised to do so, in light of the position of the ECB.

---

[2] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (AMLD).

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) 45/2001 and Decision No 1247/2002/EC.

3. FINDING OF FACTS

Processing of personal data by Europol

3.1. FIU.net is the computer network that provides information exchange between the FIUs of the European Union. Initially foreseen in Council Decision 2000/642/JHA of 17 October 2000[4], it has been subsequently referred to Directive 2005/60/EC (3rd Anti-Money Laundering Directive)[5] and in the current Anti-Money Laundering Directive[6] as a tool of information exchange between FIUs. None of these instruments provides any instructions as regards the structure of the network. Article 51 of the Anti-Money Laundering Directive require the EU FIU's Platform to exchange views and provide advice on implementation issues relevant for FIUs, such as the standardization of reporting format through the FIU.net or its successor. FIU.net is also referred to in Article 13 of Directive (EU) 2019/1153[7] as a tool for FIUs to exchange financial information, and bank account information, with Europol for the purposes of prevention, detection, investigation or prosecution of serious criminal offences, according to the provisions of this Directive.

3.2. FIU.net was created in 2002 and initially operated by the Dutch Ministry of Justice. The technical administration of the system was then transferred to Europol in 2016 after a Common Understanding was agreed in December 2015.

3.3. FIU.net is as a decentralized information exchange network. All the connected FIUs have their FIU.net equipment within their own premises and manage their own information. Europol is part of the network, as additional node. During the exchanges the EDPS had with the DPF following the informal consultation of 1 October 2019, the DPF informed the EDPS that Europol manages the system centrally, i.e. Europol has technical access to all servers in the network. In addition, some FIUs do not have the technical capabilities to perform certain operations such as the deletion of the information. This means that only Europol is able to perform such operations.

3.4. FIU.net is currently used for three main purposes: (1) cross-border reporting and dissemination[8]; (2) case building data exchange[9] ; (3) "anonymous" cross-match through Ma3tch.[10] Ma3tch (autonomous, anonymous, analysis) is a matching tool within FIU.net, which makes it possible for FIUs to match names to find relevant data that are possessed by other connected FIUs and Europol.

3.5. The possibility for Europol to have technical access to all servers in the network, as well as to perform operations over the personal data exchanged through FIU.net means

---

4 Council Decision of 17 October 2000, concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

5 Directive 2005/60/EC of The European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

6 Art. 56(1) AMLD.

7 Directive (EU) 2019/1153 of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA.

8 Art. 53 AMLD. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, even if the type of predicated offences that may be involved is not identified at the time of the exchange.

9 Joint analyses as referred to in Art. 51 AMLD.

10 Art. 56(2) AMLD.

that Europol processes personal data for the purposes of the technical administration of FIU.net.

Possibility for Europol to perform the technical administration of FIU.net without processing personal data

3.6. Between September 2018 and January 2019, Europol and the EDPS assessed whether the use of end-to-end encryption would allow Europol to perform the technical administration of FIU.net without processing personal data.

3.7. In a letter of 29 November 2018, Europol pointed out that the use of end-to-end encryption would prevent Europol to audit the system and to answer Commission's requests for statistics on the use of the system.

3.8. The EDPS discarded this solution on the basis of the technical difficulties linked to its implementation, and of the definition of pseudonymous data provided by Article 3(6) of Regulation (EU) 2018/1725[11], which entered into force on 11 December 2018. According to this definition, as long as additional information allowing the re-identification of individuals concerned by the processing is available, such processing qualifies as processing of pseudonymous data. This means that wherever a third party is able to decrypt the information exchanged over the network, such processing activity qualifies as personal data. Europol would thus be processing personal data in capacity of service provider.

3.9. As a result, the use of end-to-end encryption tools does not prevent Europol from processing personal data for the purposes of the technical administration of FIU.net.

Qualification of individuals targeted by FIUs' activities as "suspects"

3.10. Article 32 of the Anti-Money Laundering Directive requires Member States (MS) to establish FIUs in order to prevent, detect and effectively combat money laundering and terrorist financing. This obligation is however not new to this Directive. MS had already established FIUs to comply with their obligations under Directive 311/308 EEC (the 1st Anti-Money Laundering Directive). The creation of such entities responds to a need identified at international level in the context of the fight against money laundering and terrorist financing activities to connect the private sector (in particular the financial market) with structures enforcing criminal legislation.[12] Countries over the world adopted initiatives to establish a new type of a state authority, the FIU, which is meant to function as an intermediary between the private entities, subject to Anti-Money Laundering/terrorist financing obligations, and law enforcement agencies.[13]

---

[11] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) 45/2001 and Decision No 1247/2002/EC.

[12] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Financial Intelligence Units, https://www.coe.int/en/web/moneyval/implementation/fiu

[13] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Financial Intelligence Units, https://www.coe.int/en/web/moneyval/implementation/fiu

3.11. FIUs are central national units responsible for receiving and analysing suspicious transactions reports (STRs) and other information[14] relevant to money laundering, associated predicated offences or terrorist financing.[15] STRs are produced by "obliged entities" and refer to transactions where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing.[16]

3.12. "Obliged entities", as defined under Art. 2 of the Anti-Money Laundering Directive, are private parties and include entities such as credit institutions, financial institutions, auditors, external accountants, tax advisors, notaries and other independent legal professionals, estate agents, providers of gambling services.

3.13. Financial intelligence should be distinguished from financial investigations, a task for which law enforcement authorities are competent, and which purpose is to collect evidence where there are grounds to suspect money laundering, associated predicated offences or financing of terrorism. FIUs only send information about suspicious transactions to law enforcement authorities if they find that the suspicion is substantiated.

3.14. FIUs therefore act before the start of any preliminary proceedings or criminal investigation. By way of consequence, they process data about individuals about whom there is not sufficient evidence for them to be classed as suspects or "potential future criminals" under the applicable criminal law. Their only "reprehensible" activity is to be involved in a financial transaction which is unusual and thus detected as "suspicious".

3.15. Consequently, personal data processing activities of FIUs are subject to Regulation (EU) 2016/679 (the GDPR) [17] and not to Directive (EU) 2016/680 (the Law Enforcement Directive)[18].[19]

3.16. Yet, despite a clearly expressed need to keep financial intelligence tasks separated from financial investigations[20] as related personal data processing activities are set up for different purposes, MS have made different choices when establishing FIUs. In some MS, FIUs are of administrative nature and are placed under the authority of Ministries of Finance, Justice, Interior, Central banks or supervisory authorities. In others, FIUs have a law enforcement nature and are part of a structure competent to fight economic or other serious crimes. Finally, in some MS, FIUs are of a hybrid nature, in which case

---

14 Such as Suspicious Analysis Reports (SARs) or Unusual Transaction reports (UTRs).

15 Article 32(3) Directive (EU) 2015/849 of 20 May 2015 (4th AMLD).

16 Art. 33(1)(a) AMLD.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ*, L 119, 4 May 2016, pp. 1 and fol.

18 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

19 Article 41(1) AMLD.

20 For instance, see EU FIU's Platform, Mapping exercise and gap analysis on FIU's powers and obstacles for obtaining and exchanging information, 15 December 2016, p.141. The authors noted that keeping analytical activities and law enforcement tasks separated was an essential conditions for cross-border cooperation. In that sense, FIU officials note that the delimitation of intelligence and investigation is not sufficiently clear and has a negative impact on the cross-border cooperation of FIUs.

they are established in national police offices or in the offices of the attorney general/prosecutor but separated from operational/judicial units and they are composed both of police officers and analysts from non-police organisations. The choice of the nature of the FIU has, amongst other, an impact on the kind of information the FIU can get access to for its analysis[21] and the scope of its powers[22].

3.17. The EDPS' operational visit to the Belgian FIU illustrated that the work of the FIU consists of receiving STRs from obliged entities and to individualise the suspicions by gathering evidence of the involvement of a given individual into money-laundering or terrorist financing activities. The work of the Belgian FIU is supervised by a magistrate who, however, does not act in his judicial capacity. At the end of the process, the FIU refers the case to the competent judicial authority which will decide whether to open a judicial inquiry or not.

4. BREACH

4.1. The technical administration of FIU.net involves the processing of personal data.

4.2. It was not possible to devise a technical solution that would allow Europol to perform the technical administration of FIU.net without processing personal data.

4.3. Article 18(2)(d) of the Europol Regulation, read together with Annex II.B(1), limits the categories of data subjects about whom Europol can process data to suspects, potential future criminals, contacts and associates, victims, witnesses and informants, including in capacity of service provider.

4.4. According to Annex.II.B (1)(a) of the Europol Regulation "suspects" are "persons who, pursuant to the national law of the MS concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence".

4.5. Activities of FIUs are in principle not subject to national criminal procedure law.

4.6. As consequence of the above, FIUs do not process information about individuals who are classed as "suspects" according to the applicable national criminal procedure law.

4.7. The ECB, in its Opinion of 11 September 2019, in the context of its task of examining difficulties of interpretation of the Europol Regulation under Article 45(3)(b) of the Europol Regulation, took the view that "*the concept of suspect should not be broadened so as to include the investigation of other suspicious activities by private entities and competent authorities, acting within the remit of specific laws such as the ones transposing the Anti-Money Laundering Directive.*"

---

[21] For instance, law enforcement FIUs have access to law enforcement databases. See M. Penna, The 'Pre-investigative' Role of Financial Intelligence Units in Recovering Assets (April 2017) 'Chasing Criminal Money' Edited by Katalin Ligati and Michele Simonato - p269-285 - Hart Publishing, Bloomsbury Professional.

[22] For instance, administrative FIUs usually have the power to FIU the power to postpone the execution of a suspicious financial transaction or the power to block any transactions involving the bank accounts of the criminals or criminal organisation for a short period of time before the prosecutor' s office decides whether to seize the criminal proceeds. Law enforcement FIUs will have broader powers such as the power to freeze transactions and seize assets. See M. Penna, *op.cit.*

4.8. The ECB has further considered that "*the variety of FIUs' legal status and their scope of competence, combined with the specificity of each Member State's national criminal procedural law, does not provide a consistent framework which would allow to ascertain that all information and personal data to be processed under the envisioned solution would fall within the remits of Europol's competence*".

4.9. In light of the above, the EDPS considers that Europol cannot ensure that the technical administration of FIU.net will not involve the processing of data about persons who do not class as suspects.

4.10. The EDPS is therefore of the opinion that Europol does not have sufficient legal basis to provide support to all MS in the form of the technical administration of FIU.net as currently operated.

5. BAN

5.1. Taking into account that it is not possible for the EDPS to make proposals for remedying that breach and for improving the protection of the data subjects pursuant to Article 43(3)(b) of the Europol Regulation, since the only possible remedy would be to modify the applicable legal framework, a task that falls outside Europol's scope of competence,

5.2. Taking into account that it is not possible either for the EDPS to order the erasure and destruction of personal data which have been processed in breach of the provisions governing the personal data, pursuant to Article 43(3)(e) of the Europol Regulation,

5.3. The EDPS, pursuant to Article 43(3)(f) of the Europol Regulation, bans all processing by Europol of data related to individuals who are not classed as "suspects" under the applicable national criminal procedure law in the context of the technical administration of FIU.net.

5.4. The EDPS however understands that FIU.net plays a crucial role in the fight against money laundering and terrorist financing at EU level, in particular to allow and foster the cross-border cooperation between MS, and it is an important tool to ensure compliance with the new obligations introduced by the Anti-Money Laundering Directive in terms of exchanges of information.

5.5. The EDPS also takes into account that the processing of personal data by Europol for the purposes of the technical administration of FIU.net does not involve the processing of operational data but is limited to the maintenance and security of the information and the smooth functioning of the network.

5.6. For the above reasons, the EDPS suspends the ban for a period of one year, counting from the day of this decision, in order to allow Europol to ensure a smooth transition of the technical administration of FIU.net to another entity.

5.7. During this transition period, i.e. until the ban becomes effective, the EDPS asks Europol to report every two months on the steps taken to achieve such transfer. In case the EDPS finds that Europol is not taking sufficient action to ensure the transition of

the technical administration of FIU.net to another entity, or if the EDPS finds out that Europol's personal data processing activities involve significant risks for individuals' rights and freedoms, the EDPS would then remove the suspension of the ban and order its immediate implementation.

5.8. During this period, Europol is only allowed to perform technical operations, which are strictly necessary for the purpose of the technical administration of the system.

6. REQUEST OF DELETION BY THE SWEDISH FIU

6.1. The deletion of operational data shared over FIU.net and older than five years as requested by the Swedish FIU to Europol is not a task related to the technical administration of FIU.net but a processing of operational data that should be performed by each FIU or Europol in its quality of member in the network.

6.2. Europol must not execute the request of the Swedish FIU but transmit it to all other FIUs for them to proceed to the deletion of the data.

6.3. Would a FIU not be technically able to delete those personal data, this FIU should explicitly require the technical assistance of Europol, which should only act on behalf and under the instructions of this FIU.

7. JUDICIAL REMEDY

7.1. Pursuant to Article 48 of the Europol Regulation, any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.