Brussels, 5 December 2013

Jean-Philippe Walter
President of the Committee of the Convention 108 (T-PD)
Feldeggweg 1, CH-3003 Berne
Switzerland

Subject: Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime

Dear Mr Walter,

Following the hearing of private sector and civil society stakeholders on transborder access to data that was held by the Cybercrime Convention Committee (T-CY) at the Council of Europe on 3 June 2013, the Article 29 Working Party[1] decided to address, in the present letter, the issues that were submitted to the participants. More precisely, you will find below the Article 29 Working Party's comments on the draft elements for an additional protocol to the Budapest Convention on Cybercrime (hereinafter: "the draft elements").

1. *Current Article 32 of the Budapest Convention on Cybercrime*

The current Article 32 of the Budapest Convention on Cybercrime, relating to Transborder access to stored computer data with consent or where publicly available, reads as follows:

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

According to current Article 32(b), the precondition for direct access by the "searching Party" (i.e. the Party looking for the data for law enforcement purposes) to data stored in another Party (i.e. the "requested Party") is to obtain the "lawful and voluntary consent of the person

[1] Article 29 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31) sets up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The "Article 29 Working Party" has advisory status and acts independently. The Article 29 Data Protection Working Party is composed of:
- a representative of the data protection supervisory authority (ies) designated by each EU Member State;
- a representative of the data protection authority (ies) established for the EU institutions and bodies;
- a representative of the European Commission.

who has the lawful authority to disclose the data". The implementation of the said article therefore depends on what is the "lawful and voluntary consent of the person who has the lawful authority to disclose the data" according to the national law of the requested Party.

This follows current practice in international agreements and Treaties in the field of law enforcement, where, according to the national sovereignty principle, mutual legal assistance is granted on the basis of the national legal requirements of the requested Party.

The EU data protection legislation is therefore the benchmark for the interpretation and implementation of this article by EU Member States into national law. This interpretation will be explained in point 2.

Besides, in April 2010, the Spring Conference of European Privacy and Data Protection Authorities, as to the implementation of the Council of Europe's Convention on Cybercrime[2], invited EU Member States ratifying the Convention to include, in the national implementing measures, judicial review mechanisms in respect of the handling of the information collected by law enforcement authorities pursuant to the Convention. In this regard, the Working Party on Police and Justice (WPPJ) – set up by the Spring Conference of European Privacy and Data Protection Authorities to monitor the developments in the law enforcement area - also prepared a data protection model clause(s) for bilateral agreements in the law enforcement area[3].

2. *Issues relevant for the application of Article 32b Cybercrime Convention and the "draft elements" of a possible Additional Protocol*

The Article 29 Working Party wishes to present below the interpretation of issues addressed in Article 32b according to EU data protection legislation.

a. "Consent" and whether a private entity could lawfully provide access to or disclose the data

According to the EU data protection *acquis*, there are two types of consent:

- the data subject's consent means "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*[4]". The Article 29 Working Party elaborated an Opinion in July

[2] Recommendation adopted by the Spring conference of European privacy and data protection authorities on implementation of Council of Europe's convention on cybercrime (ETS 185/2001) Prague, 29 and 30 April 2010

[3] The part on transfer of data to public authorities of a third country reads as follows: "Onward transfers of personal data to other Authorities and public bodies of a Third Country for the purposes mentioned in this Agreement shall only be permitted in compliance with the national legislation and with the prior consent of the Contracting Party which transmitted the data. If the transfer of the data is essential for the prevention of an immediate and serious threat to public security or to essential interests of the receiving Contracting Party and consent cannot be obtained in time, the transfer can occur without prior consent, on a case by case basis, subject to further safeguards. The transmitting Country must be informed without delay."

[4] Article 2(h) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31) (hereafter "Directive 95/46/EC").

2011 explaining the definition of consent (WP 187[5]). One of the requirements for the consent to be given is that it has to be "*freely given*"; this criterion is only fulfilled "*in the absence of negative consequences*". In particular, the Working Party notes that *"[c]onsent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent*[6]";

- in a law enforcement context, however, "consent" is also understood to be the consent of law enforcement/judicial authorities that need, in relation to a specific case, to exchange data[7].
- Data controllers in the EU, i.e. 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, have responsibilities and obligations related to the processing they undertake under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter "Directive 95/46/EC"). According to this Directive, consent can only be given by data subjects. Therefore, companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process for e.g. commercial purposes according to the EU data protection *acquis*[8]. They can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required[9]. Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view.

b. <u>the type of data that can be disclosed by a private sector entity</u>

As derives from the explanations above, the private sector entity which processes the data would, under data protection principles, be called a controller if it determines the purposes

[5] Article 29 Working Party Opinion 15/2011 adopted on 13 July 2011 (WP 187), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[6] Article 29 Working Party Opinion 15/2011 (WP 187), p. 12.

[7] See in particular Article 11 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: "*prior consent of the transmitting Member State*".

[8] See in particular Article 25 and Article 26 Directive 95/46/EC for transfers to third countries.

[9] Article 7(e) of Directive 95/46/EC allows data processing carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. However, the concept of "public interest" has to be read in the light of the ECtHR's case law and, in particular of the principles of necessity and proportionality. The obligation of compliance with these principles requires the data controller to ask the official authority to prove the necessity of the data disclosure, i.e. to prove that it is acting in the framework of a specific investigation and, if carrying out intelligence activities, to disclose the legal basis on which the data is requested. The burden of proof of necessity and proportionality of the requested access to data lies with the requesting "party"'s official authority. Article 7(e) should also be combined with Article 17 of Directive 95/46/EC which requires the data controller to implement organizational measures to protect personal data against unauthorized disclosure or access, and thus implies that he should ensure that the data is necessary for an investigation and, at the very least, that he discloses it on a "need to know" basis.

and means of the processing of personal data. It would on the contrary be considered as a processor if it processes personal data on behalf of the controller (when e.g. the controller outsources the storing of its consumers' personal data in a cloud managed by another entity).

Amongst these private sector entities, only the controller can disclose personal data relating to a data subject to a law enforcement authority upon prior presentation of a domestic judicial authorisation/warrant or any document justifying their need to access the data.

From an EU data protection point of view, information that would not relate to an identified or identifiable natural person (for instance anonymised statistics), can be disclosed by a private sector entity without any specific safeguards. Personal data however, i.e. any information relating to a directly or indirectly identified or identifiable natural person (name, last name, picture, fingerprint, IP address, social security number, geolocation data etc.) cannot be disclosed by a private sector entity unless the EU data protection rules are respected[10].

Personal data should therefore only be disclosed if necessary and proportionate to the purpose pursued, i.e. upon prior presentation of a judicial authorisation/warrant or any document justifying their need to access the data according to the requested Party's law. For instance, a company that exploits CCTV in its premises will only be able to disclose extracts of the recordings relating to the specific period of time into which the law enforcement authority needs to look. The disclosure of the whole recording would not be considered as proportionate if the law enforcement authority is investigating an offence committed on a specific day and at a specific time.

The application of the requested Party's national law means that the requirements that need to be respected for national investigations will also need to be respected for cross-border investigations, and is therefore a guarantee for individuals' rights.

3. The issue of direct access to data and the applicable law

It seems that all five "draft elements" seek to legitimise the direct access by law enforcement authorities in one jurisdiction to data stored in another jurisdiction in the absence of a formal legal channel of cooperation, such as Mutual Legal Assistance Treaties/agreements.

Direct access to personal data by law enforcement authorities of third countries is not compatible with the data controllers' obligations according to Directive 95/46/EC.

Such requests may also call into question more general fundamental rights issues relating to e.g. due criminal process and criminal procedural guarantees.

The articulation with the EU *acquis* and the EU Charter of Fundamental Rights is a precondition for the elaboration of any international instrument to which EU Member States participate.

This articulation raises several problems, in particular with respect to:

[10] Directive 95/46/EC applies to companies acting as data controllers.

- the interpretation of the notion of “consent”, as outlined above[11];
- the option according to which the "law of the searching party" should apply; according to this option, instead of applying the law of the requested party's jurisdiction[12], the law of the searching law enforcement authority's jurisdiction would apply:
    - the issues arising from such an interpretation have been made apparent recently against the background of the revelations of intelligence programmes collecting data on a large-scale, including data of non-citizens abroad[13];
    - the "law of the searching party" means that stricter legislation applicable in the jurisdiction where the data (and potentially also the data subject) is, such as e.g. the data protection rules in the EU, could be circumvented.

The EU data protection legislation ensures continuity of protection when EU data is transferred abroad. These safeguards for data processed in the EU cannot be circumvented by applying third countries' legislation to EU processed data.

4. The legal framework surrounding the Budapest Convention on Cybercrime and the "draft elements" for an additional protocol to the Budapest Convention on Cybercrime

The ad-hoc subgroup of the T-CY on jurisdiction and transborder access to data and data flows, established in November 2011 by the T-CY (hereinafter, the "Transborder Group"), put forward some draft elements of a Protocol to the Budapest Convention on Cybercrime to allow for additional possibilities for transborder access to data[14]. These options were presented as follows:

- Proposal 1: Transborder access with consent without the limitation to data stored "in another Party".
- Proposal 2: Transborder access without consent but with lawfully obtained credentials.
- Proposal 3: Transborder access without consent in good faith or in exigent or other circumstances.
- Proposal 4: Extending the search without the limitation "in its territory" in Article 19.3 of the Budapest Convention on Cybercrime.
- Proposal 5: The power of disposal as connecting legal factor.

[11] See 2 (a).

[12] According to Article 4(1)(a) of Directive 95/46/EC, "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State...". Consequently, regardless of where the data is located, the law applicable to the situation here described is the national law implementing Directive 95/46/EC in the Member State where the controller has an establishment, in other words, the law of the data controller's jurisdiction.

[13] The Article 29 Working Party understands cybercrime is very often considered to be an issue of national security in some countries' legal frameworks.

[14] See (Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data, Proposal prepared by the Ad-hoc Subgroup on Transborder Access, T-CY (2013)14, Strasbourg, version of 9 April 2013

The Article 29 Working Party understands and is reassured that the draft elements are simply proposals and not yet complete proposals for modification of the Budapest Convention but still wishes to raise very concrete concerns since, already at this stage, they raise important issues of compatibility with the binding EU *acquis* on data protection.

As a preliminary remark, the Article 29 Working Party recognises the growing importance of cloud computing along with the subsequent difficulty to link data to a specific location. In this regard, it refers to its opinion on Cloud computing issued in 2012[15] where it stressed the lack of control and the lack of transparency inherent to cloud computing data processing together with the specific data protection risks that have to be addressed.

It also recalls that the processing of data for law enforcement purposes is legitimate provided it complies with applicable data protection legislation requirements[16].

Therefore, the Article 29 Working Party wishes to express, in the present letter, its concerns regarding the aforementioned 5 Proposals.

It firstly notes that the draft elements do not take account of the data protection requirements – of either the EU legal framework nor of CoE Convention 108 – *vis-a-vis* the different options proposed. Therefore, the Article 29 Working Party recalls that extensive data protection rules apply to international data transfers when data is within the jurisdiction of a Member State of the Council of Europe and, even more specifically, if the data is within the jurisdiction of a Member State of the European Union.

From the point of view of the Council of Europe, the right to protection of one's personal data is enshrined in the case law of the European Court of Human Rights interpreting the scope of Article 8 of the European Convention on Human Rights, as well as the provisions of Convention 108 on the right to protection of personal data and Recommendation No. R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector.

From the point of view of the European Union, this right is enshrined in Article 7 and - more specifically - in Article 8 of the Charter of Fundamental Rights. Transfers of data to law enforcement authorities should comply with the requirements presented in Directive 95/46/EC if access is directly made to data held by a private entity. If data is transferred by law enforcement authorities to law enforcement authorities, the provisions of 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 (hereafter " Framework Decision 2008/977/JHA"), including Article 13 on data transfers to competent authorities in third States or to international bodies apply.

---

[15] Opinion 05/2012 on Cloud Computing (143 kB) - WP 196 (01.07.2012)

[16] Cf. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350 , 30/12/2008, pp. 60–71.

The Article 29 Working Party, bringing together representatives national and European data protection authorities, draws attention to the fact that all five draft proposals appear to allow transborder access by law enforcement authorities of one Party - be it a Member State, Party to Convention 108 and the Cybercrime Convention, or only Party to the Cybercrime Convention - to data within the jurisdiction of another party in breach of key principles of data protection.

This would include, *inter alia*, the principles of necessity and proportionality, which contribute to the respect of the rule of law in a democratic society, as well as the principle of purpose limitation, which is a cornerstone principle of data protection. Given the fact that both Convention 108 and Convention 185 are international Conventions, it furthermore means that, in the event of an incompatibility with the European Convention of Human Rights, only European states would be subject to the jurisdiction of the European Court of Human Rights, which would not allow for full compliance by non-European States.

5. *"Draft elements" for an additional protocol to the Budapest Convention on Cybercrime*

With regard to the specifically drafted elements aimed at facilitating transborder access through an Additional Protocol to the Budapest Convention, the Article 29 Working Party's position is the following:

a. The option of "transborder access with consent but without the limitation to data stored 'in another Party'"

The Article 29 Working Party understands that this option is supposed to cover situations where consent is given under conditions similar to those of Article 32b but where it is unclear in which jurisdiction the data are located or where data are moving.

The Article 29 Working Party believes that uncertainty with respect to location does not allow for contravening the binding rules that are applicable with respect to fundamental rights' protection in the Member States and to ignore their jurisdiction[17].

Should, indeed, the controller's establishment be in another jurisdiction, and the data need to be transferred from a law enforcement authority located in an EU Member State to a third party, Article 13 of aforementioned Council Framework decision would apply laying down the conditions for such transfer[18].

For these safeguards to apply, it is necessary that the jurisdiction of the relevant Member State is respected. The solution proposed under this alternative would lead to ignoring this national jurisdiction together with the principle of national sovereignty.

b. The option of transborder access without consent but with lawfully obtained credentials

[17] See footnote 14 for specifications of data protection rules governing jurisdiction.

[18] Article 13 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

The Article 29 Working Party understands from the supporting documents that "lawfully obtained credentials" would mean credentials obtained by lawful investigative activities by either the searching or the requested Party.

The legal nature of the "lawfully obtained credentials" is not clarified, but remains a vague concept that would contribute to legal uncertainty. This is in particular relevant against the background of the possibility to apply the searching Party's domestic law, which raises issues of compatibility with the EU data protection *acquis*[19].

In particular, what can be considered as "lawfully obtained credentials" differs greatly according to whether the searching Party is bound by the provisions of the 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, the rules of Convention 108 or none of the above. Since there are no binding harmonised rules among EU Member States and Parties of either the Convention 185 or the Convention 108 in this respect, an automatic application of the "lawfully obtained credentials" of one Party that would like to have access to data stored in another Party's jurisdiction is excluded.

c. <u>the option of transborder access without consent "in good faith or in exigent or other circumstances"</u>

The Article 29 Working Party refers to the previous concerns regarding the possibility of unilateral application of the searching Party's law and insists that good faith or exigent or other circumstances would not be sufficient to justify transborder access to data. The Article 29 Working Party considers that the concepts are vague, that there is no clear definition of "good faith" and "exigent or other circumstances" and that, additionally, these concepts do not guarantee that the key principles of necessity and proportionality - as well as of the prerequisite of the well-established jurisprudence of the European Court of Human Rights for restrictions to fundamental rights to be strictly necessary in a democratic society - are taken into account.

Furthermore, the differences in data protection legislation between Parties raise issues of compliance with the requested Party's national legislation: since the searching Party may or may not be bound by the provisions of the 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 or the Convention 108 and national laws differ to a significant extent, access cannot be *a priori* granted by an automatic application of what one Party would perceive as "good faith" or "exigent circumstances" because the interpretation of such concepts may vary in different legal frameworks. Even the inclusion of safeguards (which will by definition be very general given the nature of a Convention as an international legal instrument[20]) is not sufficient to cover these significant gaps in interpretation of abstract legal terms and applicable binding rules.

[19] See below, part 3.
[20] This is true for both the Cybercrime Convention as well as the Convention 108.

d. the option of extending a search "from the original computer to connected systems without the limitation 'in its territory'" (Article 19.3 Budapest Convention)

The Article 29 Working Party draws the attention to the fact that this would enable a law enforcement authority with access to a specific computer system to access data stored in another computer system even if the latter is not within the jurisdiction of the requested Party, provided the data is lawfully accessible from or available to the initial system and located in a Party or in an unknown location.

The Article 29 Working Party recalls that such an access would breach the principle of territoriality and sovereign jurisdiction of the requested Party (the Party on whose territory or within whose jurisdiction the data is located). To the extent that the searching Party does not recognise personal data as a fundamental right, such a provision could call into question the applicability of the rights guaranteed in the EU Charter of Fundamental Rights and the European Convention of Human Rights.

Furthermore and in addition to the lack of clarity regarding the compliance with the aforementioned data protection requirements, this option seems to run contrary to the current prerequisite for the application of Article 32b Cybercrime Convention, namely the need to obtain the "lawful and voluntary consent of the person who has the lawful authority to disclose the data".

e. the power of disposal as connecting legal factor

The Article 29 Working Party notes that this proposal would run contrary to the principle of territoriality.

According to this option, it is envisaged that, even if the location of data cannot be clearly determined, it would be sufficient for data to be linked to a person having the "power of disposal[21]" and that person is physically on the territory of, or a national of the searching Party, for the law enforcement authority of this Party to be able to search or otherwise access the data.

However, pursuant to European Union data protection legislation, whether a person is physically on the territory of, or a national of the searching Party, is not a relevant criterion to restrict his/her fundamental right to data protection. The most relevant criterion of EU data protection *acquis*, including Directive 95/46/EC and Framework Decision 2008/977/JHA[22], is whether data is processed in the context of the activities of an establishment of the controller in the EU or by a law enforcement body in the EU. The aforementioned criteria are therefore not sufficient to allow the law enforcement authority of the searching Party to access the data.

[21] Power to "alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever." (see page 6 of the above-mentioned draft elements)

[22] Article 3 Directive 95/46/EC defines the territorial scope as follows: "*This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*"; cf. Article 1 paragraph 3Council Framework Decision 2008/977/JHA: "*This Framework Decision shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system*".

6. *Conclusion: Ensuring the continuity of protection of data transferred outside the EU*

The EU data protection legislation ensures continuity of protection - in principle by requiring either an adequate level of protection or adequate safeguards - when EU data is transferred abroad. These safeguards for data processed in the EU cannot be circumvented by applying third countries' legislation to EU processed data.

Against this background, the Article 29 Working Party would like to draw the attention to the risks involved in a potential Additional Protocol that would legitimise a direct access to data by law enforcement authorities of a Party to data stored within the jurisdiction of another Party. The Article 29 Working Party stresses that the application of such a principle, independently of the way in which it is implemented (e.g. by applying the law or the definitions of consent of the searching Party) would infringe upon key data protection rules and have an adverse impact on individuals' fundamental rights.

It is imperative that data transfers have a specific and legitimate legal basis in the law of the requested Party (e.g. judicial authorisation/warrant), that the principles of necessity and proportionality are respected and that no large-scale access to personal data is permitted. An additional protocol to an international Convention that would appear to provide for access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party would be in violation of the EU data protection *acquis*.

These conclusions are particularly pertinent in the light of the revelations of mass surveillance programmes. The Article 29 Working Party would like to insist that transborder data transfers in the field of law enforcement must exclude blanket/mass transborder access, collection or transfer to/of data, which is incompatible with the EU Charter of Fundamental Rights and the European Convention of Human Rights.

Last but not least, the Article 29 Working Party would kindly ask you to promptly forward this letter to all interested stakeholders, including the Council of Europe's Committee of Ministers, the T-CY Committee and the T-PD Committee.

Jacob Kohnstamm
Chairman

A letter in identical terms is being forwarded to Ms Kwasny and Mr Seger.

c.c. Mrs Viviane Reding, Vice-President of the European Commission
Mr Juan Fernando López Aguilar,
Chairman of the LIBE Committee of the European Parliament