E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

PCT/WG/17/8
ORIGINAL: ENGLISH
DATE: JANUARY 18, 2024

# Patent Cooperation Treaty (PCT) Working Group

## Seventeenth Session
## Geneva, February 19 to 21, 2024

PERSONAL DATA PROTECTION AND THE PCT

*Document prepared by the International Bureau*

**SUMMARY**

1. PCT processes should be reviewed for consistency with modern general principles of personal data protection and privacy, having regard to the wishes of applicants and inventors, the public interest and the data storage and transfer requirements of a distributed international system, which requires effective processing and long-term record keeping.

2. Document PCT/WG/17/9 includes a proposal concerning availability of email addresses, which is designed also to support further work in relation to public access to personal data such as postal addresses as outlined below. The other main area identified for consideration is whether to allow personal data to be kept up-to-date using Rule 92*bis* even after 30 months from the priority date.

**PERSONAL DATA PROTECTION PRINCIPLES**

3. The processing and use of PCT data should be in line with the United Nations principles on personal data protection and privacy (the "Principles"), as set out in the Annex to this document. With regard to their application to WIPO, the Principles state that: "The United Nations System Organizations are encouraged to adhere to these Principles and may issue detailed operational policies and guidelines on the processing of personal data in line with these Principles and each Organization's mandate." Within the mandate of WIPO, among its functions, Article 4(iii) of the WIPO Convention states the administration of international agreements designed to promote the protection of intellectual property, with PCT Article 55 assigning the administrative tasks of the PCT Union to the International Bureau, with the Director General of WIPO serving as the Chief Executive of the Union. WIPO must therefore follow any requirements of the PCT in its application of the Principles. Nevertheless, within the

legal framework of the Treaty, WIPO should endeavor to adhere to the Principles where possible. Moreover, the PCT membership can agree on any amendments to the PCT Regulations or modifications to Administrative Instructions where this would allow closer alignment to the Principles.

4. Some of the main issues concerning each of the Principles are indicated below:

5. *Fair and Legitimate Processing*: The personal data collected should be processed only for the stated purposes. The requirements imposed on national Offices in their capacities as receiving Office or International Searching and Preliminary Examining Authority should be compatible with any applicable national and regional data protection obligations.

6. *Purpose Specification*: A clear specification of the purpose of processing the data is essential to defining the other requirements. The personal data is collected for the purpose of the processing of the PCT application, noting that this includes the purposes of:

(a) processing and publishing the international application efficiently in the international and national phases, ensuring that applicants providing the required data in the international phase do not need to repeat or supplement it in the national phase, unless details have changed or translations are required;

(b) maintaining long term records of the application process; in the case of applications that have been published, most of those records should be open to inspection in the public interest;

(c) providing public search and statistical information; and

(d) recognizing and analyzing activities of the applicant or the agent so as to be able to provide more effective service across the portfolio of their interactions with the Organization.

7. *Proportionality and Necessity*: Different considerations may apply to the availability and processing of different categories of data, as discussed below.

8. *Retention*: Rule 93.2 requires that “The International Bureau shall keep the file, including the record copy, of any international application for at least 30 years from the date of receipt of the record copy.” This reflects the potential life of a patent and likely subsequent periods during which court proceedings may occur. In practice, the expectations of legitimate historical records and statistical analysis mean that at least basic name data should be kept indefinitely.

9. *Accuracy*: At present, the International Bureau is obliged to record changes of name and address on request, but only if that request is made by the applicant or receiving Office and only if it is received within 30 months from the priority date. Requests made by any other person (such as directly from an inventor concerned) or after that time must not be recorded.

10. *Confidentiality*: Articles 30 and 38 impose strict confidentiality requirements on the content of unpublished applications. However, following international publication, Rule 94 gives access to most of the content of the application file, including personal data, with only limited exceptions.

11. *Security*: Information security is a primary concern of the International Bureau, with major efforts being devoted to designing PCT IT systems to be secure and conducting continual security testing. It is expected that national Offices processing PCT data meet the requirements of the Treaty and have similar priorities concerning their IT systems.

12. *Transparency:* The requirements of international phase data processing are mainly set out within the PCT Regulations and Administrative Instructions. Following publication, certain data is made available via PATENTSCOPE and to other database providers for patent search and statistical purposes. Such data should not include personal data beyond what is necessary for the relevant purposes. All current personal data of published applications (and unpublished applications that have entered the national phase early before a particular Office) is made available to national Offices since it should not have been collected unless it may be relevant to national phase processing. The further national processing of such data is generally subject to national data protection laws, rather than the PCT.

13. *Transfers:* The International Bureau transfers personal data to receiving Offices, International Searching and Preliminary Examining Authorities and designated Offices for the purpose of PCT processing. Personal data is made available to the public through PATENTSCOPE and related systems (such as WIPO CASE and Global Dossier) as part of the public record, with measures taken to restrict the possibilities for automated extraction of certain personal data. Limited personal data may be transferred to database suppliers. The International Bureau transfers some data to translation services under obligations of confidentiality, but this would not include personal data.

14. *Accountability:* The International Bureau continually reviews its information processing policies and tests information security. Conditions of use are applied to individuals and systems accessing data supplied by the International Bureau.

**ISSUES OF INTEREST**

15. The personal data normally held in the International Bureau's records of international applications are the names and addresses of individuals - applicants, inventors and agents or other persons acting as an address for service. In principle, other personal data may appear in documents submitted to the International Bureau or national Offices in their role as receiving Office or International Searching and Preliminary Examining Authority. However, this is unusual and would not be held in a structured format allowing it to be searched and located. To the extent that someone becomes aware that such data has been submitted, it is not permitted to remove it from the record, but it may be permitted to exclude the matter from public access under Rules 26*bis*.3(h-*bis*), 48.2(l) or 94.1(d) and (e).

16. This document does not give further consideration to personal data submitted for unusual reasons embodied in general correspondence. However, in principle it is desired to increase the use of full text processing of correspondence, which might increase the visibility of such data. Consequently, comments are invited on further issues of personal data protection that may require additional work in future.

17. The issues known to be of interest concerning names and addresses are their public visibility and their accuracy. The data collected and stored are as follows:

| Person | Data | Notes |
|---|---|---|
| Applicant(s) | Name<br>Address<br>Email address<br>Telephone No.<br>Fax No.<br>Applicant's registration No.<br>Nationality and residence | Telephone and fax numbers are optional. An email address should be required for at least one applicant or agent.<br><br>Address, nationality and residence are required for at least one applicant to establish the right to file an application but may be omitted for others and are required for all applicants where a fee is reduced to show eligibility for the relevant reduction. |
| Inventor(s) | Name<br>Address<br>Email address | The paper request form uses the same boxes for inventors as for applicants so telephone number, fax, nationality and residence may appear, but are not required and are not recorded in the International Bureau's database, except where the inventor is also an applicant.<br><br>Email address is optional.<br><br>If no inventors are indicated, the receiving Office may draw attention to this fact, but cannot require the applicant to add the information (Receiving Office Guidelines, paragraph 90). |
| Agent(s) or Address for Correspondence | Name<br>Address<br>Email address<br>Telephone No.<br>Fax No.<br>Agent's registration No. | |

VISIBILITY OF NAMES AND ADDRESSES

18. The most commonly encountered data protection concern is the public availability of names and addresses.

19. Occasionally, inventors wish to have their names hidden entirely. At present, this is only possible by not submitting the names in the international phase, but this has serious consequences for national phase processing in States that require the name of the inventor to be furnished at the time of filing. Furthermore, in most Contracting States, the inventors' names and addresses will be made publicly available in the national phase as part of the national register, so the information may not remain hidden following any national phase entry.

20. The applicant may add indications of inventors after filing the application, but the PCT does not directly allow a person claiming to be an inventor to have their name added other than through the agreement of the applicant or provide for an international system for resolution of such disputes, though some national laws allow for resolution of inventorship disputes for national purposes even before national phase entry.

21. More common is that both applicants and inventors do not wish their private addresses to be visible to the public. Because they are so cheaply and easily usable for “spam”, most users do not wish their email addresses to be visible to the public. At present, efforts have been made to avoid email addresses being visible to the public in formats that are easily extracted automatically. For example, the XML version of the request form is not made available on PATENTSCOPE. However, all supplied postal and email addresses are visible in an image format view of the request form.

22. There is a clear public interest in ensuring that every patent application has at least one address made public to allow anyone to contact someone who has a relationship to the invention, but this does not necessarily require the visibility of all addresses or all forms of contact details.

23. Consequently, it would be desirable to allow certain data to be hidden from the public view of the patent application on PATENTSCOPE while still making it available to the applicant and to national Offices through ePCT or other privileged data feeds. The most immediate concern relates to email addresses. For that purpose, document PCT/WG/17/9 includes a proposed amendment to Rule 94 allowing such redaction of personal data, together with draft Administrative Instructions to apply it initially to email addresses included in XML forms. If that proposal is adopted, further modifications to the Administrative Instructions could then be used to permit the redaction of other matter, such as addresses, once the appropriate conditions and technical considerations were agreed.

24. Postal addresses appear in a variety of locations, including the main part of the request form, in different types of declaration under Rules 4.17, and in different locations within PCT Forms and the international publication. Some of these disclosures appear necessary; it is probably desirable to exclude others, but it is essential to ensure that this does not prevent receiving Offices, International Authorities and designated and elected Offices from performing their duties efficiently. Consequently, it is proposed to proceed with the amendment to Rule 94 set out in document PCT/WG/17/9, but initially to act only in relation to email addresses. Access to other personal data could be modified following a careful review of the technical options and processing needs of national Offices.

25. Consideration would need to be given to whether information on PATENTSCOPE might be restricted in all cases or only upon special request. The most simple and reliable system would involve treating all equivalent information the same way, noting that it is effectively impossible to “unpublish” information that has accidentally been made available. Public interest in information concerning the origin of inventions suggests that inventors’ names should be indicated unless there is a strong reason not to. On the other hand, there would appear to be no public interest in the routine availability of inventors’ postal or email addresses, provided that these are available to relevant national authorities. It might be appropriate to list inventors’ names with sufficient information to allow statistical analysis of inventor origin, for example listing addresses to the level of country or city.

UPDATING OF NAMES AND ADDRESSES

26. Current Rule 92*bis* allows changes of name and address data on the request of the applicant or the receiving Office, provided that the request for recording is received by the International Bureau within 30 months from the priority date.

27. Occasionally, inventors directly submit requests to correct their name and address. This is only permitted if the request is resubmitted in time by the applicant (in the usual sense of the agent where one has been appointed or the common representative in the case of multiple applicants without an agent). Unlike some national data protection laws, the Principles do not explicitly offer rights to individuals to ensure that their own data is correct. Ensuring that such requests are valid and made by the individual concerned would introduce a significant burden

on the International Bureau, which does not have any authority to resolve disputes. Consequently, it is proposed to leave this situation unchanged, noting that in some cases national laws might give receiving Offices the power to investigate and make appropriate changes to their own records, which might result in the receiving Office in turn requesting a change to be made.

28. With regard to the period within which updates may be requested, a future session of the Working Group might consider whether Rule 92*bis* should be amended to allow the International Bureau's records to be updated at any time. To avoid unnecessary work being created for the International Bureau and national Offices, it would need to be made clear that:

(a) any changes would not necessarily have effect in designated Offices where national processing has already started - this is already implicitly the case, but the difference is only relevant to early national phase entry and would probably need to be stated explicitly to avoid creating unrealistic expectations; and

(b) national Offices should not be pushed notifications of changes that cannot be relevant to them.

29. Such a change does not appear to be a high priority since it would have limited effect on national processing. Nevertheless, it would allow applicants with an opportunity to allow contact details to be kept up to date in the international record where this is useful to them. Furthermore, it might simplify the introduction of more effective customer IDs, allowing changes of names and addresses across a portfolio of international applications, without having to make special arrangements to "freeze" data after a certain date.

**TECHNICAL APPROACHES**

30. Any change to the visibility of names and addresses would need to ensure that the International Bureau and national Offices remained able to access and use all the information necessary to process international applications efficiently.

31. Where data is supplied in XML, this should form the complete and official version of the file. Redacted PDF views might be generated for the public file, but the full information would need to be processed. In principle, it would be possible also to render an unredacted view in PDF format. However, generating and storing multiple different versions of a document risks adding complexity and the possibility of Offices making the wrong version visible to the public. It will usually be preferable to process the data automatically as far as possible, generating temporary views of relevant parts of the data where it is necessary for it to be read by the applicant or an Office user.

32. An important example of this would include processing of new applications and of changes in names and addresses. It should not be necessary for the PDF versions of request forms or Form PCT/IB/306 (Notification of the Recording of a Change) to show personal data in full. It should be sufficient that a notification ensures that records are properly updated in all relevant databases, while ensuring that applicants and Offices have easy access to both the current data and the history of changes. Offices should nevertheless receive all the information necessary to determine quickly, accurately and usually automatically both what the change is and whether it is relevant to them, such as the effective date of the change where this was made close to the time when national phase processing began.

33. PATENTSCOPE's delivery of XML corresponding to documents would likely be limited only to that for the application body. Other documents on file would be shown in image views only (this is already the case for some key documents such as the request form in order to protect email addresses). XML for specific documents may remain available to

PATENTSCOPE in order to allow rendering of translated versions of forms, but would not be delivered directly to the public.

34. More generic bibliographic data feeds may need to be updated. The International Application Status Report already excludes email addresses. Any further changes to public visibility of personal data would mean that database suppliers would need to be provided with an appropriate new XML data feed.

**POSSIBLE RULE CHANGES**

35. Document PCT/WG/17/9 contains a proposal to amend Rule 94 to allow the exclusion of personal information from the public record under conditions to be set by the Administrative Instructions. The proposal is included in that document as an immediate measure to support electronic processing, allowing email addresses to be redacted. This is done to eliminate a concern from applicants over the proposal to require applicants to supply at least one email address for processing purposes, which would otherwise become visible to the public. However, the proposal is framed also to allow other personal data to be hidden, likely including the postal addresses of inventors and potentially of at least some applicants. This would be the subject of further consultations, following further analysis of technical issues and the requirements of national Office processing before proposing Administrative Instructions going beyond the issue of email addresses.

36. The most likely future proposal would be to amend Rule 92*bis* as discussed in paragraphs 26 to 29, above. However, the International Bureau is open to other suggestions to improve the handling of personal data in PCT processing.

**COSTS AND TIMING**

37. The cost of any changes to the current arrangements will be highly dependent on their scope, complexity and timing. The cost to the International Bureau of measures to hide from public availability personal data that is supplied in structured XML format will be fairly small provided that all needs can be served by a single stylesheet and there is no need to maintain dual PDF views of the data to enable processing by national Offices and the same visibility rules apply to all equivalent data. Costs to both the International Bureau and national Offices may be further reduced by making changes at the same time as related work on the relevant systems and processes.

38. Enabling applicant choices on data visibility or delivering different versions of forms to national Offices and to the public would significantly increase costs and risks. Furthermore, identifying and removing personal data from image based or otherwise unstructured data is time consuming, costly, difficult or impossible to automate and liable to error. It is envisaged that any work on personal data protection would focus on automating processes for data submitted in structured formats and that special handling of other personal data would generally require reasoned requests under Rules 26*bis*.3(h-*bis*), 48.2(l) or 94.1(d) and (e) or similar provisions.

*39. The Working Group is invited to comment on issues and priorities concerning personal data protection and the PCT.*

[Annex follows]

# UNITED NATIONS PRINCIPLES ON PERSONAL DATA PROTECTION AND PRIVACY

## INTRODUCTION: PURPOSE AND SCOPE

**Purpose:** These principles (the "Principles") set out a basic framework for the processing of "personal data", which is defined as information relating to an identified or identifiable natural person ("data subject"), by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.

These Principles aim to:

(i) harmonize standards for the protection of personal data across the United Nations System Organizations;
(ii) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations System Organizations; and
(iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy.

**Scope:** These Principles apply to personal data, contained in any form, and processed in any manner.

The United Nations System Organizations are encouraged to adhere to these Principles and may issue detailed operational policies and guidelines on the processing of personal data in line with these Principles and each Organization's mandate.

Personal data should be processed in a non-discriminatory, gender sensitive manner.

Where appropriate, these Principles may also be used as a benchmark for the processing of non-personal data, in a sensitive context that may put certain individuals or groups of individuals at risk of harms.
United Nations System Organizations should exercise caution when processing any data pertaining to vulnerable or marginalized individuals and groups of individuals, including children.

In adherence with these Principles, the United Nations System Organizations should conduct risk-benefit assessments or equivalent assessments throughout the personal data processing cycle.

**Implementation of these Principles is without prejudice to the privileges and immunities of the relevant United Nations System Organizations concerned.**

## PRINCIPLES

| | | |
|---|---|---|
| *1* | *Fair and Legitimate Processing* | The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations System Organization concerned; (iii) the mandates and governing instruments of the United Nations System Organization concerned; or (iv) any other legal basis specifically identified by the United Nations System Organization concerned. |

| | | |
|---|---|---|
| *2* | *Purpose Specification* | Personal data should be processed for specified purposes, which are consistent with the mandates of the United Nations System Organization concerned and take into account the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes. |
| *3* | *Proportionality and Necessity* | The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing. |
| *4* | *Retention* | Personal data should only be retained for the time that is necessary for the specified purposes. |
| *5* | *Accuracy* | Personal data should be accurate and, where necessary, up to date to fulfill the specified purposes. |
| *6* | *Confidentiality* | Personal data should be processed with due regard to confidentiality. |
| *7* | *Security* | Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing. |
| *8* | *Transparency* | Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated. |
| *9* | *Transfers* | In carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfies itself that the third party affords appropriate protection for the personal data. |
| *10* | *Accountability* | United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles. |

[End of Annex and of document]