The Data Protection Gap

From Private Databases to Criminal Files

Els De Busser

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

The article examines the "data protection gap" in EU law concerning the transfer of personal data from private companies to law enforcement authorities for criminal investigations. While commercial data processing falls under the proposed regulation and police/judicial processing under the proposed directive, transfers between the two remain unregulated. The author analyses how such transfers affect core data protection principles, including accuracy, reliability, purpose limitation, necessity, and security, drawing on Europol's practices and existing EU–US agreements. She argues that the proposed directive should explicitly cover these transfers, with complementary obligations for private companies under the proposed regulation, to ensure effective protection while enabling criminal investigations.

AUTHOR

Els De Busser

Assistant Professor
Universiteit Leiden

CITATION SUGGESTION

E. De Busser, "The Data Protection Gap", 2013, Vol. 8(1), eucrim, pp17–22. DOI: https://doi.org/10.30709/eucrim-2013-003

Published in
2013, Vol. 8(1) eucrim pp 17 – 22
ISSN: 1862-6947
https://eucrim.eu

Debates on the reform of the EU's data protection legal framework are currently being held in the Council of the EU and the European Parliament.[1] One particular issue has, however, not (yet) been included in these debates: the processing of personal data by law enforcement authorities for the purpose of criminal investigations after these data were originally collected by private companies for the purpose of their commercial activities. This topic has, however, been discussed at several other negotiation tables. On the EU level, the Cybersecurity Strategy[2] released in February 2013 and the continuing debate on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences[3] and serious crime as well as the controversy that surrounded the Data Retention Directive[4] demonstrate the difficult balance between the protection of personal data and the need to obtain private sector information for the purpose of investigating and prosecuting criminal offences. This debate has also been held in the context of transatlantic cooperation. The 2010 EU-US Agreement on the processing and transfer of financial messaging data for the purposes of the Terrorist Finance Tracking Programme (TFTP Agreement)[5] is one of the best examples of how private sector information is used to prevent and prosecute serious crime such as terrorism. The second EU-US joint review of the implementation of the TFTP Agreement listed several cases in which the information received from a company called SWIFT[6] – the market leader in the transmission of financial messaging data between banks worldwide – helped in tracing, identifying, and, ultimately, prosecuting persons involved in the preparation or execution of terrorist attacks.

Since the above-mentioned cases indicate that the exchange of personal data between private companies and law enforcement authorities has significant added value, it is all the more surprising to see that this form of cooperation is neither dealt with on the EU level in the proposed data protection directive nor in the proposed data protection regulation. In fact, the transfer of personal data from a private company to a law enforcement authority for the purpose of a criminal investigation or prosecution falls in the gap between both proposed legal instruments. Whereas data processing by private companies is governed by the proposed regulation, data processing by law enforcement authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties is dealt with by the proposed directive. The question of which legal instrument should contain provisions on safeguarding data protection in this type of transfer should thus be part of the ongoing discussions in the Council and the Parliament. This contribution will attempt to address that particular question. It is only by analysing the effect of the data transfer from private companies to law enforcement authorities on data protection principles that the question can be answered as to what the applicable legal instrument should be. For this reason, the quality and security of the personal data that are the subject of this transfer are examined here. Logically, the currently applicable legal instruments on data protection will be considered as well as the pending reform proposals.

The proposed directive will not be applicable to Europol. However, Europol plays a key role in the EU's law enforcement cooperation and has experience in dealing with data transfers from private companies. Its rules on data processing can function as an inspiration for the proposed EU legal instruments on data protection. For this reason, this contribution will also include the analysis of data transfers involving Europol.

I. Data Processing Standards

Directive 95/46/EC is applicable to the processing of personal data wholly or partly by automated means. It is equally applicable to the processing of personal data other than by automated means which are part of a filing system or are intended to become part of a filing system in the course of an activity that falls within the scope of Union law. Processing of personal data for the purpose of commercial activities is thus included in the scope of Directive 95/46/EC. The proposed regulation does not change this scope. Framework Decision 2008/977/JHA is applicable to the transmitting of personal data that a Member State receives from another

Member State for the purpose of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. The proposed directive expands its scope to include also domestically gathered personal data.

No legal instrument adopted on the EU level lays down standards on personal data transfers from private companies to law enforcement authorities in general, although for specific types of companies legal instruments exist.[7] With two applicable legal instruments in the area of data protection at the moment and two new and revised legal instruments pending, the question is where to include provisions on these transfers. For answering this question, the precise nature of this transfer should be defined. The currently applicable legal instruments do not contain a definition of transfers from private companies to law enforcement authorities. It is certainly not "processing under the authority of the controller and processor"[8] since there is no reporting or supervision between both parties. It can also not be qualified as "processing on behalf of a controller"[9] because that would mean that the law enforcement authority would be processing the data for a commercial purpose or vice versa. It is also not a transfer to a third state or international organisation. Obviously, it could constitute a transfer to a third state's law enforcement authority but it can also be a transfer within the EU or even within one Member State.

Because both the company and the law enforcement authority are data controllers but both process the data for the performance of different activities unrelated to each other, the transfer of personal data from a company to a law enforcement authority should be defined as a transfer from a data controller to another data controller where the purpose of the data processing changes from a commercial purpose to that of a criminal investigation or prosecution.

The data protection principles that are the basis of the aforementioned legal instruments are enshrined in the 1981 CoE Data Protection Convention. Even though this convention is also being modernized at present, the basic principles of data protection still remain the same. Nonetheless, it should be analysed how these principles are or could be affected when a transfer of data from private companies to law enforcement authorities is concerned.

1. Degrees of Accuracy and Reliability

Directive 95/46/EC and Framework Decision 2008/977/JHA both state that the data controller must ensure that personal data are accurate and, where necessary, kept up to date. The proposed directive made this provision more precise by explicitly making it the competent authority's responsibility as a data controller to adopt policies and implement appropriate measures to ensure that the processing of personal data is performed in compliance with the provisions adopted pursuant to the directive. This includes the right to rectification of inaccurate or incomplete data and the right to deletion. More importantly, in accordance with the proposed directive, law enforcement authorities are also obliged to indicate the degree of accuracy and reliability of the personal data they process.

When personal data are transferred from a private company that is a data controller to a law enforcement authority, which then becomes the data controller, the accuracy of the data should be safeguarded. The personal data as such can be accurate but that does not make the assessments or conclusions drawn from them accurate. When a person buys several litres of artificial fertiliser needed for his vegetable farm and, shortly after, buys a timer for a sprinkler system in his backyard, the data regarding these purchases may be correct, but one of the conclusions that can be drawn from these purchases could be that this person is producing explosives in his home. A "new"[10] provision in the proposed directive obliges law enforcement authorities to distinguish different degrees of accuracy and reliability when processing different categories of personal data: in particular, the distinction between personal data based on facts, on the one hand, and

personal data based on personal assessments, on the other hand. The provision is not entirely new as it is a copy of principle 3 of CoE Recommendation (87)15 regulating the use of personal data in the police sector.

In its own rules on analysis work files, Europol has included the stipulation that data stored in these files for analysis purposes shall be distinguished according to the assessment grading of the source and the degree of accuracy or reliability of the information. This means that data based on facts are distinguished from data based on opinions or personal assessments.[11] Information is evaluated by Europol using a 4x4 system that awards a code to the source of the information and a code to the information itself. Based on these codes, decisions are made regarding the accuracy of the information or the reliability of the source.[12] The responsibility for data processed at Europol, particularly as regards transmission to Europol and the input of data, as well as their accuracy and their up-to-date nature, lies with the Member State that has communicated the data. However, with respect to data communicated to Europol by third parties, including data communicated by private parties, this responsibility lies with Europol.[13]

Where the quality of personal data that law enforcement authorities (including Europol) have received from private entities is concerned, the currently applicable rules do not provide for the necessary safeguards. However, as long as the provision on distinguishing degrees of accuracy and reliability survives the negotiations on the proposed directive, it is not necessary to provide for further rules on ensuring the quality of data transferred from private entities to law enforcement authorities.

2. Processing for Compatible Purpose and Necessity

Personal data can be processed for legitimate purposes only and should not be processed for purposes incompatible with the purpose they were collected for. Processing for a compatible purpose is allowed but a definition of a compatible purpose has not been developed yet. The concept could be defined as having "functional equivalence" or similarity to the original purpose. Additionally, the data subject should be able to reasonably foresee[14] the processing of his data for that purpose.[15] Functional equivalence means that both purposes have a large degree of similarity, e.g., a pharmacist's database contains personal data on patients' purchases of specific medication as well as their contact data. Using these data to advise the patient on the dosage of his medication would be a functionally equivalent and foreseeable, and thus compatible, purpose. Giving access to this database to labour inspectors visiting pharmacies in order to verify that all their employees are registered would not be a compatible purpose. In order to process personal data for incompatible purposes the legality and necessity requirement should be fulfilled. This includes the cases where personal data are collected for commercial purposes and afterwards processed for the purpose of a criminal investigation or prosecution,

The traditional purpose limitation principle is included in Directive 95/46/EC as well as in the proposed regulation. Derogating from the principle is allowed when this is necessary to safeguard the prevention, investigation, detection and prosecution of criminal offences. What it really means is that no mass transfer of personal data is allowed. It is essential to maintain the nexus between the data that are transferred by a law enforcement authority and the criminal investigation or prosecution that they should be processed for. For example, when the pharmacist in the aforementioned example is under investigation for selling a counterfeit cancer drug, searching his database for all patients who had bought this particular cancer drug during a specific period of time would be an allowed derogation from the purpose limitation principle, because there is a clear nexus between the personal data and the ongoing investigation. If a pharmacist would be requested to give a law enforcement authority access to his database to "comb" through it, however, such a nexus would not exist.

Mass transfers of data were one of the problems with respect to first version of the 2010 TFTP Agreement that was rejected by the European Parliament. The second version included a new role for Europol. Article 4

of the agreement gives Europol the power to give binding force to the requests from the UST. Europol was thus put in the unexpected position as the authority that decides upon the legitimacy of the requests to obtain data from a private company. Since the entry into force of the agreement Europol verifies the requests formulated by the UST on three aspects. The request should identify as clearly as possible the categories of data requested, the necessity of the data should be demonstrated and the request should be tailored as narrowly as possible. The company in question, SWIFT, must wait for Europol's authorisation before carrying out the request.[16] At the moment of the first joint review of the TFTP Agreement in 2011, an inspection report by the Europol Joint Supervisory Body (JSB) concluded that the requests that had been sent made a proper verification by Europol within the terms of the agreement, impossible. The second joint review report highlighted that Europol's verification role is based on an operational assessment of the validity of the request. The reviewers concluded that Europol is best placed for deciding on the requirement of tailoring the requests as narrow as possible while enjoying a certain margin of discretion.[17] Nonetheless, the Europol JSB still has concerns regarding the amount of data being transferred since subsequent requests – that have all been positively verified by Europol – with an average of one per month essentially cover an uninterrupted time-period. Another concern expressed by the JSB is the continuing role that oral information provided by the UST to Europol plays in the verification process.[18] Therefore, in practice mass transfers of personal data are not entirely ruled out.

The proposed directive will not be applicable to Europol; yet, for transfers from private companies to the Member States' law enforcement authorities, the necessity requirement included in the proposed directive should be strengthened. The same goes for the proposed regulation. A provision should be added stipulating that the necessity requirement means that a nexus should be present between the personal data requested and the criminal investigation or prosecution for which their transfer and processing will be carried out.

II. Data Security

Data controllers are responsible for implementing appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other forms of unlawful processing. The level of security should be appropriate for the risks presented by the processing and the nature of the data in question.[19] Companies that transfer personal data to law enforcement authorities should thus secure the data until the moment of transfer. Law enforcement authorities have a similar obligation of ensuring data security under Framework Decision 2008/977/JHA. The provisions are more specific, also including equipment access control, data media control, storage control, communication control, transport control, etc.

The proposed directive and the proposed regulation both introduce the obligation for the data controller to notify the supervisory authority of a personal data breach.[20] The provision states that the controller needs to document any personal data breaches, comprising the facts surrounding the breach, its effects, and the remedial action taken. If personal data are sent to law enforcement authorities that were the subject of a data breach when under the control of a company as data controller, the above-mentioned documentation should also be transferred to the law enforcement authority in question. This is not included in any of the proposed legal instruments. The purpose of this notification is not to verify compliance with the regulation but to be informed of possible manipulation of personal data that can be used in a criminal investigation or prosecution at a later stage. In view of the accuracy and reliability of personal data processed by law enforcement authorities, the fact that a security breach may have affected or disclosed these data at an earlier stage could be vital information.

Europol itself takes the necessary technical and organisational steps to ensure data security. Each Member State and Europol implement measures to ensure controls regarding data access, data media, etc. In accord-

ance with the Europol Decision, direct contact with private companies however is not allowed. Europol may only process personal data transmitted by companies via the National Unit of the Member State under whose law the company was established, and the transfer should be in accordance with the national law of that Member State.[21] Thus, for the security of the personal data in the hands of the private company, the national law, which needs to comply with Directive 95/46/EC and, in the future, with the proposed regulation, will be applicable.

The introduction of data breach notifications in the proposed data protection legal framework of the EU is highly important to data processing for commercial purposes and data processing for the purposes of a criminal investigation or prosecution. In view of distinguishing different degrees of accuracy and reliability, a transmission of the notification by the private company to the receiving law enforcement authority should be made mandatory.

III. Data Protection Reform Package

Now that the EU institutions are discussing the reform of the data protection legal framework, the timing is appropriate to also include clear provisions on how to organise transfers of personal data from private companies to law enforcement authorities and ensure that the data protection principles are respected. The question is whether these provisions should be incorporated in the proposed directive or in the proposed regulation. For answering this question, the scope of both legal instruments is significant.

The scope of the proposed directive is limited to the processing of personal data by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The proposed regulation is defined by the processing of personal data in the course of an activity which falls within the scope of Union law. The focus of this contribution is a transfer from what is covered by the proposed regulation to what is covered by the proposed directive. This means that most of the necessary data protection provisions already exist. Only this particular transfer is not regulated yet. It would be more efficient including the lacking provisions on this type of transfer in one of the existing legal instruments than creating a fully new one.

Considering the ECJ's jurisprudence on the purpose of data processing, the element of safeguarding the internal market that was used in the case on the Data Retention Directive, could not be used in the data transfers that are discussed here.[22] The element of essential objective or the final purpose of the data processing would lead to the conclusion of regulating these transfers in the proposed directive.[23] This would be in accordance with the jurisprudence of the ECJ and it would respect the scope of the proposed directive that is limited to processing of data by law enforcement authorities. Therefore the proposed directive should include the stipulation that its provisions also apply to the personal data a Member State's law enforcement authority receives from a private company.

IV. Closing the Data Gap

No discussion has taken place on whether or not personal data collected by private companies are needed by law enforcement authorities. Without these data, investigations into many criminal offences would be unsuccessful. The question is how data protection can be guaranteed when personal data are transferred from private companies to law enforcement authorities, since both data controllers' processing activities fall within the scope of two different legal instruments. Moreover, these two legal instruments are undergoing a reform process at the present time.

For law enforcement authorities, it is crucial to have clarity on the accuracy and reliability of personal data processed for the purpose of criminal investigations and prosecutions. For this reason, it should be mandatory for the company transferring data, which were the subject of a data security breach, to inform the receiving law enforcement authority of this incident. Besides being accurate, personal data should also be proportionate in relation to the purpose they are processed for. With respect to the transfers discussed here, because the data are processed for a purpose that is incompatible with the purpose they were collected for, the necessity requirement should be fulfilled. Thus, only those data that have a clear nexus with a specific criminal investigation or prosecution should be transferred.

The necessity requirement should be explicitly added to the provisions of the proposed directive. Informing law enforcement authorities of a data breach that occurred before the data were transferred to them by private companies is the private company's obligation and should therefore be included in the proposed regulation. To rule out confusion as to which data protection rules govern the processing of personal data after a transfer from private companies to law enforcement authorities, an explicit provision should be included in the proposed directive declaring the provisions applicable to these data.

Now that the EU's legal framework on data protection is being revised, the momentum should be used to include provisions on the protection of personal data that are the subject of a transfer from a private company to a law enforcement authority.

---

1. Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD), 16.01.2013 and Draft Report on the 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, 2012/0010(COD), 20.12.2012.↩
2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07.02.2013.↩
3. Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 02.02.2011.↩
4. Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. L 105, 13.04.2006, p. 54.↩
5. Agreement on 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, O.J. L 195, 27.07.2010, p. 5.↩
6. Society for Worldwide Interbank Financial Telecommunication.↩
7. Legal instruments such as the aforementioned Data Retention Directive and the TFTP Agreement as well as the 2012 Agreement between the EU and the US on the processing and transfer of passenger name record data (the PNR Agreement), etc.↩
8. Article 16 of Directive 95/46/EC (Article 27 of the proposed regulation) and Article 22 of the proposed directive.↩
9. Article 17 of Directive 95/46/EC (Article 26 of the proposed regulation) and Article 21 of the proposed directive.↩
10. This provision was included in the proposal for Framework Decision 2008/977/JHA but did not make it to the final text.↩
11. Council Decision on adopting the implementing rules for Europol analysis work files, O.J. L 325, 11.12.2009, p. 14.↩
12. Europol Information Management Booklet, File no: 2510-271. See also "Europol: '4x4' intelligence handling codes includes 'dodgy data'", Statewatch, accessed January 7, 2013, http://www.statewatch.org/news/2013 /jan/03europol-dodgy-data.htm.↩
13. Article 28 Europol Decision.↩
14. ECtHR,The Sunday Times v. United Kingdom, 1979, §49; Malone v. United Kingdom, 1984, §§67-68; Rotaru v. Romania, 2000, §55 and Amman v. Switzerland, 2000, §56.↩
15. L. Bygrave, Data protection law. Approaching its rationale, logic and limits, The Hague, Kluwer law International, 2002, p. 340. See also E. De Busser, Data Protection in EU and US Criminal Cooperation, Antwerp, Maklu, 2009, p. 68.↩
16. Article 4 of the TFTP Agreement.↩
17. Report on the second joint review 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 TFTP, SWD(2012) 454 final, 14.12.2012, pp. 6-7.↩
18. Ibid., pp. 2-3.↩
19. Article 17 Directive 95/46/EC.↩
20. This notification was inspired by the personal data breach notification in Article 4(3) of e-privacy Directive 2002/58/EC.↩
21. Article 24 Europol Decision.↩
22. ECJ C-301/06, Ireland v. Council and Parliament, 2009.↩
23. ECJ C-317/04 and C-318/04, Parliament v. Council, 2006.↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union