Improving criminal justice in cyberspace

Fields marked with * are mandatory.

QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace

This questionnaire is designed to provide further information to the European Commission Task Force on Cross-border Access to Electronic-Evidence, in order to facilitate swift progress of our work. We would be grateful for receiving your replies by Friday 16 September 2016.

Whereas some of the questions mainly refer to the legal framework, other questions are more related to current (working) practices in your Member State. The diversity in questions may require you to involve multiple organisations, including e.g. your responsible ministry, prosecutors and / or your national or regional police.

We are aware that you receive many questionnaires, including on these issues. Therefore, where you have provided information already under GENVAL or the Council of Europe, please feel free to simply refer us to answers already provided elsewhere. As the picture is not yet complete across Member States we could not altogether avoid certain questions. If you would like to share existing documents or responses to other questionnaires with us, please feel free to upload them here or to email them to us at **home-cybercrime@ec.europa.eu**.

If you prefer to respond to all or parts of the questionnaire in a separate document, you can download a PDF of this questionnaire by clicking on the link to the right and email your response to **home-cybercrime@ec.europa.eu**. You can also contact us at that email address for a Word version.

We very much appreciate your time and efforts and would like to thank you for your participation. Your contribution is a key element in our effort to address the existing problems.

The E-Evidence Task Force

Administrative questions

*

Please indicate on behalf of which EU Member State you are responding to the questionnaire

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden
- United Kingdom

*

Please indicate which organisation you are representing

Ministry of Justice – Directorate general for Criminal Affairs – Office I – Legislative and International Affairs

*

Please provide your contact details (name, e-mail address, phone number)

*

Did you coordinate your response to the questionnaire amongst different organisations in your Member State?

- (•) Yes
- ( ) No

If yes, could you please indicate amongst which organisations you coordinated your response to the questionnaire?

Optional inclusion of files

Please provide any details about the file(s) you are including

Please upload your file(s)

1. Direct cooperation with service providers for obtaining access to electronic evidence

Part 1 of the questionnaire only concerns direct cooperation between law enforcement authorities and private sector service providers (e.g. providers of telecommunications services or providers of cloud services).

It may concern both mandatory and voluntary cooperation, depending on whether there is (i.e. search warrant) or there is no legal title for compelling the service provider to disclose the electronic evidence.

It does not cover situations where requests are made between authorities from a requesting and a receiving state, e.g. in the framework of a mutual legal assistance or mutual recognition procedure (see Part 2 of the questionnaire).

1.1 Normal practice within your domestic jurisdiction

1. What is the relevant legal framework for direct cooperation requests in your Member State? Could you please copy or include reference to the relevant provision(s) in your legislation?

Currently, there's not mandatory direct cooperation between Law Enforcement and third parties service providers (telecommunications and cloud). Requests could be made under law regulation and through specific court order (except basis data such as account subscriber, registration forms).

The legal framework that permits and regulate the request is provided for by Legislative Decree 1 August 2003 no. 259, Article 96 paragraph 1 ("Operators shall be obliged to provide services for the purposes of justice in response to requests for wiretapping and information submitted by the competent Judicial Authorities") and by **Section 132** (Traffic Data Retention for Other Purposes) of Personal data Protection Code (***see attachment***).

2. For these direct cooperation requests, is there a difference in your legal framework between providers of telecommunications services and providers of information society services (e.g. cloud service providers)?

No, the same legal framework is applied.

3a. How many domestic requests for direct cooperation are made per year by your authorities? Could you please specify the number of requests per section of the applicable legal framework and type of service provider?

There is not a unique database, the only statistics available are kept within the Italian national point of Contact for the G7 24/7 network (also titled for the Budapest Convention).

Prosecutors can make requests independently from any LE cooperation channels, for there is no statistics available.

3b. Which are the "top" service providers in terms of numbers of domestic requests for direct cooperation? Please include the names of the "top" 5 service providers.

We are not able to provide any answer for the same reason as explained in the answer to question 3a.

1.2. Practice when the service provider is outside your domestic jurisdiction

4. How do you distinguish between domestic and foreign service providers when making a request?

- [X] Main seat of the service provider in question
- [ ] Place where services are offered
- [ ] Place where data is stored
- [ ] Other criteria

4a. If you selected "Other criteria", please specify:

N/A

5. Do authorities from your Member State make direct requests to service providers in another EU Member State or in third countries?

- (X) Yes, both in EU Member States and third countries
- ( ) Yes, but only in other EU Member States
- ( ) Yes, but only in third countries
- ( ) No, none of the above

5a. If yes, please indicate which third countries (i.e. outside the EU) are most relevant for you in this context

No detailed data are available as this depends on each single Authority handling the request.

6. Does your domestic law address such direct requests from your authorities across borders specifically? Or do you apply the same framework as for domestic requests?

X The same legal framework

( ) Regulated specifically

6a. If regulated specifically, please copy or reference the relevant article(s):

7. Are direct requests sent from your country directly to a service provider in another country considered mandatory or voluntary for the provider to comply with?

( ) Mandatory

X Voluntary

7a. In case they are mandatory, can and do you enforce them, legally and in practice? Could you please explain how?

8. Does your domestic law allow service providers established in your Member State to respond to direct requests from law enforcement authorities from another EU Member Sate or third countries?

( ) Yes, both from EU Member States and third countries

( ) Yes, but only from other EU Member States

( ) Yes, but only from third countries

X No, this is not covered / allowed

8a. Please copy or reference the relevant article(s) providing for the legal basis to allow / prohibit service providers to do so:

the requests are regulated by **Section 132** (Traffic Data Retention for Other Purposes) of Personal data Protection Code (***see attachment***).

9. Do you have a definition (legal or administrative/practical) of different types of data for law enforcement requests? Does your legal framework distinguish between different types of electronic evidence (e.g. subscriber data, traffic data, content data) ?

- ( ) Yes
- (X) No

9a. If yes, please provide us with the definition(s):

10. What kind of data can be requested directly from service providers according to your domestic law / the law applicable to the service provider?

- [X] Subscriber data
- [ ] Traffic data
- [ ] Content data
- [ ] Other data

10a. If you selected "Other data", please explain which type or category of data:

11. Do you limit direct requests to cases with specific (e.g. exigent) circumstances or to specific (e.g. serious) crimes?

- ( ) Yes
- (X) No

11a. If yes, please explain:

What is the typical process in your Member State for making a direct request? Which authority typically initiates a request? Which other authorities are involved in processing the request?

The Public Prosecutors in charge of the proceedings initiate the requests, that are communicated through Police channels.

12. Are these requests made in electronic form (e.g. by e-mail or sent through an online portal)? How are these requests tracked? Is there a central repository of requests that is managed by one single authority?

The requests are made in electronic form, but are not tracked and there is not a central repository.

13. Do any specific agreements on direct requests exist (or are currently being negotiated) between your authorities and foreign service providers?

X Yes

○ No

14a. If yes, could you disclose which service providers your authorities have such an agreement with? How are these agreements established? What is included in these agreements? Could you please explain?

Agreement are made with the most popular social media and content provider from above, such as
facebook
twitter
Ask
Google
Microsoft
skype

limited to subscriber data and IP connections (for Law Enforcement request)

14. For these requests that go beyond your domestic jurisdiction, what is the current practice of your authorities? How many requests are made per year? Which are the "top" service providers in terms of numbers of requests? For these questions, could you please make a distinction between requests within the EU and request outside the EU?

As previously answered, currently there's no standard practices and no statistics available, also considering that in most cases the requests are submitted through (directly) a portal provided by the owning companies.

15. What is the average timeframe to obtain data through direct requests to service providers? Are there any fixed deadlines that you include in your request? Do service providers commit to respect certain deadlines?

No deadline are fixed and no data available regarding the timeframe of the answers.

16. What are the means of transmission of evidence gathered in response to direct request?

- ☐ Paper (letter)
- ☐ Disks (optical or magnetic)
- ☐ Fax
- ☐ Normal email
- X Web portal
- ☐ Secure channel (encrypted email, special ftp, etc.)
- ☐ Other

17a. If you selected "Other", please specify:

17. Is information gathered through direct requests admissible as evidence in court in your Member State?

- X Yes
- ○ No
- ○ It depends on other conditions

18a. If you selected "Yes", could you please provide any article(s) that (either implicitly or explicitly) provide for that? In addition, if addressed by case law, could you please include references to relevant decision(s)?

Law 17 april 2015, n. 43 introduced art. 234 bis of Italian criminal procedural code:

Article 234 bis - Document and computer data acquisition

It is always permitted the acquisition of documents and computer data stored abroad, including those not available to the public, with the consent, in this last case, of the legitimate holder.

18b. If you selected "No" or "It depends on other conditions", please explain:

2. Mutual Legal Assistance

Part 2 of the questionnaire concerns requests for electronic evidence between authorities of a requesting and a receiving state (Mutual Legal Assistance or Mutual Recognition procedures).

19. What is the legal framework in your Member State for Mutual Legal Assistance requests for third countries?

- X **Budapest Cybercrime Convention**
- X **Other multilateral conventions**
- X **Bilateral agreements**

19a. If you selected "Other multilateral conventions", please specify:

As to incoming or outgoing requests with States that have not signed the Budapest Convention, all the multilateral or bilateral conventions on legal assistance signed by Italy are applicable, even in the absence of a specific reference to "electronic evidence", the latter being considered as "documents" and also in consideration of the general duty of contracting parties to "afford each other … the widest measure of mutual assistance" in view of combating the offences object of conventions.

19b. If you selected "Bilateral agreements", please specify with which countries:

See answer 19.a.

20. How many Mutual Legal Assistance requests to third countries for electronic evidence are made by your authorities per year? Which are the "top" third countries that you send requests to (outside the EU)?

Statistical information is not available. In any case, the competent Office (*Directorate General for Criminal Affairs, Office II*) only sent requests to Canada and the US. A search carried out on the period from 1 January 2000 to 11 May 2016 revealed that 263 requests for legal assistance were sent to the US, 140 of which contained requests for acquiring computerized data processed and stored by Providers located on the territory of the United States of America.

21. What is the typical process in your Member State for making a Mutual Legal Assistance request to a third country? Which authority initiates such a request? Which other authorities are involved?

In the absence of a convention, and also when the applicable convention does not provide for direct transmission of the request for assistance by Judicial Authorities, the latter shall be submitted by the Minister of Justice. In this case the request shall be forwarded through the diplomatic channel or through Interpol, Eurojust or Liaison Magistrates, if any.

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?

X **Subscriber data**

X **Traffic data**

X **Content data**

Other data

22a. If you selected "Other data", please explain the type or category of data: **N/A**

23. Could you explain the situation for incoming Mutual Legal Assistance requests from third countries? How many requests are received per year? Which are the "top" countries that you receive requests from? What kinds of data are usually requested? Which authorities are involved when processing such a request?

Statistical information is not available

In the cases, and under the conditions, laid down in Article 15 CoE or Article 53 SIC, requests for legal assistance may directly be addressed to the Court of Appeal of the place where they shall be executed or to the Court of Cassation when the requested activity is supposed to be executed in more than one Court of Appeal district; the Court of Cassation shall identify the competent Court of Appeal, and in doing this account will be taken of the number of measures to be adopted as well as their type and importance with reference to the location of the judicial offices concerned (Article 724 of the Code of Criminal Procedure).

If a direct transmission is not allowed, letters of request shall always be addressed to the Ministry of Justice that gives effect to the proceedings and transmits them – together with the documents enclosed therewith, if any – to the Office of the Prosecutor General attached to the competent Court of Appeal (or to the Court of Cassation for a preliminary identification of the competent Court of Appeal), unless:

1) the requested measures are considered to jeopardise the sovereignty, security or other essential interests of the State;
2) it is evident that the requested measures are expressly prohibited by the law or are contrary to the fundamental principles of the Italian legal system;
3) there are reasons for believing that considerations on grounds of race, religion, sex, nationality, language, political opinions or personal or social conditions may have a negative impact on the course or outcome of the trial and apparently the defendant has not spontaneously given his or her consent to the letter of request;
4) the requesting State does not provide adequate assurances of reciprocity (Article 723 of the Code of Criminal Procedure).

24. What is the average timeframe for obtaining electronic evidence through Mutual Legal Assistance from your main destination countries outside the EU? Are there any fixed deadlines provided for in your agreement with the countries? Are these deadlines usually respected?

See answer 16.

25. When a Mutual Legal Assistance request is refused by a foreign authority, what are the main grounds for refusal (e.g. your main destination country)?

This information is not available. In any case it should be pointed out that the requests for computerized data submitted to the United States of America are mostly rejected because of the type of offence; actually with regard to the offences of defamation or slander, the U.S. refuses assistance in that they are expressions enshrined by the 1 Amendment (except for phrases inciting the accomplishment of acts of violence or that can be connoted as threats).

26. What are the means of transmission of Mutual Legal Assistance requests to other EU Member States (how you send it)?

- **X** Regular mail (letter)
- **X** Fax
- **X** Normal email
- Web portal
- Secure channel (encrypted email, special ftp, etc.)
- **X** Other means

26a. If you selected "Other means", please explain: **DHL**

27. What are the means of transmission of Mutual Legal Assistance requests to third countries (how you send it)?

- **X** Regular mail (letter)
- **X** Fax
- **X** Normal e-mail
- Web portal
- Secure channel (encrypted email, special ftp, etc.)
- **X** Other means

27a. If you selected "Other means", please explain: **DHL**

28. What are the means of transmission of electronic evidence gathered in response to Mutual Legal Assistance requests to other EU Member States (how you receive it)?

- **X** Regular mail (letter)
- **X** Fax
- **X** Normal e-mail
- **X** Disks (optical or magnetic)
- Web portal
- Secure channel (encrypted email, special ftp, etc.)
- **X** Other means

28a. If you selected "Other means", please explain: **DHL**

29. What are the means of transmission of electronic evidence gathered in response to Mutual Legal Assistance requests to other Third Countries (how you receive it)?

- **X** Regular mail (letter)
- **X** Fax
- **X** Normal e-mail
- **X** Disks (optical or magnetic)
- Web portal
- Secure channel (encrypted email, special ftp, etc.)
- **X** Other means

29a. If you selected "Other means", please explain: **DHL**

3. Jurisdiction in cyberspace / other issues

Part 3 of the questionnaire concerns other measures that law enforcement authorities could use to obtain electronic evidence in cases where
a) it is not clear that they would stay within their own jurisdiction, e.g. because it is not possible to determine where evidence is stored, or
b) it is clear that they would operate beyond their jurisdiction without using the measures covered under part 1 and 2 of the questionnaire.

30. Can your law enforcement authorities still access electronic evidence when it is unclear what the location of the electronic evidence is / when it is impossible to establish the location of electronic evidence (e.g. when it may be stored beyond your own jurisdiction)?

- Yes
- No

X It depends on circumstances

30a. If you selected "Yes", or if "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

Law Enforcement can acquire/access the evidence provided that suspects/persons under investigations are granted their personal rights.

31. Can your law enforcement authorities still access electronic evidence when it is impossible to obtain electronic evidence that is stored in another country through direct cooperation with a service provider or a request based on Mutual Legal Assistance or Mutual Recognition (e.g. the service provider refuses to cooperate and there is no legal basis for a Mutual Legal Assistance or Mutual Recognition request)?

- ( ) Yes
- ( ) No
- X It depends on circumstances

31a. If you selected "Yes" or "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

See answer to question 30

32. In the above two situations (see questions 30 and 31), does your domestic law make a distinction between the framework for obtaining access to stored data and the real-time collection of data?

- ( ) Yes
- X No
- ( ) Not applicable

32a. If you selected "Yes", please explain how the difference is framed and how this works out in practice: **N/A**

33. To what extent do your authorities use police-to-police cooperation for obtaining cross-border access to electronic evidence? What is the legal framework for such cooperation and what are current practices (e.g. how often, what data, for which purpose)?

To access electronic evidence, there are several channels of cooperation in addition to Europol and Interpol such as: G7 High Tech Crime 24/7 Network, Requests under the Art. 35 of Budapest Convention (24/7 Network).

34. Is information obtained through police-to-police cooperation admissible as evidence in court in your Member State?

- [x] Yes
- [ ] No
- [ ] It depends on circumstances

34a. If you selected "Not" or "It depends on circumstances", please explain: **N/A**

ATTACHMENT

Section 132 [1] - [2]

(Traffic Data Retention for Other Purposes)

1. Without prejudice to Section 123(2), telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes[3].

1-bis. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days[4].

2. [Repealed][5].

---

[1] As amended by Decree-Law no. 354 of 24th December 2003, converted, with amendments, into Act no. 45 of 26th February 2004; Decree-Law no. 144 of July 27, 2005 converted with amendments into Act no. 155 of July 31, 2005 ("Urgent Measures to Fight Terrorism"), Decree-Law no. 248/2007 converted with amendments into Act no. 31/2008 dated 27 February 2008, Act no. 48 dated 18 March 2008 ratifying the Council of Europe's Convention on Cybercrime of 23 November 2001, and Presidential Decree no. 109 dated 30 May 2008 (implementing directive 2006/24/EC).

An excerpt of the relevant provisions contained in the decree-law no. 144/2005 is reported here for the sake of completeness, as subsequently amended by decree no. 248 dated 31 December 2007 converted with amendments into Act no. 31/2008 dated 27 February 2008:

"Article 6. (*New Provisions on Telephone and Internet Traffic Data*) (1) As of the date of entry into force of this decree [August 2, 2005] until entry into force of the legislative instrument implementing directive 2006/24/EC of the European Parliament and the Council, of 15 March 2006, and in any case until no later than 31 December 2008, application of laws, regulations and/or administrative measures providing and/or allowing for erasure of telephone and/or electronic communications traffic data shall be suspended, regardless of whether the said data are needed for billing purposes; the data in question shall have to be retained by providers of publicly available communications networks and/or electronic communications services until entry into force of the legislative instrument implementing directive 2006/24/EC of the European Parliament and the Council, of 15 March 2006, and in any case until no later than 31 December 2008, except for the contents of the communications and by having regard to the information allowing accesses and – where available – services to be tracked, whereby any provisions in force envisaging longer retention periods shall have to be left unprejudiced. Any traffic data that is retained beyond the period set out in Section 132 of legislative decree no. 196/2003 may only be used for the purposes set out herein, subject to prosecution of offences that are prosecutable in any case.
(…)

Article 7. (*Provisions Supplementing the Administrative Measures on Public Establishments Offering Telephone and Internet Access Points*). (1). As of the fifteenth day following the date of entry into force of this decree [August 2, 2005] until December 31, 2008, whoever plans to open up a public establishment and/or a private club of whatever kind whose activity consists, either exclusively or predominantly, in making available terminal equipment to the public, customers and/or members, whereby the said equipment may be used for electronic or other communications, or where over three pieces of such equipment are installed, shall have to apply to the competent *questore* [Head of provincial police office] for a licence. No licence shall be required if only public payphones are installed allowing exclusively voice calls to be made. (2) As regards the entities already carrying out the activities referred to in paragraph 1, the licence shall have to be applied for within sixty days as of the date of entry into force of this decree."

[2] As for the retention of telephone and Internet traffic data, reference should also be made to Section 4a of legislative decree No. 7 of 18 February 2015 as enacted, including amendments thereof, by Law No. 43 of 17 April 2015 and subsequently amended by decree No. 210 of 30 December 2015 as enacted, including amendments thereof, by Law No. 21 of 25 February 2016.

The text of the said Section is reported below:

'Section 4a. Provisions on the Retention of Telephone and Internet Traffic Data. – 1. By way of derogation from the provisions made in Section 132(1) of the Code referred to in legislative decree No. 196 of 30 June 2003 as amended thereafter, the telephone and Internet traffic data – except for the contents of communications – that are held by telecommunication service operators as of the date of entry into force of the Law enacting this decree along with the data of telephone and Internet traffic occurring thereafter shall be retained until 30 June 2017 for the purposes of detection and suppression of the criminal offences mentioned in Sections 51(3c) and 407(2), letter a), of the Criminal Procedure Code. – 2. The data relating to the unsuccessful calls made as from the date of entry into force of the Law enacting this decree, which are processed on a temporary basis by the providers of publicly available electronic communications services or public communication networks, shall be retained until 30 June 2017. – 3. The provisions under paragraphs 1 and 2 above shall no longer apply as from 1 July 2017.'

[3] This paragraph was amended firstly by Section 6(3) of decree no. 144/2005, and thereafter by Section 2 of legislative decree no. 109/2008.
[4] This paragraph was added by Section 2 of legislative decree no. 109/2008 and entered into force as per the time schedule set forth in Section 6(3) thereof.

[5] This paragraph was repealed by Section 2(1)c. of legislative decree no. 109/2008 along with paragraph 4 and paragraph 4-bis hereof.

3. Within the term referred to in paragraph 1, the data may be acquired from the provider by means of a reasoned order issued by the public prosecutor also at the request of defence counsel, the person under investigation, the injured party, or any other private party. Defence counsel for either the defendant or the person under investigation may directly request the provider to make available the data relating to the subscriptions entered into by his/her client according to the arrangements specified in Section 391-quater of the Criminal Procedure Code without prejudice to the requirements set out in Section 8(2), letter f), with regard to incoming phone calls.

4. [Repealed.]

4-bis. [Repealed.]

4-ter. The Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, also in connection with requests lodged by foreign investigating authorities, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties[6].

4-quater. Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence.

4-quinquies. The measures taken under paragraph 4-ter above shall be notified in writing without delay, in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.

[6] This paragraph was added by Section 10 of Act no. 48 dated 10 March 2008 along with paragraph 4-quater and 4-quinquies hereof.

5[7]**.** Data processing for the purposes referred to in paragraph 1 shall be carried out by complying with the measures and precautions to safeguard data subjects as required under Section 17, which are aimed at ensuring that the retained data fulfil the same quality, security and protection requirements as network data as well as at:

a. providing in all cases for specific systems allowing both computer-based authentication and authorisation of persons in charge of the processing as per Annex B, and

b. [Repealed][8].

c. [Repealed].

d. laying down technical mechanisms to regularly destroy the data after expiry of the term referred to in paragraph 1[9].

[7] This paragraph was amended by Section 2(1)d. of legislative decree no. 109/2008.

[8] This letter was repealed by Section 2(1)d. of legislative decree no. 109/2008 along with letter c. hereof.

[9] This letter was amended by Section 2(1)d., point 3, of legislative decree no. 109/2008.