CBPL-CPVP-15018237

CPP
Commission for the protection of privacy

Please contact: Priscilla de Locht
T: +32 2 274.48.59
F: +32 (0)2 213 85 65
E-mail: Priscilla.deLocht@privacycommission.be

The International Conference of Data Protection & Privacy Commissioners
To the attention of The Secretariat
Office of the Privacy Commissioner
PO Box 10-094, The Terrace
WELLINGTON
NEW ZEALAND

Your reference	Our reference	Enclosure(s)	Date
	AH-2015-0097/010/SA2/pdl	1	

Re: Global Cross Border Enforcement Cooperation Arrangement

15 -07- 2015

Dear Sir,
Dear Madam,

I am writing in regard to the Global Cross Border Enforcement Cooperation Arrangement referred to in the Resolution on enforcement cooperation adopted in October 2014 at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Mauritius.

At the conference, the Belgian Data Protection Authority stressed that the Arrangement raises legal issues and expressed doubts about its practical implementation. Please find attached the written contribution of Mr Vermeulen (Belgian Commissioner), which elaborates the Belgian reservations about the Arrangement. We would highly appreciate the circulation of this note to the ICDPPC for discussion at the next conference in October 2015.

We remain of course available for any question you might have as regards the attached note.

Yours sincerely,

Willem Debeuckelaere
President

Quis custodiet ipsos custodes?
Critical notes on the Global Cross-Border Enforcement Cooperation Arrangement [version 16]

Gert Vermeulen
Privacy Commissioner at Belgian DPA
Full Professor International and European Criminal Law, Director Institute for International Research on Criminal Policy (IRCP), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University
Extraordinary Professor of Evidence Law, Faculty of Law, Maastricht University

---

1. Fuzzy scope

a. *Ratione personae* | privacy enforcement authorities

The scope of the Arrangement *ratione personae* is limited to 'privacy enforcement authorities' (PEA's). Such PEA is defined (under Section 1: 'Definitions') as "any public body that has as one of its responsibilities the enforcement of a privacy and/or data protection law, and that has powers to conduct investigations or take enforcement action". In a footnote, both in the preamble and under Section 1 ('Definitions'), it is further clarified that whichever DPA qualifies as a PEA.

There are several problems with this definition and consequently with the demarcation *ratione personae* of the Arrangement:

- a body may qualify as a PEA even if having no power to take enforcement action itself, as long as it has the power to conduct investigations; this is reinforced by the addition that whichever DPA (irrespective of its nature and competencies) qualifies as a PEA

- no purpose distinction whatsoever is being made between administrative, civil or penal investigation/enforcement powers, which constitutes a flagrant denial of the purpose limitation principle

- moreover, a possible cross-over between the various abovementioned spheres (by information sharing and exchange as promoted by the Arrangement) raises serious concerns, especially as regards:

    - the impact on suspects' procedural rights: the non-granting of procedural rights proper that normally accrue to suspects or defendants in criminal matters in the requesting jurisdiction may easily prompt the non-usability of information or evidence gathered by a requested PEA that, even though complying in full with its own domestic data protection legal framework, has not granted such rights (e.g. a duty for the person under investigation to cooperate with an investigating PEA may well come down to a violation of the so called *nemo tenetur* principle)

    - the adverse effect on viable later enforcement (e.g. prosecution) by traditional competent authorities for the same facts (possible administrative-penal *ne bis in idem* effects, impossibility to use evidence in criminal matters that was gathered by PEA's having administrative investigation/enforcement powers only, etc.)

b. *Ratione materiae* | enforcement cooperation/coordination and related activities/assistance

'Enforcement cooperation' (PEA's "working together") and 'enforcement coordination' (i.e. when PEA's "link their enforcement activities [...] in their respective jurisdictions") are defined (under Section 1: 'Definitions') in an strikingly vague, actually non-defining fashion.

It further appears (from the preamble) that various activities are comprised under 'enforcement cooperation': "sharing best practice, internet sweeps, co-ordinated investigations, or joint enforcement actions leading to penalties/sanctions". Apart from the fact that the preamble is not the place to define the activities that qualify as enforcement cooperation and that no clarity exists as to whether the listed activities are limitative or merely exemplary, especially the mention of "joint enforcement actions leading to penalties/sanctions" raises concerns. It is unclear whether this goes beyond 'enforcement coordination' (as defined under Section 1: 'Definitions', and further clarified under Section 8: 'Coordination principles') (not any longer from their respective jurisdictions?), whether the "penalties/sanctions" are administrative, civil or penal in nature (*supra*, under 1.b, as well as para 60.2[1] of the explanatory report to Convention 108) and whether PEA's need to have such penalizing/sanctioning power themselves (if yes, this contradicts the 'open' definition of PEA above; if no, the question arises whether PEA's not having such power have the ability altogether to conduct such "joint enforcement actions").

2. Convention 108

The preamble recalls "the provisions of the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), specifically those under Chapter IV on mutual assistance". Also the eligibility criteria (under Section 12, ii.a) refer to Convention 108 as a criterion for possible partnership under the Arrangement.

Above all, it seems key to recall that at least Council of Europe DPA's are legally bound by Convention 108. Obviously, the Arrangement, which is just an MoU between PEA's, essentially governed by the Executive Committee of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), acting as a depository with certain executive powers as regards membership etc. (under Section 13)), has no legal force whatsoever (which the Arrangement itself confirms under Section 4: 'Nature of the Arrangement') and can surely not alter or divert from binding international law instruments, such as Convention 108.

In several instances, however, the text of the Arrangement conflicts with Convention 108, which of course undermines the very potential of the Arrangement itself:

a. by not respecting the administrative cooperation nature of Convention 108

Chapter IV of Convention (mutual assistance) allows for administrative cooperation only. The explanatory report (para 71) is explicit on the matter: "The main provisions of this chapter are based on the two recent European conventions relating to mutual assistance in *administrative* matters [...]". The CoE keeps administrative cooperation conventions systemically separate from cooperation conventions in criminal matters, both on the level of mother conventions or thematic conventions. The reasons therefore are obvious, and have also to do with purpose limitation as a core data

[1] "In keeping with the non self-executing character of the convention, it should be left to each State to determine the nature of these sanctions and remedies (civil, administrative, criminal)".

protection issue.[2]

By denying the administrative cooperation nature of Convention 108, the Arrangement can hardly be entered into by PEA's from jurisdictions that are bound by Convention 108. It seems, therefore, that the Arrangement should either be limited to PEA's having administrative investigation/enforcement competencies only, or should provide adequate safeguards to make sure that, as from the moment penal/criminal investigations or enforcement may be envisaged or triggered by a cooperating PEA, a convention basis proper for cooperation in criminal matters is used.

b. by denying the need for a legal basis for cooperation in either international or domestic law

(Most) CoE DPA's/PEA's have no other lawful cross-border cooperation basis than Chapter IV of Convention 108, unless their domestic law autonomously provides such basis. It seems that the latter is not the case for at least the (vast) majority of CoE jurisdictions.[3]

c. by allowing/promoting the sharing between PEA's of personal data

The Arrangement envisages to allow/promote the exchange and sharing of personal data between PEA's. This becomes clear from:

- the preambule: "information [...] which may or may not include personal data"

- Section 7: 'Respecting privacy and data protection principles', leaving it to PEA's themselves to assess the necessity and proportionality of exchanging personal data (*Quis custodiet ipsos custodes*?), whilst at the same time recognizing that some PEA's may require more specific data protection safeguards (as allegedly provided in Schedule One, to which PEA's may choose to opt-in)

- Schedule One, which essentially has been drafted for the sole purpose of enabling personal data exchange and sharing

Article 13, under 3.b of Convention 108 is quite explicit in prohibiting the exchange between DPA's of personal data: "An authority designated by a Party shall at the request of an authority designated by another Party take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed." The explanatory report (para 76) adds: "With regard to factual information, paragraph 3.b specifies that States may not reveal to each other the contents of data contained in data files. This provision is an obvious data protection safeguard for the protection of the privacy of the people concerned".

Consequently, it seems that all DPA's bound by Convention 108 cannot lawfully enter into the Arrange-

[2] See e.g. the CoE Convention on Mutual Administrative Assistance in Tax Matters. Para 225 of the explanatory report prohibits that "normally, information [...] be used for other [than administrative] purposes except by arranging, if this were possible under the laws of the supplying State, for it to be provided under an instrument specially designed for such other purposes (for example, a treaty concerning mutual assistance in judicial matters such as the European Convention on Mutual Assistance in Criminal Matters, ETS No. 30)". Para 266 continues: "It is, in principle, conceivable that the use of information for purposes other than those stated in the Convention could lead to a breach of privacy and clash with the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108)".

[3] Even at EU level, Article 28.6, 2nd paragraph, of Directive 95/46 requires transposition into domestic law.

ment, not even where their domestic law would create an autonomous legal basis for the exchange of personal data with DPA's abroad. In order to serve the purpose of enforcement cooperation, it is advised therefore to limit any exchange of information under the Arrangement to non-personal data. That will still allow for best practice exchange, coordinated internet sweep actions and mutual administrative assistance relating to both legal or factual information in the sense of Article 13 of Convention 108.

3. Adequacy requirement in cross-border relations

Under (1), 2nd paragraph, Schedule One duly recognizes that it "does not, however, preclude circumstances where privacy and data protection laws of a Participant require further safeguards to be agreed between Participants in advance of any sharing of personal data". Whilst in previous versions of the Arrangement/Schedule one (including version 14, which was submitted to the 36th ICDPPC), there was a reference in footnote 3 to the specific obstacles for EU member states to exchange information with 3rd states having no (proven) adequate data protection regime, the omission of the concerned footnote does not exempt EU member states from the prohibition to exchange personal data with such states. Moreover, the suggested 'solution' in the footnote concerned,[4] to rely on "standard contractual clauses [...] to frame transfers of personal data between a Participant rom the EU and a Participant subject to a law and conditions in its country that have not been subject to a positive adequacy finding", is to simple a suggestion. While it is correct that Article 26, under 2, in fine of Directive 95/46 recognizes that sufficient guarantees may derive from "adequate contractual clauses", which may enable a "member state" to set the non-adequacy of a 3rd state's data protection regime aside, Directive 95/46 does not sort direct effect, but requires transposition into domestic law instead. Looking at e.g. the Belgian domestic law, it is up to the Government (as the representative under international law of the Belgium as an EU "member state", after advice of the Belgian DPA), to possibly allow a transfer based on sufficient guarantees derived from adequate contractual clauses. It is anticipated that most EU domestic data protection laws, like the Belgian law and in full conformity with Directive 95/46, will not allow their DPA to assess autonomously whether contractual clauses will be sufficient to allow for personal data transfers to PEA's from non-adequate jurisdictions, but will at least require a government decision instead. It does not seem, therefore, that the adequacy hurdle can be easily overcome in the context of ad hoc needs to exchange/share personal data between PEA's. This problem is all the more a reason to strictly limit the scope of the Arrangement to the exchange of non-personal data (which is a necessity in light of Article 13, under 3.b of Convention 108 in any event; *supra,* under 2.c).

4. Schedule One

From a subsidiary perspective (since Schedule One envisages personal data exchange/sharing, it ought to be deleted altogether in order to enable CoE jurisdictions to join the Arrangement), the following remarks are formulated as regards a number of other specific provisions contained in Schedule One:

a. Under (1) (iv) it is stated that PEA's should "not make a request for assistance to another Participant on behalf of a complainant without the complainant's express consent". At least for all PEA's from jurisdiction bound by Convention 108, this is a mandatory restriction following from Article 15.3 of the latter Convention: "In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned". It seems inopportune, therefore, to include this

[4] Which read as follows: "For example, for the European Union Participants, where binding agreements for transfer are required, the standard contractual clauses provide one option to frame transfers of personal data between a Participant rom the EU and a Participant subject to a law and conditions in its country that have not been subject to a positive adequacy finding".

guarantee in the optional Schedule One.

b. Under (1) (vi) [...] PEA's must "ensure that where sensitive personal data are being shared and further processed, additional safeguards are put in place, such as the requirement that the data subjects give their explicit consent". Since it remains fairly doubtful that domestic laws will allow for the processing of sensitive data by DPA's in the first place, this clause is deemed inappropriate.

c. Under (1) (viii) DPA's must "ensure that any entity to which the receiving participant makes an onward transfer of personal data is also subject to the above safeguards". Not only is it unclear whether the "above" safeguards refer back to these meant under (1) (vii) only (technical and organizational security measures) or to all preceding safeguards ((1) (i-vii)), the exact reasons or purposes of any "onward transfer", if allowed altogether, should clearly feature in the Arrangement.

d. Under (1) (ix) PEA's must "ensure that, where a Participant receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of personal data received from another Participant", the receiving Participant does whatever is in its power to not disclose the information received, seek the consent of the providing Participant or inform the latter if disclosure is mandatory under its laws. This clauses roughly mirrors Section 6.1 (iv) of the Arrangement itself, be it that the latter Section deals with confidential information (not necessarily personal information). In cases where the third party is a judicial body or law enforcement agency, it is hard to understand why the Arrangement and Schedule One equally promote cross-border information exchange/sharing between PEA's rather than domestic information sharing/exchange with the regular authorities competent for enforcement. *Quis custodiet* ...

e. Under 1 (x) PEA's must "ensure mechanisms for supervising compliance with these safeguards and providing appropriate redress to data subjects in case of non-compliance". Is this to be understood as if DPA's/PEA's are to provide independent oversight by a super-DPA? Are there (many) states that can provide such guarantee and that will be capable therefore of opting in into Schedule One? According to oral replies to this question during the 36th ICDPPC, such supervisory task would be taken up by the Executive Committee (sic). Supervision and independent compliance monitoring of DPA's/PEA's by private persons in the executive committee of a conference? *Quis custodiet* ...