Brussels, 28 November 2014

Mr Alexander Seger
Data Protection and Cybercrime Division
DG of Human Rights and Rule of Law
Council of Europe
F-67075 Strasbourg CEDEX

By E-mail: Alexander.SEGER@coe.int

Dear members of the Cybercrime Convention Committee,

During the 2014 Cybercrime@Octopus Conference, several scenarios have been presented in relation to transborder access to personal data.[1] The scenarios were intended to stimulate a discussion on the consequences of data protection legislation and principles when obtaining such data in a criminal investigation. At the time, given the complexity of the issues raised by these scenarios, it was decided that the participating representatives of the European Union's Article 29 data protection working party (WP29) and the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) would provide written comments rather than on-the-spot reactions. In view of the plenary session that the T-CY will hold on 2 and 3 December 2014 and considering that transborder access to data will be one of the topics for discussion, we would like to share with you a first assessment of the data protection implications of the various scenarios. If need be, a more in depth analysis of the scenarios could follow.

We identified three main situations with different data protection implications:

1. The general principle: the transfer of personal data takes place between law enforcement authorities in application of national criminal law procedures and bilateral or multilateral treaties on cooperation in criminal matters.

In this context, activities of law enforcement authorities in the European Union should comply with the principles laid down in Article 8 of the European Convention on Human

[1] The scenarios are available at http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/cyber_COE_TB_Scenarios_june2014%20V5web.pdf

Rights[2] (ECHR) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[3] (hereafter: Convention 108). According to Article 9 of the latter, "derogations from the provisions of Articles 5, 6, and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of : […] the suppression of criminal offences". However, these derogations should remain exceptional. Besides, as considered by the European Court of Human Rights in its case law on the interpretation of the exemptions contained in the European Convention on Human Rights, the exemptions contained in the Convention should be interpreted restrictively. In addition, law enforcement authorities of EU Member States have to respect Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Articles 7, 8 and 52(1) of the Charter of Fundamental Rights. As a result of the aforementioned legal framework, before they access or transmit personal data, law enforcement authorities have to make sure that the interference in the right of EU residents to the protection of their personal data is necessary and proportionate, corresponds to the purpose pursued and that the powers exercised by the law enforcement authorities of both Parties are explicitly laid down by law. Compliance with these rules should also be subject to the control of an independent authority.

Amongst other, these requirements were reflected on the EU level concerning law enforcement activities by the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union and and by the 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. Data protection authorities also reflected on this issue at the Spring Conference 2010 of the European Data Protection Commissioners and agreed upon data protection model clause(s) in bilateral agreements in the law enforcement area[4]. Besides, the Recommendation No. R(87) 15 of the Committee of Ministers to Member States regulates the use of personal data in the police sector at Council of Europe level.

Building on these documents, law enforcement authorities exchanging personal data in a criminal/cybercrime cooperation context should comply with the following requirements:

The transmitting Party should check:

- that the data processing is lawful, i.e. compliant with national legislation and, if relevant, international agreements,

- that the request is made for specified, explicit and legitimate purposes and that the data will be processed only for the purpose mentioned in the cooperation agreement (fight against cybercrime in this case),

[2] Convention for the Protection of Human Rights and Fundamental Freedoms – Rome, 4 November 1950
[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Strasbourg, 28 January 1981 – ETS No. 108
[4] Bilateral agreements data protection model clause(s) in the law enforcement area adopted at the Spring Conference 2010 of the European Data Protection Commissioners
http://194.242.234.211/documents/10160/10704/1799288

- that only data that is accurate, complete and updated, as well as adequate, relevant and not excessive in relation to this purpose is transmitted,
- that any further processing for a different purpose, transmission to another authority, agency or body, is authorized by the sending State and subject to strict conditions (see page 1 as regards conditions for derogations from data protection principles),
- that the data will not be retained longer than necessary for the purpose pursued,
- that transmissions and receptions of personal data are logged or documented,
- that security of the data processing is ensured,
- and finally, that an independent supervisory authority[5] is responsible for checking that these requirements were respected in both the transmitting and the receiving Party.

In this regard, we note that many delegations insisted during the Cybercrime@Octopus Conference that the mutual legal assistance procedures in practice do not always function in a satisfactory way. However, these dysfunctional practices do not justify the circumvention of applicable rules but rather call for their recast and improvement.

We consider that criminal justice treaties must be compliant with fundamental rights and, therefore, with data protection requirements. Considering that most of these treaties do not seem to already include data protection requirements, we also recall our availability to help advise European Governments improving or inserting data protection clauses in mutual legal assistance agreements to ensure that minimum data protection safeguards are complied with when exchanging personal data between law enforcement authorities.

2. The exception to the abovementioned principle, i.e. the direct transfer of data from a private entity/or natural person to the law enforcement authority of a third country in exceptional circumstances and where provided for by law of the Searched State or applicable cooperation agreements:

In situations of particular urgency and life or death questions and **only in cases where it is provided for by the national legislation of the searched State or in applicable mutual legal assistance agreements**, direct transfer of data from the private entity or the natural person to the law enforcement authority of a third country could be exceptionally envisaged. In any case, the competent authority of the searched State should be notified as soon as possible.

In such case where a direct transfer of data from the private entity or the natural person to the law enforcement authority of a third country is allowed by the national legislation of the searched State or by the bilateral agreement concluded between the searching State and the

[5] In most of the cases, a judicial authority.

searched State, we recall that the following applies: when data are initially collected and stored for purposes covered by Directive 95/46/EC, then this Directive is to be considered applicable to the transfer of personal data taking place from a private sector entity subject to EU data protection legislation to the law enforcement authority of a third country. Therefore, the principles laid down in Articles 25 and 26 of Directive 95/46/EC apply together with the principles laid down in Article 6 of the Directive: in other words, the transfer is prohibited unless an adequate level of protection of personal data is afforded in the searching State. If the level of protection of personal data is not adequate, Article 26(e) allows for the transfer of personal data in case it would be necessary for the protection of vital interests of the data subject provided that data protection principles laid down in Article 6 are respected.

Also with regard to the Parties to the Convention 108 the situation is similar. The Convention is applicable to the processing of personal data in the private and in the public sector, including police and justice. Transfers of data between Parties cannot, in principle, be prohibited on data protection grounds. Exceptions to this rule include cases where the law of the Party from which the transfer takes place requires an equivalent protection. Concerning the transfers to third countries, the additional protocol to Convention 108 regarding supervisory authorities and transborder data flows[6] foresees that each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a state or organisation that is not Party to the Convention only if that state or organisation ensures an adequate level of protection for the intended data transfer (art. 2.1). In absence of an adequate level, the transfer is possible under the similar condition as for EU members (art. 2.2). In addition, in the field of police, the aforementioned Recommendation No. R(87) 15 is to be considered part of the standard level of data protection to be ensured since its principles were made binding by reference to them in some EU instruments of cooperation such as the 1990 Schengen[7] and Europol[8] Conventions and Council Framework Decision 2006/960/JHA of 18 December 2006.

3. <u>The hypothesis where the data controller[9] cannot be located and it cannot be deduced which data protection regime would be applicable:</u>

The data protection principles cannot be ignored simply on the premise that the identity or jurisdiction of the data controller is unclear or unknown. Fundamental rights in Europe need

[6] Strasbourg, 8.XI.2001

[7] See Articles 115 and 129 of the Convention of 19 june 1990 applying the Schengen agreement of 14 june 1985 between the governments of the States of Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the gradual abolition of checks at their common borders

[8] See Article 14 of Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)

[9] The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (For further details, see Article 2 of Directive 95/46/EC).

to be respected. Therefore, in these situations, it needs to be assumed that the data could be processed in any of the other Parties' jurisdiction and thus, it is our view that it would be the most appropriate solution if the searching Party respects the conditions of the Party that has set the highest data protection standards to ensure that the data protection law of the searched Party is not violated. In this respect, it would be advisable if all States Party to the Budapest Convention would also ratify Convention 108 and its additional Protocol and transpose its principles into their national law. To the extent that countries are already Party to Convention 108, they should ensure its provisions are respected. We also advise that these principles are translated in cooperation agreements in criminal matters as aforementioned under point 1.

In any case, we advise that, as soon as the data controller is identified, the procedural rules described under point 1 are respected *a posteriori* and that the competent counterpart authority is informed of the access made to data.

As a general remark, we insist that in order for consent to serve as a valid legal basis to process (access/collect) personal data, it should be freely given, specific and informed[10]. Consequently, in a law enforcement context, it is very unlikely that such data processing can be legitimized on the basis of the consent of the data subject[11]. Such consent should be distinguished from the "consent" or authorisation given by the competent law enforcement authority to the transmission of the data to its counterpart in a third country.

We trust that this letter will provide you a better understanding of the implications of the data protection legislation on trans-border access to personal data. Naturally, we are willing to further discuss these issues should any questions on your side remain.

Sincerely yours,

Yours sincerely,

Isabelle Falque-Pierrotin
Chairwoman WP29

Jean-Philippe Walter
Chairman T-PD

[10] For further information on this issue, see Article 29 Data Protection Working Party Opinion 15/2011 (01197/11/EN WP187) on the definition of consent, adopted on 13 July 2011 and in particular developments on what should be understood by a consent that is "freely given" on pages 12 and 13

[11] The data subject is the identified or identifiable natural person to which the personal data processed relates.