SC 1961 APOSTILLE

OCTOBER 2021

PREL. DOC. NO 10

Title	Privacy and Data Protection
Document	Prel. Doc. No 10 of August 2021
Author	PB
Agenda Item	Item 10.i.
Mandate(s)	C&R No 36 of CGAP 2019
Objective	To outline potential issues related to privacy and data protection in the operation of the Apostille Convention.
Action to be Taken	For Decision ☒ For Approval ☐ For Discussion ☐ For Action / Completion ☐ For Information ☐
Annexes	N/A
Related Documents	N/A

Table of Contents

Privacy and Data Protection

I. Introduction

1 When the Apostille Convention was drafted, the complex issues of privacy and data protection facing the global community today could not have been contemplated. Our increased reliance on information technology continues to generate unprecedented levels of data, all of which must be collected, processed, and retained. This has driven enhanced regulatory frameworks for privacy and new regulatory schemes relating to data protection and retention.[1]

2 These legal and technological trends affect all sectors and disciplines, and the operation of the Apostille Convention is no exception. These developments are particularly relevant in the context of the electronic Apostille Programme (e-APP), as data is collected, processed, and retained in a digital form when issuing e-Apostilles and maintaining e-Registers.

3 During the May 2021 meeting of the Experts' Group on the e-APP and New Technologies, the Group discussed privacy and data protection in relation to the e-APP and noted that the potential interaction of regulatory frameworks with the provisions of the Convention may merit further discussion by the Special Commission.[2]

4 While recognising that compliance with both the Convention and applicable regulatory frameworks remains the responsibility and prerogative of individual Contracting Parties, this document outlines a number of matters to be considered at each stage of the Apostille issuance and verification process.

II. Convention Framework and Practical Implications

5 An Apostille Certificate does not itself contain any personal information. All 10 numbered standard informational items are related to the underlying document and the certifying authority. However, the issuance process naturally requires some additional data to be collected, which may give rise to some privacy and data protection issues.

6 To issue an Apostille under Article 3, the Competent Authority collects information from the applicant, both of a personal nature and in relation to the public document to be apostillised. While it is the discretion of the Competent Authority to determine how this is done, the collection, processing, and retention of data may be governed by data protection regimes, irrespective of whether applications are made electronically or in hard copy.

7 To certify the origin of the underlying public document, most Competent Authorities use a database of sample signatures, seals, and stamps, against which the origin of the public document can be verified.[3] Any personal information about the signatory stored for this purpose would typically only be in relation to those acting in an official capacity and is therefore unlikely to give rise to privacy or data protection issues.

8 Once issued, an Apostille should not be shared with persons other than the applicant. For in person applications, this may involve verification of the identity of the applicant. In an electronic context, this may involve securely delivery or transmission.

---

1 See, *e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (European Union).

2 See Prel. Doc. No 6 of May 2021, "Report from the Chair on the Experts' Group on the e-APP and New Technologies", Annex I, para. 12.

3 See Prel. Doc. No 2 of August 2021, "Summary of Responses to the Apostille Questionnaire", paras 26 *et seq*.

9 Once an Apostille has been issued, Article 7 requires that Competent Authorities record specific information on the certificates it issues in a "register or card index", namely:

a. the number and date of the Apostille certificate; and

b. the name of the person signing the underlying public document and the capacity in which that person has acted, or in the case of unsigned documents, the name of the authority which has affixed the seal or stamp.

10 Today, Competent Authorities in over a third of Contracting Parties maintain e-Registers, enabling online Apostille verification.[4] The majority maintain registers that are not publicly available in either electronic or paper form. Regardless of the form or accessibility of a register, the recording and retention of data for the purpose of Article 7 may give rise to a number of privacy and data protection considerations.

11 The first consideration relates to the type of information being recorded (*i.e.*, the data being retained). The recording requirements of Article 7(1)(a) are general in nature and those of Article 7(1)(b) are related to persons acting in an official capacity, neither of which pose problems for privacy or data protection. However, Competent Authorities may record additional information about the application and / or applicant in their register. For example, some Competent Authorities may retain an image or copy of the underlying public document. While this practice facilitates the user experience of an e-Register, the underlying public document may contain personal or otherwise sensitive information.[5] Depending on the nature of the information being recorded, this may give rise to privacy or data protection concerns, such as whether the applicant must give express consent to the collection and retention of their personal data (and whether and how that consent can be revoked).

12 The second relevant consideration is security. While the text of Article 7(2) invites Apostille verification requests from "any interested person", in practice this is generally deemed to refer to the applicant and intended recipient(s) of the Apostille. The register should not be accessible to persons who do not have access to the relevant Apostille, or a need to verify its authenticity. In this context, the e-APP Forum has stressed the importance of preventing "fishing expeditions" (*i.e.*, attempts by users of an e-Register to access or collect information about Apostilles that they have not received) through random numbering and / or requiring a separate code.[6]

13 The third consideration relates to the period of data retention. The Convention does not impose any time limitations on the validity of an Apostille, nor does it impose a specific retention period for records in a register. This means that an Apostille does not expire and is valid for as long as it remains identifiable and attached to the underlying public document.[7] Accordingly, the registers maintained by Competent Authorities must be able to offer verification of these Apostilles. The Special Commission has previously noted that it is a matter for each Contracting Party to develop objective criteria regarding how long Apostille records should be retained.[8] With the introduction of e-Registers, the recommendation has evolved, encouraging Contracting Parties to maintain access to entries online for "as long as possible".[9]

---

4 See "Implementation Chart of the e-APP" available on the Apostille Section of the HCCH website at < www.hcch.net >.

5 The relevance of data protection laws in the context of displaying the underlying public document (and / or the Apostille) in an e-Register was identified by the e-APP Forum as early as 2012 (see 11(c) of the Seventh (Izmir) Forum), and has been recalled on multiple occasions since: see, *e.g.*, C&R No 28 of the Tenth (The Hague) Forum (endorsed by C&R No 21 of the 2016 SC).

6 See C&R No 29 of the Tenth (The Hague) Forum (endorsed by C&R No 21 of the 2016 SC).

7 The fact that an Apostille does not expire has been recognised by the e-APP Forum. See C&R No 23 of the Tenth (The Hague) Forum (endorsed by C&R No 21 of the 2016 SC).

8 See C&R No 21 of the 2003 SC. It is worth noting this discussion was had in the context of Contracting Parties that maintained paper registers, or electronic registers on CDs which had limited capacity.

9 See C&R No 33 of the Tenth (The Hague) Forum (endorsed by C&R No 21 of the 2016 SC).

14 This quasi-permanent retention of data may give rise to data protection concerns if the register contains the underlying public document, in particular in jurisdictions where retention of an individual's private data is prohibited absent express consent. A related issue may arise in data protection regimes where an individual is able to revoke consent, such as in the context of the "right to erasure" / "right to be forgotten" under the General Data Protection Regulation of the European Union.[10]

15 At least one Contracting Party has noted that potential conflicts in this context are resolved by allowing Apostille applicants to decide whether the content of the underlying public document is visible in the register, and if so, to specify that it should be removed after a certain time.[11]

16 In short, while Apostilles alone do not contain the personal information of the applicant, an Apostille may still be associated with protected information, depending on the practices of Competent Authorities. Contracting Parties should carefully consider what information is recorded for internal archiving purposes, what is publicly accessible via an e-Register, how long these records are maintained, and the privacy or data protection implications in the relevant jurisdiction.

III. Proposal for the Special Commission

17 The Special Commission is invited to consider whether additional guidance is needed in relation to the intersection of the operation of the Convention and existing privacy and data protection frameworks.

18 Contracting Parties are invited to inform the PB of challenges that have arisen in the context privacy and data protection, together with any practices or procedures that have been implemented to resolve them.

10 General Data Protection Regulation, Art. 17. The GDPR also provides for a limited number of exceptions to the right to erasure (see Art. 17(3)).

11 Estonia reported this practice during the May 2021 meeting of the Experts' Group on the e-APP and New Technologies. For more information, see Estonian Chamber of Notaries, "What is an e-Apostille", *Certification of Public Documents by Apostille*, available at: < https://www.notar.ee/en/teabekeskus/apostille >.