EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime

Brussels, 4 May 2021

1 CONSULTATION PROCESS AND SCOPE OF CONTRIBUTION

The EDPB welcomes the opportunity given by the Council of Europe Cybercrime Convention Committee (T-CY) to submit written comments on the draft Second Additional Protocol to the Budapest Convention, following the publication on 14 April 2021 of the first complete draft of the protocol, now including draft provisions on conditions and safeguards, and in particular those related to the protection of personal data.

The EDPB already had the occasion to provide and publish its observations and recommendations during previous rounds of consultations, addressing its points of concerns and attention in relation to the draft provisions published at the time. In these previous contributions[1], the EDPB had notably considered essential that the provisional text made public at the time is complemented by dedicated provisions on data protection safeguards, which must then be assessed together with other provisions, in order to **ensure that the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights of the EU (hereinafter the Charter).**

However, **the EDPB deplores that the timeframe of three weeks for this new consultation round, allowing stakeholders to comment for the first time on draft provisions related to the protection of personal data, does not allow for a timely and in-depth analysis.** Such expedite process does not ensure the conditions for a thorough impact assessment of the draft protocol on data protection, which is highly regrettable given the importance of the draft provisions at stake and the need to ensure a sound consultation of all parties, and in particular data protection authorities, in this regard.

Under these circumstances, the EDPB is only in a position of providing a preliminary feedback on the new draft provisions published within the framework of the complete draft protocol now available. In addition to assessing the effect of the draft protocol on the EU legal framework applicable to the protection of personal data and recalling previous recommendations, this contribution focuses on a first assessment of the draft provisions published under Chapter III of the draft protocol related to "conditions and safeguards", and in particular the draft provisions under Article 14 on the protection of personal data.

This contribution is without prejudice to any further analysis and recommendation the EDPB may provide at a later stage or any opinion it may adopt in the context of the signature and ratification process of the finalised protocol.

2 EFFECT OF THE ADDITIONAL PROTOCOL ON AND INTERACTION WITH EU LAW IN THE FIELD OF PERSONAL DATA PROTECTION

The Council of Europe Convention on Cybercrime (hereinafter Cybercrime Convention), as well as any of its additional protocols, are to be considered as legally binding and enforceable international instrument. In this regard, the EDPB stresses that, in line with the Court of Justice of the European Union (CJEU) case law, the "obligations imposed by an international agreement cannot have the effect

[1] EDPB contribution of 13 November 2019 to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime and EDPB Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention).

of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness."[2] **It is therefore essential, in light of the finalisation process of the text being negotiated, that EU negotiating Parties ensure that the provisions laid down in the additional protocol do comply with the EU acquis in the field of data protection in order to ensure its compatibility with EU primary and secondary law.**

From an EU data protection law point of view, the draft protocol, as per its level of norm, provisions and legal effect, would be applicable to the disclosure and transfer of personal data from the EU to third countries. The EDPB also notes in this regard that several Parties to the Cybercrime Convention are neither members of the Council of Europe, nor parties to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Council of Europe Convention 108).

For this preliminary assessment, the EDPB has therefore considered provisions and principles of EU law defining the substantive and procedural conditions for access to personal data, in the situations defined under the draft protocol. Additionally, as this future instrument aims at qualifying as providing appropriate safeguards for personal data transfer from the EU to third country Parties to the protocol, it must be assessed in light of EU law and case law in this regard, in particular by considering the provisions on appropriate safeguards as referred to in Chapter V of Regulation (EU) No 2016/679 (GDPR) and Chapter V of Directive (EU) No 2016/680 (Law Enforcement Directive). In this context, the EDPB signals that the impact of the draft protocol on the requirements under Article 39 of the Law Enforcement Directive remains to be further assessed.

In this context, the EDPB recalls that the CJEU stated that "*although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to 'appropriate safeguards', 'enforceable rights' and 'effective legal remedies', it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled 'General principle for transfers', which lays down that 'all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined'. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out."*[3]

In light of the above and as far as EU Member States are concerned, the EDPB considers that it has to be assessed whether the draft protocol and in particular the draft provisions related to the protection of personal data, ensure that the level of protection of personal data guaranteed under Union law is not undermined. In this regard, the EDPB deems relevant to take into account the recommendations provided in the WP29 adequacy referential [under the GDPR][4] and the EDPB recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive[5], albeit meant for an adequacy assessment. The EDPB also recalls that the European Data Protection Supervisor adopted an opinion following the Commission Recommendation for a Council Decision

[2] CJEU Judgment of 3 September 2008 in joined cases C-402/05 P and C-415/05, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, ECLI:EU:C:2008:461, par. 285.
[3] CJEU Judgment of 16 July 2020 in case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559, par. 92.
[4] WP 254 rev.01, as last revised and adopted on 6th February 2018.
[5] EDPB Recommendation 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2nd February 2021.

authorising the Commission to participate on behalf of the Union in the negotiations of the protocol[6], which is also relevant for this assessment.

The EDPB also wishes to highlight that several provisions of the draft protocol, and in particular those under Chapter II, section 2 related to the direct cooperation with providers and entities in other Parties may, given the level of norm and legal effect of the protocol, also have an effect on transfer and disclosure not authorised by Union law, as per Chapter V GDPR and in particular its Article 48.

Given this possible legal effect of the draft protocol and possible consequences for data subjects, the EDPB therefore considers essential that the draft provisions in this regard are carefully assessed in order to ensure an essentially equivalent level of protection.

3 COMMON PROVISIONS AND MEASURES FOR ENHANCED COOPERATION (CHAPTERS I AND II OF THE DRAFT PROTOCOL)

The EDPB regrets to note that its previous recommendations in relation to these chapters, to a great extent, have not been taken into account. While assessing the now published draft data protection provision (Article 14-see section IV below), **the EDPB considers its previous comments are still valid and calls once more on the negotiators to review their draft in light of the risks identified as to the level of protection of personal data and the possible legal solutions put forward by the EDPB in its previous contributions to remedy these risks.**

- *General principles*

As the various international agreements providing for cross-border exchanges of evidence impact on the fundamental rights of data subjects to privacy and the protection of their personal data, it is important that the legal framework in which they operate is defined as clearly as possible. It stems from paragraph (8) of the draft Article 5 that Chapter II of the protocol "[does] not restrict cooperation between Parties, or between Parties and services providers or other entities, through other applicable agreements, arrangements, practices, or domestic law". This provision leaves an ambiguity as to the nature of the envisaged protocol. To ensure legal certainty, the EDPB recommends clarifying the binding and mandatory nature of the instrument, as a principle and without prejudice to bilateral agreements between Parties to the protocol concluded on the same matters only, provided such agreements ensure the same or a higher level of protection regarding privacy and personal data than the envisaged protocol.

- *Systematic involvement of judicial authorities of the requested Party*

The EDPB recalls that in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and "except in cases of validly established urgency"[7], to a "prior review carried out by a court or an independent administrative body", "following a reasoned request of [competent national]authorities submitted within the framework of procedures of prevention, detection or criminal prosecution."[8] The systematic involvement of judicial authorities in the requested Parties is also essential to preserve the application of the principle of dual criminality in the field of judicial cooperation. The EDPB recalls that

[6] EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.
[7] See CJEU joint cases C-203/15and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, par. 120.
[8] See CJEU joint cases C-293/12and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238, par. 62.

the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State.

- *Disclosure of subscriber information (Article 7)*

The EDPB reiterates its recommendation that further requirements are included in order to ensure that judicial authorities designated by the authorities of the service provider are involved as early as possible in the process of gathering subscriber information in order to give these authorities the possibility to effectively review compliance of the orders with the protocol and ensure the obligation for these authorities to raise grounds for refusal on that basis.[9] In light of the CJEU case law, the EDPB had also considered that the type of requesting authorities who may issue such order should be limited to prosecutor, a judicial authority or another independent authority.

The EDPB furthermore recalls its recommendation that the definition of subscriber information, as per Article 18(3) of the Cybercrime Convention, be further clarified in order to avoid inclusion of any traffic data or content data.

Finally, although Article 7(6) and Article 8 (5) of the draft protocol provide that appropriate levels of security and authentication may be required, the EDPB encourages the development of further specifications and requirements in this regard.

- *Request for domain name registration information (Article 6) and expedited disclosure of stored computer data in an emergency (Article 9)*

The EDPB recalls in this regard that the conditions under which the providers of electronic communications services or the entity providing domain name services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis and that the data protection safeguards contained in the instrument are enforceable upon receiving private entities in the territory of the Parties (see comments on Article 14 below). The lack of commitment at the level of the protocol therefore entails the risk to strip this provision of any protecting effect as to the processing of the personal data already disclosed. Given the third countries which might be Party to the protocol and the level of data protection standards under their domestic law, this raises in particular concerns for the data transmitted by requesting authorities within the EU to another third country Party to the protocol.

4 CONDITIONS AND SAFEGUARDS RELATED TO THE PROTECTION OF PERSONAL DATA (CHAPTERS III AND IV OF THE DRAFT PROTOCOL)

The EDPB very much welcomes the opportunity given to provide, for the first time, comments in relation to the draft provisions related to conditions and safeguards, and in particular those related to the protection of personal data. Given the potential legal effect of the draft protocol already mentioned, it is indeed essential that these provisions do provide for an appropriate level of safeguards and guarantees in order to ensure full compatibility with EU law, in particular in the field of personal data protection. These new draft provisions on conditions and safeguards must furthermore be assessed in conjunction with the provisions concerning the measures for enhanced cooperation already published by the T-CY and commented by the EDPB, as their application may vary depending

[9] See EDPB contribution to the consultation, page 6-edpbcontributionbudapestconvention_en.pdf (europa.eu)

on the type of processing, access and/or transfer resulting from the application of the different chapters of the draft protocol.

Article 13 – Condition and safeguards

The EDPB very much welcomes the direct reference to Article 15 of the Cybercrime Convention, clarifying that "*the establishment, implementation, and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties".* Furthermore, the explanatory report for Article 13 clarifies that the interpretation applicable to the Cybercrime Convention is also valid for Article 13 of the protocol and that therefore "*the principle of proportionality "shall be implemented by each Party in accordance with relevant principles of its domestic law" "*. **In order to ensure legal certainty and clarity, and to enshrine this principle for any processing of personal data resulting from the application of the protocol, the EDPB recommends that the application and implementation of the principle of proportionality is included in the text of Article 13.**

The EDPB indeed notes that all Parties to the Cybercrime Convention may not be bound by the same international obligations as referred to in Article 15 of the Cybercrime Convention. While all Parties are parties to the UN International Covenant on Civil and Political Rights, which notably enshrines the principle that "*no one shall be subjected to arbitrary or unlawful interference with his privacy*", several Parties to the Cybercrime Convention are not parties to the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. This may therefore lead to differences, with regard to specific commitments and safeguards in relation to the right of protection of personal data. This may lead to situations where the protection of personal data may be subject to a different level of international commitments and domestic safeguards, depending on which Parties implement the measures envisaged by the protocol and the applicable law, thus also impacting on the applicable international jurisdiction and avenues for redress.

Article 14 – Protection of personal data

The EDPB regrets that, contrary to all other draft provisions published, the explanatory report for the draft Article 14 is not being published for this consultation process. **The EDPB is therefore not in a capacity to fully assess the extent to which the proposed provision would apply and be interpreted by the Parties, and is consequently only able to provide a preliminary assessment on these provisions, on the basis of the text available to date.**

- *Scope of Article 14*

The EDPB notes that safeguards related to the protection of personal data only apply insofar as "*each Party shall process personal data that it receives under this protocol*", thus excluding dedicated provisions for personal data processed by requesting authorities when implementing, as a whole, the measures enhancing direct cooperation with providers and entities in other Parties, international cooperation between authorities for the disclosure of stored computer data, or emergency mutual assistance. In the absence of specific safeguards applicable to the overall processing of personal data by requesting authorities and private entities implementing the provisions, as well as to any possible resulting personal data transfer to a third country, the EDPB understands that requesting Parties must comply with the requirements under the requesting authorities' domestic law.

The EDPB also notes that paragraphs 2 to 15 would apply to any personal data processing referred above unless "*at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data*" (paragraph 1 b) or the Parties "*mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned*" (paragraph 1 c). **In order to avoid legal uncertainty, the EDPB would recommend to work on clarifying that the draft protocol applies to Parties, unless another agreement or arrangement between the concerned Parties provides the same or higher level of protection regarding privacy and the protection of personal data than the protocol itself.**

The EDPB welcomes the possibility for a receiving Party to impose stronger safeguards than the one provided for under the draft protocol for its own authority, as per paragraph 1(e). The EDPB notes however that it is not clear whether this provision covers both the scenario of the personal data included in the request and received by the requested Party on the one hand, and the personal data received by the requesting authority upon its request, on the other hand. **The EDPB recommends clarifying that both cases are covered and extending therefore the scope of this provision to authorities and private entities for the personal data they receive as included in the request. This should be clarified under paragraph 1(a).**

Paragraph 1(d) provides that "*no further authorization for transfer shall be required under that legal framework*", which may imply the impossibility for Parties to add conditions such as supplementary data protection safeguards to the transfer of personal data when entities under their jurisdiction reply to a request or send a request containing personal data. It seems therefore that while for the processing of personal data by its authorities within its territory a Party may impose stronger safeguards, it would not be allowed to require from the Party receiving the data the provision of equivalent safeguards for the transfer to take place. This means first, that a requesting Party may not give instructions to the requested entity (public authority or private party) for the processing of the personal data included in its request and second, that a requested Party may not refuse to transfer the requested personal data or add conditions to it, based on data protection rules under its domestic law, unless the reference to Articles 25(4) and 27(4) of the Cybercrime Convention under Article 7(5)c)ii), Article 8(8) and Article 10(7) of the draft protocol could be interpreted as allowing such refusal or that the possibility of imposing conditions under Article 8(8) and Article 9(6) of the draft protocol could be interpreted as allowing the possibility of imposing additional data protection safeguards.

By stating that "*each Party shall consider the processing of personal data pursuant to paragraphs 1.a and 1.b to meet the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorization for transfer shall be required under that legal framework*", paragraph 1(d) equates to a "presumption" of compatibility of the draft additional protocol with EU law, or of essential equivalence when it comes to the level of protection of personal data when transferred to a third country Party to the Cybercrime Convention as per the draft additional protocol. It is however essential that such "presumption", to be validly considered as per EU law, is made effective through compliant and operational safeguards and conditions as per the draft protocol.

Such reasoning also applies where, in application of the specific measures envisioned by the draft additional protocol, the latter may be considered as providing appropriate safeguards under Article 37(1)(a) of the Law Enforcement Directive, provided that it can be considered as a legally binding instrument between competent authorities.

Therefore, given the current and possible future third country Parties to the Cybercrime Convention, in light of the above and taking into account applicable CJEU case law, **the EDPB strongly recommends incorporating the additional safeguards requested in its contributions in the protocol and allowing the Party transferring personal data - either within its request or in reply to a request - to require from the receiving Party additional safeguards for the processing of the personal data it transferred or to allow the requested Party to refuse such transfer so as to ensure that any transfer of personal data as per the draft additional protocol will be subject to safeguards assuring that the level of protection of personal data guaranteed under Union law is not undermined.**

- *Purpose and use*

The EDPB welcomes that dedicated provisions are included in relation to the purpose and use of personal data received by the requesting Party under paragraph 2, purpose limitation and the compatibility of purposes being an essential principle to ensure the lawfulness and fairness of personal data processing.

However, the EDPB expresses concerns on the lack of clarity and preciseness of the provision when referring to incompatible purposes which mentions only the "domestic legal framework" of the receiving Party in this regard. This concern is all the more significant considering that, while the transferring Party may impose additional conditions pursuant to the draft Protocol in a specific case, paragraph 2 also specifies that "such conditions shall not include generic data protection conditions". Furthermore, the lack of clarity and preciseness of this provision is likely to affect also the obligations concerning the retention periods since paragraph 5 of Article 14 refers to paragraph 2 of the same article.

The EDPB recalls that EU law, and in particular the Law Enforcement Directive, provides that processing for the purpose of the prevention, investigation, detection or prosecution of criminal offences other than that for which the personal data has been collected shall be permitted in so far as the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.[10] When it comes to personal data whose processing is subject to the GDPR, the EDPB recalls that processing for a purpose other than that for which the personal data have been collected is subject to specific conditions[11], and may be allowed for instance based on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) GDPR.

The domestic legal framework of third country Parties to the Cybercrime Convention applicable to the compatibility of purpose may significantly diverge from the one in the Union or Member States law, thus possibly resulting in further processing that may not be considered as compatible under Union or Member States law.

The EDPB therefore recommends that the provisions of the draft protocol related to purpose and use do allow requested Parties to impose additional generic data protection conditions, and specifies in the text of paragraph 2 that the further processing of personal data by the receiving Party should be provided by law, and should constitute a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest.

[10] See Article 4(2) of the Law Enforcement Directive.
[11] See Article 6(4) GDPR.

- *Sensitive data*

The EDPB notes that paragraph 4 does not provide for a principle of general prohibition with exceptions for the processing of special categories of personal data, but mandates that such processing may only take place "under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination".

The EDPB furthermore considers that, to be fully compatible with EU law, the provisions of the draft protocol related to the processing of sensitive data may only take place where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject, beyond the sole reference to "the risk of unwarranted prejudicial impact from the use of such data".

The EDPB also wishes to recall, with regard to the observance of the principle of proportionality, that the CJEU has stated that "*in order to satisfy that requirement, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake*"[12].

As per paragraph 4, biometric data is only included under sensitive data if "considered sensitive in view of the risks involved". The EDPB highlights that the discretionary margin inherent to any such assessment may allow receiving third country Parties to the Cybercrime Convention to potentially consider biometric data "for the purpose of uniquely identifying a natural person" as non-sensitive, thus without applying the appropriate safeguards as referred to under paragraph 4; hence, **the EDPB strongly recommends replacing "considered sensitive in view of the risks involved" by "which allow or confirm the unique identification of that natural person".**

- *Retention periods*

While recalling its concerns in relation to the draft provision on purpose and use which may have an impact on paragraph 6, the EDPB welcomes the inclusion of a specific provision in relation to retention periods.

- *Automated decisions*

The EDPB welcomes the fact that limitations apply to decisions based solely on automated processing of personal data, but points out that such limitation, and therefore possible authorisation, may significantly vary depending on the domestic law of the receiving Party. **The EDPB therefore recommends that paragraph 6 is amended in order to clarify, in addition to the possibility to obtain human intervention, that safeguards under domestic law of the Parties authorising such processing provide guarantees for the rights and freedoms of the data subject.**

Furthermore, the EDPB notes that paragraph 6 does not specifically provide for a general prohibition of processing of sensitive data in the context of automated decisions. **The EDPB therefore strongly recommends that paragraph 6 includes a specific provision prohibiting the processing of sensitive**

[12] CJEU Opinion 1/15, par. 141.

data for the purpose of automated decision-making, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are explicitly mandated for under paragraph 6.

- *Maintaining of records*

The EDPB notes that the obligation set forth under paragraph 8 is limited to the "how" of accessing, using and disclosing an individual's personal data in a specific case and highlights that the requirements under EU law go beyond a mere "how" and recommends therefore enhancing this obligation.

The EDPB also notes that this obligation is applicable only to certain processing activities (access, use and disclosure) and not to other processing activities such as storage. **The EDPB recommends therefore explicitly extending the application of paragraph 8 (on maintaining records) to any processing activities and in particular to "storage".**

- *Onward sharing within a Party*

While welcoming the provisions under paragraph 9 related to onward sharing within a Party, the EDPB notes that such sharing may only take place in accordance with all the provisions under Article 14 of the draft protocol, including the provisions related to purpose and use. The EDPB therefore recalls in this context its concerns and recommendations related to the provisions on purpose and use of the draft protocol.

Furthermore, the EDPB highlights that, in accordance with EU law, onward sharing within a Party would amount to a further processing of personal data transferred to a third country and must therefore comply with the applicable requirement thereof. **The EDPB notably considers that the draft provisions under paragraph 9 should be complemented, in order to include a mechanism so that the transferring authority is informed by the receiving Party of the envisioned onward sharing and further processing[13].**

- *Onward transfer to another State or international organisation*

The EDPB welcomes the clear provision under paragraph 10, mandating the prior authorisation of the transferring authority for the transfer by the receiving Party to another State or international organisation.

The EDPB recalls in this regard, and in order to make this draft provision fully effective and operational, the need for a systematic involvement of the authority in the requested Party, including when it comes to direct cooperation with providers or other entities in other Parties.

- *Transparency and notice*

The EDPB notes that the contact details of the controller are not included in the list of information to be made available to the data subjects under Article 14(11) and recommends extending the list to this information.

The EDPB also highlights that, in the context of direct cooperation with providers and entities in other Parties, the limitations and restrictions related to personal notice as per paragraph 11(c), would have

[13] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, par. 40.

to be complied with by the service provider or entities concerned, subject, where the requesting Party is within the EU, to the provisions of Article 23 GDPR.

Paragraph 11 of the draft protocol, read in conjunction with paragraph 12(a)(i), implies that these possible limitations and restrictions to transparency and notice are to be permitted under the domestic legal framework of the receiving Party. The domestic legal framework of third country Parties to the Cybercrime Convention applicable to restrictions on transparency and notice may significantly diverge from the ones in the Union's or Member States' law, thus possibly resulting in limitations that may not be considered as compatible with Union or Member States law.

The EDPB wishes to recall in this regard that measures laying down restrictions to data subject rights must be provided for by law and need to be foreseeable. The domestic law must be sufficiently clear in its terms to give individuals an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions[14]. Furthermore, the EDPB also recalls that any restriction shall respect the essence of the right that is being restricted. This means that restrictions that are so extensive and intrusive that they void a fundamental right of its basic content cannot be justified[15].

- *Access and rectification*

The right of access and the right to rectification are essential elements of the right to data protection under Article 8(2) of the Charter. The EDPB recognises that exercise of data subjects' rights are usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations. The EDPB recalls however that in its Opinion 1/15, the CJEU found that "*air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities" considering that "[t]hat information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal*"[16].

Article 14(12)(a) foresees the right to access and rectification for data subjects whose personal data has been received under this protocol and not to any data subjects whose personal data has been processed under this protocol. There might indeed be cases where the personal data included in the request relate to a different data subject from the one whose personal data are received by the requesting Party. In such case and if this provision is to be given a narrow interpretation, it would mean that the rights to access or rectify the data are ensured only for the data subject whose personal data has been transferred to the requesting authority but not for the data subject whose personal data were included in the request.

Furthermore, the EDPB notes that the provision related to access under paragraph 12(a) provides that any individual may seek and obtain "a written or electronic copy of the documentation kept on that individual". The scope of the right of access as per the draft protocol may not be fully consistent with EU data protection law which also provides that data subjects are entitled to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. **The EDPB therefore recommends complementing the provisions under paragraph 12 in order to ensure that**

[14] See EDPB Guidelines10/2020 on restrictions under Article 23 GDPR, under public consultation, par. 17.
[15] See EDPB Guidelines10/2020 on restrictions under Article 23 GDPR, under public consultation, par. 14.
[16] CJEU Judgment of 6 October 2015, in case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95[Emphasis added].

any individual may seek and obtain information as to whether or not personal data concerning him or her are being processed.

As for the draft provisions on transparency and notice under paragraph 11, the EDPB also recalls that measures laying down restrictions to data subject rights must be provided for by law and need to be foreseeable, and that any restriction shall respect the essence of the right that is being restricted.

The EDPB notes that paragraph 12(b) specifies that "any expense for obtaining access should be limited to what is reasonable and not excessive", while as per EU law, information and action taken by a data controller for the exercise of data subject rights shall be free of charge, unless requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character. The EDPB therefore recommends to update the provision under paragraph 12(b) in order to reflect this principle and ensure that, as a general rule, information to individuals related to access and rectification shall be provided free of charge.

Considering the above, the EDPB wishes to insist on the importance of information and the exercise of data subject rights, also with a view to ensuring an effective availability of remedies. **The EDPB considers that these draft provisions, and in particular the conditions under which information and data subject rights may be restricted should be clarified and specified in order to be fully consistent with EU law, and notably meet the foreseeability and proportionality criteria.**

- *Absence of any specific safeguards in relation to privileges and immunities*

The EDPB notes that the draft protocol does not ensure the respect of other safeguards attached to the personal data such as privileges and immunities and calls for the introduction of such safeguards.

- *Judicial and non-judicial remedies*

The EDPB welcomes the draft provision under paragraph 13 stating that each Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of the draft protocol safeguards on the protection of personal data. The EDPB stresses that such remedies need to be effectively available under the jurisdiction of all Parties to the Cybercrime Convention, to any concerned data subjects.

The EDPB recalls that the CJEU found[17] that the lack of effective judicial redress when personal data are transferred to a third country goes to the essence of Article 47 of the Charter, which provides for the right to an effective judicial protection. In that context, the CJEU found that "*legislation not providing for <u>any</u> possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" and that "*the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article*"[18].

Also, the CJEU has stressed that it is essential for individuals to be able to file complaints with independent supervisory authorities[19] and seek, therefore, administrative redress.

[17] CJEU Judgment of 6 October 2015, in case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.
[18] CJEU Judgment of 6 October 2015, in case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95 [Emphasis added].
[19] CJEU Judgment of 6 October 2015, in case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 56 to 58.

While welcoming that the obligation under the draft protocol for each Party to have in place effective judicial and non-judicial remedies to provide redress (paragraph 13), **the EDPB recommends clarifying the text and the explanatory report, in order to ensure that both redresses are available under the jurisdiction of each Party to the Cybercrime Convention to any concerned data subjects. Such clarification appears** all the more important considering that not all Parties to the Cybercrime Convention fall under the jurisdiction of the European Court of Human Rights.

- *Oversight*

The EDPB welcomes the draft provisions on oversight and recommends **establishing mechanisms to foresee the cooperation and exchange of information between established public authorities ensuring oversight in each Party**, thus allowing for a coordinated and consistent supervision of the implementation of the draft protocol and providing additional contribution in light of the assessment foreseen under its Article 23.

- *Consultation and suspension*

The EDPB welcomes that the draft protocol provides for a specific provision allowing for the suspension of transfers to a Party to the protocol in case of breach of the terms of Article 14. It notes however that the clause is limited to a suspension of the transfers under the protocol and has no effect on personal data transferred prior to this suspension. It therefore would not suspend the legal effect of other provisions of the protocol such as the further use, onward sharing or onward transfers of personal data obtained prior to the suspension. **The EDPB therefore recommends extending the effects of the suspension to the whole protocol.**

- *Article 23: Consultations of the Parties and assessment of implementation*

While welcoming the introduction of a mechanism to periodically assess the effective use and implementation of the provisions of this protocol, the EDPB recommends first that the review focuses not only on the implementation of the protocol but also on the evaluation of its necessity and proportionality. For the purposes of such a review, it should provide detailed information and statistics about the implementation of the protocol and foresee that the review teams include data protection experts and involve EU Data Protection Authorities. Finally, the EDPB however notes, as far as Article 14 is concerned, that such assessment would not commence before at least 10 Parties to the Cybercrime Convention have expressed their consent to be bound by this protocol. **The EDPB strongly recommends aligning the obligation to assess the implementation of Article 14 with the entry into force of the protocol hence according to Article 16(3), as soon as five Parties to the Cybercrime Convention have expressed their consent to be bound by this protocol.**

5 CONCLUSION

Given the significant legal effects the draft protocol may have on the EU legal framework in the field of personal data protection, and in light of the concerns and need for clarification highlighted in this contribution and the previous ones, **the EDPB calls on the T-CY members and protocol drafters, to amend the draft provisions presented for consultation, in order to ensure the finalised protocol is fully compatible with EU primary and secondary law, guaranteeing that the level of protection of personal data as per EU law is not undermined.**

The EDPB acknowledges that situations where judicial and law enforcement authorities are faced with a "cross-border situation" with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB recalls that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement purposes, which are fully compatible with the EU Treaties and the Charter.

The EDPB recalls its availability to further exchange with the T-CY and drafters, in order to meet this objective.