Strasbourg, 20 November 2019 T-PD(2019)8FIN

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Opinion on the provisional text and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data

Directorate General Human Rights and Rule of Law

1. Background

1. The Cybercrime Convention Committee (T-CY) started in 2017 to work on the drafting of a second Additional Protocol to the Cybercrime Convention, in view of rendering traditional mutual assistance (MLA) under the Convention more effective (including through the provision of video conference hearing and emergency MLA procedures) and introducing the possibility of *direct disclosure* from service providers in other jurisdictions. Such direct disclosure poses new challenges, implying that data protection safeguards inserted in the Protocol must *also* adequately cover the scenario of direct cooperation, in addition to traditional MLA scenarios to obtain data from service providers.

2. It bears relevance to recall that, leading up to the 2018 Octopus Conference, the 36th Plenary of Convention 108 (19-21 June 2018) adopted Provisional Answers to the Discussion paper for the 2018 Octopus Conference. In addition, the available preparatory documents for the 38th Plenary of Convention 108 (13-14 June 2019), were a T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses, a T-CY discussion note for the consultation with data protection experts (consultation which was held in Strasbourg on 26 November 2018, in which both the Secretariat of the Committee of Convention 108 and the expert participated), and an expert note on the inclusion of data protection safeguards relating to law enforcement trans-border access to data in the second Additional Protocol (document T-PD(2019)3). The Committee of Convention 108 recalls that the Second additional Protocol should adequately reflect the Council of Europe *acquis* on fundamental rights and freedoms, in particular on the protection of personal data. It is therefore essential to ensure consistency of the Second additional Protocol with Convention 108+ (Convention 108 as amended by Protocol CETS 223) which applies to all data processing carried out in the public and private sectors. The current opinion draws and expands on a number of elements, listed hereafter, which were already raised in the Committee of Convention 108 provisional answers to the above mentioned discussion paper for the 2018 Octopus conference and/or in the recent expert note:

a. priority must be given to improving traditional MLA procedures, whereas direct cooperation should be kept for specific cases as an expedited procedure;
b. envisaged direct cooperation or expedited MLA procedures should ideally be limited to subscriber information only;
c. when pertaining to subscriber information, the data protection, procedural and rule of law safeguards of at least both the requesting and the requested Parties should be taken into account;
d. if pertaining to traffic information after all, the data protection, procedural and rule of law safeguards of at least both the requesting Party and the Party where the data subject has used the service(s) should be taken into account;
e. envisaged direct disclosure or expedited MLA procedures must be established on a proper legal basis, and be in conformity, as far as transfer of personal data is concerned, with Article 14 of Convention 108+, avoiding systematic reliance on derogations at all price;
f. any newly established cooperation regime must comply with other relevant data protection requirements, such as with regard to the limited storage of data, subsequent use of data, processing of sensitive data, data breach notification, transparency, accountability, and effective independent oversight;
g. any newly established disclosure regime must either be framed in a unified data protection regime, based on Convention 108+, ideally by inviting Parties to join the latter, or in an optional data protection regime, comparable with that of Article 26.3, 2nd indent of ETS 182, allowing for the combined application of the data protection regimes of the relevant Parties, in line with their national and international data pro-

tection commitments, and reflecting compliance with a range of jointly established substantive data protection principles, in line with Convention 108+.

3. In light of the upcoming Octopus Conference of 20-22 November 2019 and related consultation, the T-CY has now released new provisional text of provisions of the draft Second Additional Protocol, as well as a discussion guide for consultations, thereby seeking written comments from stakeholders, including data protection authorities, and the Committee of Convention 108.

4. The present document provides the provisional position of the Committee of Convention 108 on the newly released provisional text and explanatory report of the draft second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) regarding specifically the provisions on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data (other provisional texts of provisions submitted to consultation fall out of the Committee's field of expertise).

5. In a note preceding the draft text and explanatory report of the articles concerned, the T-CY has set out that these "may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received" and that they "should be considered by the [T-CY Protocol Drafting Group and Protocol Drafting Plenary] in order to determine whether further changes are required […] (in view of the unique circumstances of direct cooperation between authorities and providers) once the ongoing work on conditions and safeguards, including with regard to data protection and privacy, has resulted in a text and explanatory report" [emphasis added].

6. Consequently, the present opinion does not only pertain to the provisional text and explanatory report of both articles concerned, but also provides provisional input of the Committee of Convention 108 for the T-CY's on-going work on conditions and safeguards with regard to data protection. Reference is made here to page 18, point 4.2, para 11, *in fine*, respectively page 29, point 5.2, para 19-20 of the draft explanatory report (to paragraph 2 of the draft article on direct disclosure of subscriber information respectively paragraph 8 of the draft article on expedited production of data between traditional authorities). In these instances, the T-CY explicitly envisages to include an article in the Second Additional Protocol to conditions and safeguards with regard to data protection. The Committee of Convention 108 looks forward to the provisional text of this crucial part of the second Additional Protocol, and highlights that the present opinion is intrinsically dependent on the content of that important part, on which it stresses it wishes to be consulted in as early a stage possible and for which the Committee stands ready to provide its expertise (including on the interpretation of the data protection principles included under 7).

2. Direct disclosure of subscriber information

7. In line with the proposed scoping in the explanatory report (on pages 16-17, in point 4.2, para 4) of subscriber data as potentially inclusive of both static and dynamic IP addresses:

> "Information needed [in specific cases] for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time",

The Committee of Convention 108 recognises that access to both static or dynamic IP addresses may be required in specific cases for the sole purpose of establishing the information as meant in Article 18.3 of the Budapest Convention. It stresses, however, that subscriber data should never be inclusive of any (other) traffic data or content data. The Committee therefore recommends to specify under which circumstances IP addresses could be considered as subscriber information, as meant in Article 18.3 of the Budapest Convention, especially paying due attention to the fact that, depending on the circumstances, an IP address may be evidence of who owns a subscriber account, but does not necessarily identify the individual user at any given time. Moreover, The Committee can only support the potential inclusion of IP addresses under subscriber information if it is specified in the actual Protocol text (both in the articles on direct disclosure and traditional orders for expedited disclosure) and it the corresponding parts of the explanatory report that IP addresses are to be used solely for identification purposes and in specific cases only.

8. The Committee of Convention 108 equally recognises that some Parties currently treat dynamic IP address information as traffic data (for constitutional or other principled reasons, as documented in the T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses). Based thereon, the T-CY has suggested, through the insertion of para 9.b of the draft text, to allow such Parties to reserve the right not to apply the provision on disclosure of subscriber information to "certain types of access numbers" (also reflected in the proposed explanatory report on page 17, in point 4.2, para 4: "Accordingly, paragraph 9.b provides a reservation for some Parties"). The Committee of Convention 108 regrets that the proposed solution might lead to a fragmented regime for criminal cooperation and the protection of personal data, thus impacting the effectiveness of the Protocol.

9. Along the same lines, the Committee of Convention 108 notes the full opt-out possibility (in point 9.a of the draft text) for Parties not to apply the direct disclosure regime. Due to the fragmentation that is likely to arise from the variability of regimes, the "[high] expectations set for the new Protocol", in that it "will need to stand the test of time in order to make a difference in terms of an effective criminal justice response with human rights and rule of law safeguards" (T-CY discussion guide for the upcoming 2019 Octopus Conference, *in fine*), may not be met. If introduced at all, any new direct disclosure regime should be sufficiently straightforward and binding for all ratifying Parties, sustainably building on a common commitment to shared data protection conditions, safeguards or principles (*infra*, under points 6 and 7).

10. The Committee of Convention 108 favours a mandatory notification regime instead of the optional notification possibility foreseen under point 5.

3. Giving effect to orders from another Party for expedited production of data

11. Whilst the explanatory report to paragraph 4 of the proposed text on traditional orders for expedited production of data (page 28, point 5.2, para 14) rightly points out that "under some Parties' domestic laws, the production of traffic data may require further information because there are additional requirements in their laws for obtaining such data", the Committee of Convention 108 questions the position that the only consequence thereof is that "additional information may need to be provided to the requested Party in order for it to give effect to the order". The possibility of an opt-out from the regime as far as traffic data is concerned, as foreseen in paragraph 12 of the proposed text, is equally insufficient.

12. The Committee of Convention 108 believes that the mere reference to potentially higher domestic standards or the opt-out possibility for Parties in relation to obtaining traffic data does not adequately capture the principled and historical distinction the Budapest Convention has made between measures relating to subscriber data vs. measures relating to traffic data. The Committee of Convention 108 believes that such principled distinction should not be sacrificed for alleged reasons of efficiency.

13. Even more fundamentally, and in line with its provisional answers to the discussion paper for the 2018 Octopus Conference, the Committee of Convention 108 takes the position that, as a minimum requirement, a Protocol regime for disclosure of traffic data should allow for the combined data protection, procedural and rule of law safeguards of at least the Party of the requesting competent authority and the Party where the data subject was present whilst using the targeted service(s), if different from the requesting Party or the Party where the service provider is present. A person who is communicating or using services in a Party's territory has a legitimate expectation of privacy under primarily the laws of that Party. As soon as it is possible to establish, based on the prior obtaining of subscriber data, where a person was while using any targeted service(s), it is key for the Protocol to make sure that the data protection, procedural and rule of law safeguards of the latter Party may be applied and complied with. If that Party is the Party where the order originates from, such assurance is implied already. Only in such case, the Protocol may suffice allowing for the combined data protection, procedural and rule of law safeguards of at least the Party of the requesting competent authority and the Party where the service provider [or executing competent authority] is located (as in para 27, *infra*). The Protocol should moreover contain specific provisions which would guide Parties in case of conflict of laws, in that the laws offering the widest protection to the data subject will apply.

4. Insufficient criteria for determining territorial 'presence' of a service provider

14. Both the suggested direct disclosure and traditional cooperation mechanism pertain to the obtaining of data from service providers in another Party's territory. The related draft explanatory report to both mechanisms (respectively in paragraph 10 page 18 and paragraph 5 page 26) reads as follows:

> "[T]he term 'a service provider in the territory of another Party' requires that the service provider be physically present in the other Party. Under this Article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being 'in the territory' of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control."

15. The Committee of Convention 108 insists that further clarification be added, ideally in the text of the draft articles themselves, if not at least in the corresponding parts of the explanatory report, on when a service provider will be considered 'physically present' in a Party's territory. Against the back-drop of the significant jurisprudential contention in the past decade around jurisdiction over service providers abroad, in which a multitude of criteria (a range of 'establishment' criteria, 'offering' criteria etc.) has passed in review, the above two criteria (negatively: that a contractual relationship does not suffice; positively: that data must be in the service provider's possession or control) seem insufficient to bring optimal clarity. The Committee of Convention 108 finds such clarity crucial in order for any future mechanism not to be undermined as well as to avoid forum shopping by authorities/Parties (which would be avoided if mandatory common safeguards were to be incorporated in the Protocol). Not only may the latter confront multinational service providers with parallel orders issued to its establishments or branches in several jurisdic-

tions, it may also encourage authorities/Parties to opt for sending orders to the jurisdiction of presence of the service provider where the lowest data protection standards apply. The Committee of Convention 108 sees relevance in adding more clarity, e.g. by stipulating in the Protocol or in the explanatory report that a service provider will be considered 'physically present' in a Party's territory when it has a stable infrastructure through which it actually pursues an economic activity for an indefinite period and from where the business of providing services is carried out or managed.

5. Confidentiality

16. The explanatory report to paragraph 4.f of the envisaged article on disclosure of subscriber information (page 19, point 4.2, para 17) clarifies that the "special procedural instructions" that need to accompany a disclosure order submitted to service providers are meant to "cover, in particular, any request for confidentiality, including a request for non-disclosure of the order to the subscriber or other third parties". Even if the Committee of Convention 108 sees no difficulty with this, it does however request reconsideration of the opening left in the further explanation given for domestic laws or discretionary policies of service providers that would not guarantee the confidentiality sought ("Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to be aware of applicable law and a service provider's policies concerning subscriber notification, prior to submitting the order under paragraph 1 to the service provider"). Whilst confidentiality may be important to maintain efficiency in criminal investigations, it may equally be vital in safeguarding data protection. The Committee of Convention 108 therefore favours the inclusion of a self-standing provision on confidentiality in the Protocol, for which it suggests inspiration is drawn from:

> Article 26.2 of the Budapest Convention (ETS 185): "Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them";
>
> Article 27.8 of the Budapest Convention (ETS 185): "The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed";
>
> Article 25 of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182): "The requesting Party may require that the requested Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting Party".

17. The explanatory report to the envisaged article on traditional orders for the expedited production of data (page 26, point 5.2, para 8) clarifies that "[u]nder paragraph 3.c, the request should also include all special instructions, including for example requests for certification or confidentiality under Article 27.8 of the Convention, at the time of transmission to ensure the proper processing of the request". Whilst the Committee of Convention 108 sup-

ports the reference to confidentiality and to Article 27.8 of the Budapest Convention, it stresses that, from the draft T-CY text as it stands, it cannot be derived that Article 27.8 of the Budapest Convention applies in a Protocol context. The reference, however, underlines the importance, stressed above by Committee of Convention 108, that a self-standing provision on confidentiality be included in the Protocol itself, for both the direct and the traditional mechanism for obtaining information from service providers.

6. Data protection conditions and safeguards

18. In the absence of a draft text for the envisaged article on data protection (*supra*, under para 6), the Committee of Convention 108 raises particular concern regarding the non-insertion in the draft text and explanatory report as they stand of two-directional data protection conditions, including for asymmetrical transfers under the direct disclosure of subscriber information regime (point 4 of the T-CY draft), but equally for traditional MLA to giving effect to orders for expedited production of data (point 5 of the T-CY draft).

19. The Committee of Convention 108 stresses the importance of making sure, at least, that data protection conditions and safeguards be inserted in the Protocol, applicable in two directions, since the receiving entity may be:

- either a competent authority:
    - in the case of traditional MLA: both the requesting and requested authority being the recipient of personal data, i.e. of the personal data provided in the request or of the personal data transferred as a result of the execution of a request;
    - in the case of direct, asymmetrical transfers: the requesting authority being the recipient of personal data transferred by a private data controller (service provider);
- or a private data controller (service provider), which, in the case of direct, asymmetrical transfers is the recipient of personal data provided in the request.

20. The draft text and explanatory report as they stand, remain silent on the matter, save for a double reference in the explanatory report to paragraph 2 of the proposed draft text on direct, asymmetrical disclose of subscriber information (page 18, point 4.2, para 11), and a single reference in the explanatory report to paragraph 8 of the draft article on expedited production of data between traditional authorities (page 29, point 5.2, para 19 and 20). The three references are exclusively targeted at “parties that have data protection requirements” (first two) or would wish to limit or refuse cooperation based on “conditions and safeguards (including with regard to data protection)” (third). The first reference is only a reminder to parties having data protection requirements of their obligation under domestic laws to provide “a clear basis for the processing of personal data” by service providers in response to an order which they directly received. The second reference relates to international data transfers, without, however, stipulating the actual safeguards that a service provider may require (from the recipient Party or authority) to be able to transfer “responsive subscriber information”. In contrast, the explanatory text only features a blank cross-reference to a future article on data protection, whilst axiomatically stating that (a Party’s implementation law for) the Protocol reflects the “important public interest” of the direct cooperation regime (discussion continued *infra*, under para 20). The framing of the third reference is of concern: the explanatory report (page 29, point 5.2, para 20) warns that “mutual assistance is in principle to be extensive, and impediments thereto strictly limited”, so that “accordingly, conditions and refusals should also be limited in line with the objectives of this Article to eliminate barriers to transborder sharing of subscriber information and traffic data and to provide more efficient and expedited procedures than traditional mutual assistance”. The Committee of Convention 108 considers

that labelling data protection conditions and safeguards as potential 'impediments' and 'barriers' is inappropriate and does not reflect the balanced functioning of democracies safeguarding human rights and the rule of law. It is furthermore not in line with the case-law of the European Court of Human Rights. It believes – based on tangible experiences – that the efficiency of cooperation would be genuinely enhanced when embedded in a shared commitment to respect common data protection principles.

21. In claiming that the envisaged direct disclosure regime in the Protocol reflects an "important public interest" (*supra*, under 19), the T-CY proposal seeks to base the entire direct disclosure concept exclusively on the derogations provided in Article 14.4.c of Convention 108+ and, as far as EU Member States are concerned, in Articles 49.1(d) *juncto* 49.4 GDPR [emphasis below added]

> *Article 14.4 Convention 108+ – Transborder flows of information*
>
> Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if: […] c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; […].
>
> *Article 49 GDPR – Derogations for specific situations*
>
> 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: […] (d) the transfer is necessary for important reasons of public interest; […].
>
> 4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

22. In line with its provisional answers to the discussion paper for the 2018 Octopus Conference and the recent expert note (document T-PD(2019)3), the Committee of Convention 108 disagrees firmly with the above approach, and opposes the envisaged structural and systemic reliance on derogations as a standardised means to allow for direct, asymmetrical transfers.

23. The Committee of Convention 108, in contrast, reiterates its position that the most straightforward, sustainable and widely acceptable way to guarantee an appropriate level of data protection under the Protocol would be the accession by the Protocol Parties to Convention 108+. As a result, an appropriate level of data protection would be generically guaranteed by all Parties to the Protocol and indirectly become a default standard also for the application amongst them of the Budapest Convention itself.

24. In a subsidiary manner, i.e. where the option of accession by the Protocol Parties to Convention 108+ (*supra*) does not prove feasible, the Committee of Convention 108 favours the incorporation in the Protocol (as a legally binding instrument between the Parties) of common mandatory data protection safeguards [list as included *infra*, under point 7], grounded in, closely aligned with and consistently interpreted in line with Convention 108+.

25. In an even more subsidiary manner and as an absolute minimum, the Committee of Convention 108, in line with the recent expert note (document T-PD(2019)3), urges the T-CY to take Article 26 (pertaining to "Data protection") of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182) as a point of departure, thus ensuring consistency with at least the Council of Europe's data protection *acquis* in the context of judicial cooperation in criminal matters. This would imply insertion in the Protocol (as a legally binding instrument between the Parties) of an optional regime, comparable with that of Article 26.3, 2nd indent of ETS 182:

> "Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols where […] the Party to which the data should be transferred is not bound by [Convention 108+], unless the latter Party undertakes to afford such protection to the data as is required by the former Party",

which would need to be rephrased so as to enable two-directional applicability, both in the context of direct transfers and transfers between traditional competent authorities.

26. Further, in case the Protocol Parties were not all to accede to Convention 108+ or no new, mandatory data protection conditions and safeguards were to be inserted in the Protocol, the Committee of Convention 108 suggests, in order to enable and ensure (and if necessary: enforce) compliance by private data controllers (service providers) with the data protection conditions and safeguards in the Protocol (i.e. a public international law instrument, incapable of directly binding private parties), to stipulate in the latter that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if:

> "the receiving competent authority or data controller of the latter Party undertakes to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [i.e. the Party from where personal data would be transferred], including obligations upon the latter under Convention 108 and its Protocol and/or other applicable bilateral, regional or international data protection agreements or instruments guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [list as included *infra*, under point 7]".

27. In doing so, as a minimum requirement, as posited also in the provisional answers to the discussion paper for the 2018 Octopus Conference and the recent expert note (document T-PD(2019)3), a Protocol regime for disclosure of subscriber data should allow for the combined data protection obligations of at least the Party of the requesting competent authority and the Party where the service provider or executing competent authority is located. This would also be seen as a step forward into international harmonisation of data protection requirements in the field of criminal justice cooperation.

28. Since an undertaking as above lacks the "legally-binding and enforceable" character of safeguards as required under Article 14.3.b of Convention 108+, the Committee of Convention 108, in line with the expert note (document T-PD(2019)3), further suggests to introduce an additional obligation in the Protocol for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws.

29. The Committee of Convention 108 notes that, whilst paragraph 1 of both of the draft articles on direct and traditional, expedited ordering of information limits the issuing of orders to information which is needed for the issuing Party's specific criminal investigations or proceedings, the draft text remains fully silent on the purposes for which transferred personal data can be used by the receiving competent authority or service provider. The Committee of Convention 108 furthermore recommends in this regard to include explanations at least in the Explanatory Report on a commonly agreed distinction between data processing (including transfers) for criminal investigation purposes and those undertaken for national security purposes in line with the Issue paper "Democratic and effective oversight of national security services" published by the Commissioner for Human Rights of the Council of Europe.

30. The Committee of Convention 108 requests that clear use restrictions be inserted in the Protocol, applicable to both direct and traditional, expedited cooperation. It suggests to phrase such use restrictions based on the provisions of Article 26 of ETS 182 (*supra*), amending them *mutatis mutandis* and extending them to also cover use limitations upon a service provider to which a request is transferred. This could translate in three provisions, in which it is stipulated respectively that:

1. [*mutatis mutandis* adaptation of Article 26.1 ETS 182] personal data transferred by a competent authority or data controller of a Party as a result of the execution of an order issued under the Protocol by a competent authority of the receiving Party, may be used by the latter only:

   a. for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;
   b. for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);
   c. for preventing an immediate and serious threat to public security;

2. [*mutatis mutandis* adaptation of Article 26.2 ETS 182] such data may however be used by the competent authority for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject[1].

[1] If solely addressed from a data protection perspective, the consent of the data subject ought to be avoided as a ground for data processing in the context of judicial and law enforcement cooperation in criminal matters. However, it should be stressed that the possibility of reliance on the consent of the person concerned is formally part of the contemporary *acquis* of MLA in criminal matters, both at Council of Europe (Article 26.2 ETS 182) and EU level (Article 23.1, under (d) of the EU MLA Convention of 29 May 2000, which was not abrogated from by the European Investigation Order Directive). It is actually the case that the possibility to rely on consent of the person concerned functions here as an extra guarantee for that person in the context of the so called specialty principle (which is the traditional correlative of the purpose limitation principle in data protection law). The specialty principle traditionally has a trust function: the requesting sate or authority ought not to use data for other purposes than the initial purposes, so as not to betray the trust put in it by the executing state or authority in sending the data concerned for those initial purposes. Since the requested state or authority might have refused cooperation or data transfer for other than the initial purposes, the specialty principle stipulates that additional consent of the executing state or authority must be sought in case of intended use beyond the initial purposes (comparable with the control principle in data protection law). To allow for consent of the data subject as a basis for further use could be supported in the very context of use restrictions in the future Protocol regime.

3. [extension to cover use limitations for service providers] the request received and the information it contains can only be used by the receiving service provider for the purpose of the execution of an order issued under this Protocol.

7. Substantive data protection principles

31. To the extent that the option of accession by the Protocol Parties to Convention 108+ (*supra*, under para 22) does not prove feasible, the Committee of Convention 108 urges that the below safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+, would be incorporated in the Protocol as mandatory common safeguards. In an even more subsidiary manner, the Committee of Convention 108 urges that, as an absolute minimum, the Protocol allows service providers or competent authorities to require, as a precondition before transferring any personal data, the receiving competent authority or service provider to undertake to process the personal data transferred subject to the conditions and safeguards under the domestic law of the Party from where personal data would be transferred, guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [allowing flexibility as to possible re-ordering, clustering etc.]:

a. purpose legitimacy, purpose specificity and purpose limitation;
b. lawfulness;
c. fairness and transparency;
d. necessity for and proportionality to the legitimate purpose pursued;
e. non-excessive data processing and data minimisation;
f. adequacy, relevance and accuracy of data;
g. data retention limitation;
h. accountability of controllers and processors;
i. logging, data security and data breach notification duty;
j. information security
k. specific, additional safeguards for special categories of sensitive data;
l. lawful use of exceptions and derogations;
m. enforceable data subjects' rights and effective administrative or judicial redress;
n. appropriate protection in (onward) data transfers;
o. effective independent oversight.

31. Finally, the Committee of Convention 108 stresses the importance of the effectivity of the data protection safeguards and ensuring that Parties to the Second additional Protocol effectively apply and enforce them in practice. The Committee proposes that an evaluation of the implementation of the data protection safeguards be carried out, possibly relying on the findings and recommendations of the mechanism introduced in Article 4.3 of Convention 108+ for Parties to Convention 108+, and, for other countries, on Article 23.f of Convention 108+. The articulation of the work of the T-CY and of the Committee of Convention 108+ in that regard should be further examined.