Luciana Duranti

The InterPARES Framework for the development of policies, strategies and standards

Luciana Duranti
She is research aims at finding solutions to digital records issues that are not specific to a given socio-cultural and juridical context but can be universally applied. She is presently Project-Director of InterPARES, a large multinational, collaborative and interdisciplinary research project on the long-term preservation of authentic electronic records. She graduates degrees in Archival Science from the University of Rome, Special School for Archivists and Librarians, and in Archivistics, Paleography, and Diplomatics from the School of Archivistics, Paleography and Diplomatics of the State Archives of Rome.

Introduction

The InterPARES projects, between 1998 and 2006, have examined the creation, maintenance and preservation of electronic records. A major finding of the research is that, in order to preserve trustworthy records, i.e., records that can be demonstrated to be reliable, accurate and authentic, records creators must create them in such a way that it is possible to maintain and preserve them. This entails that a relationship between a records creator and its designated preserver must begin at the time the records are created.

The research undertaken in records and information-related legislation showed that no level of government in any country to date has taken a comprehensive view of the records lifecycle, and that, in some cases, legislation had established significant barriers to the effective preservation of electronic records over the long-term, most notably with respect to copyright.

On the basis of several surveys, case studies and analyses of texts reflecting on directives, laws and regulations of various kids, InterPARES developed a framework of principles that should guide policies, strategies and standards, which is flexible enough to be useful in differing national environments, and consistent enough to be used in its integrity as a solid basis for any such document. In particular, this framework balances different cultural, social and juridical perspectives on the issues of access to information, data privacy, and intellectual property.

The framework comprises two complementary sets of principles, one for records creators and one for records preservers. The principles for records creators are directed to the persons responsible for developing policies and strategies for records creation,

maintenance and use within any kind of organization, and to national and international standards bodies. The principles for records preservers are directed to those responsible for developing policies and strategies within administrative units or institutions that have as their core mandate the preservation of the bodies of records created by persons, administrative units, or organizations external to them and selected for permanent preservation under their jurisdiction for reasons of legal, administrative, or historical accountability.

Here the two sets of principles are presented in an integrated way, discussing together a principle directed to the records creator with the corresponding principle directed to the preserver. The purpose is to make evident the relationship between records creator and designated preserver and declare its nature. The principle statements for the creator are identified by a C and the principle number. The principle statements for the preserver are identified by a P and the principle number. The two statements are followed by an explanatory narrative. The principles are more often phrased as recommendations ("should") rather than imperatives ("must"), because some of them might not be relevant to some records creators or preservers. The complete text of the Framework will be published on the InterPARES Project web site at www.interpares.org.

Principles for policy development for records creators and records preservers

[C1] Digital entities must have fixed documentary form and a stable content to be considered records and to be capable of being preserved over time.

[P5] Authentic copies should be made for preservation purposes only from the creator's records, that is from digital entities that have a fixed documentary form and a stable content.

The InterPARES project has defined a record as "a document made or received in the course of a practical activity[1] as an instrument or a by-product of such activity, and set aside for action or reference," adopting the traditional archival definition. This definition implies that, to be considered as a record, a digital entity must first be a document, that is, present a fixed documentary form and a stable content. Only digital entities possessing both these characteristics are capable of serving the record's memorial function because, without them, a digital entity cannot be reproduced for future reference.

Digital entities can be given any form and any content needed for business or reference

[1] Glossary definitions, in Terminology Database, online at http://www.interpares.org/ip2/ip2_terminology_db.cfm

purposes. When the action in which the digital entities participate is completed, all those entities that need to be retained for subsequent use, reference or accountability purposes must be kept as records by stabilizing their content and fixing their documentary form.

The concept of stable content is self-explanatory as it simply refers to the fact that the data and the message in the record are unchanged and unchangeable. This implies that data cannot be overwritten, altered, deleted or added to. Thus, if one has a system that contains fluid, ever changing information, one has no records in such a system until one decides to make one and to save it with its unalterable content.

The concept of fixed form is more complex. A digital entity has a fixed form when its binary content is stored so that the message it conveys can be rendered with the same presentation it had on the screen when first saved. Because the same presentation of a record can be produced by a variety of digital presentations, fixed form does not imply that the bit streams must remain intact over time. It is possible to change the way a record is contained in a computer file without changing the record; for example, if a digital entity generated in Word is later saved in PDF, its presentation, or "documentary form," has not changed, so one can say that the entity has a fixed form.

One might produce digital information that can take many different documentary forms-can be presented on the screen in several different way but the content presented in each instance is selected from a fixed store of content within the system and the rules that govern the selection of content and the form in which it is presented on the screen do not vary. Each presentation of such digital information in the limited series of possibilities allowed by the system is to be considered as a different view of the same record having stable content and fixed form.

In addition, one has to consider the concept of "bounded variability,[2]" which refers to situations where variations in the record's form and content are either caused by technology (e.g. different operating systems or applications used to access the document), or due to the intention of the author or writer of the document (e.g. the construction of documentary forms that enable users to select subsets of content and control both the sequencing and presentation features, such as image magnification). In consideration of the fact that what causes these variations also limits them, they are not considered to be violations of the requirements of fixed form and stable content.

[2] See Luciana Duranti and Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES," *Archival Science* (2006)

Organizations should establish criteria for determining which digital entities need to be maintained as records and what methods should be employed to fix their form and content if they are fluid when generated. The criteria should be based on business needs but should respect as well the requirements of legal, administrative and historical accountability.

Based on this understanding, any preservation policy should clearly state that reproductions of authentic copies for preservation purposes can only be made from the creator's records, as they are determined by the creator, and may or may not be captured in a recordkeeping system. The preserver should know (or help establishing) the creator's criteria for determining which digital entities are maintained as records and what methods were employed to fix their form and stabilize their content. This is consistent with the preserver's responsibility to advise the creator on its record creation processes and technologies. This advising activity will also provide the preserver with the critical information needed to understand the business activities and processes that caused the records to come into being and with the ability to assess their continuing identity and integrity.

[C2] Records creation procedures should ensure that the digital components of records can be separately maintained and reassembled over time.

[P4] Records preservation procedures should ensure that digital components of records can be separately preserved and reassembled over time.

A digital record is a record in digital format, meaning it is a record output from a computer system, typically on a screen, when needed by a human, or in interactions between systems. Differently from an analogue record, in which medium, form and content are inextricably linked and can be stored and preserved as a unit, in a digital record, medium, form and content can be separated and, in addition, parts of form and content can exist as quite separate components and stored in one or more bit streams, which in turn constitute one or more digital components that can be interpreted or presented by specific computing software and hardware. A digital component may contain all or part of the content of a digital record, and/or data or metadata necessary to order, structure, or manifest the content. For example, an e-mail containing a textual message, a picture and a digital signature has at least four digital components: the header data, which enable systems to properly route and manage the message, the text of the message, and two attachments having different storage requirements: the picture, and the digital signature.

The fundamental finding that emerged from the studies conducted by the InterPARES project is that to preserve a digital record means to preserve the ability to reproduce it, that is, to

preserve its various digital components, the linkages among them, and the methods of reassembling them as a record. Digital preservation in this sense requires the early identification of a record's digital components necessary to reproduce it for subsequent access and use. Organizations should establish polices and procedures that stipulate the identification of digital components at creation stage and that ensure they can be maintained, transmitted, reproduced, upgraded, and reassembled over time.

The preserver must be prepared to advise the creator, directly or through development of recommended standards, on the types of digital components that the preserver's system is able to sustain. Where standards governing the types and formats of digital components are common to the record creation/maintenance and preservation systems, the preserver can directly influence those standards in favour of those that meet preservation requirements. Where there are no such common standards, the preserver must understand the degree of interoperability of certain types and formats of digital components. This understanding will provide a basis for the preserver to assess the capability of the preservation system to preserve the digital components and their relationships as they emerge from the creator's record creation/maintenance systems.

Highly interoperable formats, that is, formats that are not tied to specific applications or versions of applications, are generally seen to provide a better basis for preservation work. It is important, however, not to focus exclusively on the interoperability of formats at the expense of the relationships between them that also must be preserved. For example, an HTML-based web page may be comprised of digital components that are highly interoperable but the version of HTML coding used to structure the components may be an old version with many deprecated terms, i.e., terms that are not recognized by current software browsers that may be used to reproduce the web page.

[C3] Records creation and maintenance requirements should be formulated in terms of the purposes the records are to fulfill, rather than in terms of the available or chosen record-making and recordkeeping technologies available.

[P6] Preservation requirements should be formulated in terms of the purpose or desired outcome of preservation, rather than in terms of the available or chosen technologies available.

Digital records rely, by definition, on computer technology and any instance of record exists within a specific technological environment. For this reason, it may seem useful to establish record creation and maintenance requirements in terms of the technological applications in which the records may reside, or the technological characteristics of the records. However, not only do technologies change, sometimes very frequently, but they are also governed by proprietary considerations established (and modified at will) by their developers. Both these factors can significantly affect the accessibility of records over time. For these reasons references to specific technologies should not be included in records policies, strategies and standards governing the creation and maintenance of an organization's records.

Only the business requirements and obligations that the records are designed to support should be explicitly kept into consideration at such a high regulatory level. At level of implementation the characteristics of specific technologies should be kept into account in order to support established business requirements and make possible their realization.

Technological solutions to record creation and maintenance are dynamic, meaning that they will evolve as the technology evolves. New technologies will enable new ways of creating records that meet an organization's business requirements. As they will be used to create records, reference to new archival knowledge will continue to be required.

Technological solutions also need to be specific in order to be effective. Although the general theory and methodology of digital preservation applies to all digital records, the maintenance solutions for different types of records require different methods. Their choice should be based on the specific administrative-juridical context in which the records are created and maintained, the functions and activities to which the records are related, and the technologies employed in their creation to ensure the best solutions are adopted for their maintenance.

Records creation and record preservation policies that are expressed in terms of, respectively, business or preservation requirements rather than technologies will need to be periodically updated as the organization's or the preserver's business requirements change, rather than as the technology changes. It is the role of a specific action plan to identify appropriate technological solutions for the maintenance or preservation of specific aggregations of records. The identified solutions must be monitored with regard to the possible need for modifying and updating. This requires the creating organization and the preserving entity to be aware of new research developments in the archival and records management fields and to collaborate with interdisciplinary efforts to develop appropriate methods for the management or preservation of digital records.

[C4] Records creation and maintenance policies, strategies and standards should address the issues of record reliability, accuracy, and authenticity expressly and separately.

[P2] Records preservation policies, strategies and standards should address the issues of record accuracy and authenticity expressly and separately.

In the management of electronic records, reliability, accuracy and authenticity are three vital considerations for any organization that wishes to sustain its business competitiveness and to comply with legislative and regulatory requirements. These considerations should be directly and separately addressed in records policies and promulgated throughout the organization. The concept of reliability refers to the authority and trustworthiness of a record as a representation of the fact(s) it is about, that is, to its ability to stand for what it speaks of. In other words, reliability is the trustworthiness of a record's content. It can be inferred from two things: the degree of completeness of a record's form and the degree of control exercised over the procedure in the course of which the record is generated. Reliability is then exclusively linked to record's authorship and is the sole responsibility of the individual or organization that makes the record.

An accurate record is one that contains correct, precise and exact information. Accuracy of a record may also indicate the absoluteness of the data it reports or its perfect or exclusive pertinence to the matter in question. The accuracy of a record is assumed when the record is created and used in the course of business processes to carry out business functions, based on the assumption that inaccurate records harm business interests. However, when records are refreshed, converted or migrated for continuous use, or the technology in which the record resides is upgraded, the data contained in the record must be verified to ensure their accuracy was not harmed by technical or human errors occurring in the transformation processes. The accuracy of the data must also be verified when records are created by importing data from other records systems. This verification of accuracy is the responsibility of the organization receiving the data; however such organization is not responsible for the correctness of the data value, for which the sending organization is accountable. Thus, the receiving organization should issue a disclaimer regarding reliability of records using other organizations' data.

The concept of authenticity refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted. In other words, authenticity is the trustworthiness of a record as a record. An authentic record is as reliable and accurate as it was when first generated. Authenticity depends upon the record's transmission and the manner of its maintenance and custody. Authenticity is maintained and verifiable by maintaining the identity and integrity of a record. The identity of a record is established and

maintained by indicating at a minimum the names of the persons participating in the creation of the record (e.g., author, addressee); the action or matter to which the record pertains; the date(s) of compilation, filing or transmission; the relationship of the record to other records through a classification code or a naming convention; and the existence of attachments. Establishing the integrity of a record requires identifying the responsibility for the record through time by naming the handling office(s) and the recordkeeping office, and indicating any annotations or modifications (technical or otherwise) made to the record by the offices. Thus, reliability and accuracy are qualities that are established when records are created while authenticity is a quality that is connected with the maintenance of the record. The latter is therefore a responsibility of both the record creator and any legitimate successor. Authenticity is not a quality that can be bestowed on records by any preservation process, which can only protect and maintain it is there. It is protected and maintained through the adoption of methods that ensure that the record is not manipulated, altered, or otherwise falsified after its creation, either during its transmission or in the course of its handling and preservation, within both the recordkeeping and record-preservation systems. It is the preserver's responsibility to assess authenticity of records considered for acquisition into a preservation system, and to ensure that it remains intact by respecting the same Benchmark Requirements that bind the creator (e.g. access privileges, measure against corruption or loss) and the Baseline Requirements for preservers.[3]

[C5] A trusted record making system should be used to generate records that can be presumed reliable and accurate.

No corresponding requirement for the Preserver other than as a Record Creator itself.

A trusted record-making system consists of a set of rules governing the making of records, and a set of tools and mechanisms used to implement these rules. In order to generate reliable and accurate records, every record-making system should include in its design integrated business and documentary procedures, record metadata schemes, records forms, record-making access privileges and record-making technological requirements.

Integrated business and documentary procedures are business procedures linked to documentation procedures and the file management plan (i.e. classification system)

[3] The concepts of presumption of authenticity and of authenticity as composed of identity and integrity were developed by InterPARES 1. See the *Authenticity Task Force Report* at http://www.interpares.org/book/interpares_book_d_part1.pdf and, more specifically, the *Requirements for Assessing and Maintaining the Authenticity of Electronic Records* at http://www.interpares.org/book/interpares_book_k_app02.pdf.

established in the organization. This integration reinforces the control over record-making procedures: it supports the reliability and accuracy of records by explicitly connecting records to the activities in which they participate and to the records organization system thereby standardizing the procedures for creating and managing those records. The integration of business and documentary procedures also establishes the basis and central means to demonstrate ownership of and responsibility for the records.

A record-making metadata scheme is a list of all metadata elements that need to be documented in the course of record-making processes for the purpose of uniquely identifying each record and enabling the maintenance of its integrity and the presumption of its authenticity. Such a scheme can also be used later on to verify authenticity when questioned. Record forms are specifications of the documentary forms for the various types of records generated in the record-making system.

Access privileges refer to the authority to compile, edit, annotate, read, retrieve, transfer, and/or destroy records in the record-making system, granted to officers and employees by the organization based on job duties and business needs. Access privileges control access to the record-making system and are established in the course of integrating business and documentary procedures through connecting specific classes of records to the office of primary responsibility for a business function or activity. The establishment and implementation of access privileges is the most important step towards ensuring that the reliability and accuracy of records can be presumed. Record-making technological requirements include the hardware and software specifications for the record-making system that have a direct impact on the documentary form of records.

[C6] A trusted recordkeeping system should be used to maintain records that can be presumed accurate and authentic.

[P11] Archival appraisal should assess the authenticity of the records.

[P12] Archival description should be used as a collective authentication of the records in a fonds.

A trusted recordkeeping system consists of a set of rules governing the keeping of records, and a set of tools and mechanisms used to implement these rules. Every recordkeeping system should include in its design a recordkeeping metadata scheme, a classification scheme, a retention schedule, a registration system, a recordkeeping retrieval system, recordkeeping technological requirements, recordkeeping access privileges, and procedures for maintaining authentic records.

A recordkeeping metadata scheme is the list of all necessary metadata to be attached to

each record to ensure its continuing identity and integrity in the recordkeeping system. A classification scheme is a plan for the systematic identification and arrangement of business activities and related records into categories according to logically structured conventions, methods and procedural rules. A retention schedule is a document specifying and authorizing the disposition of records series and/or classes as identified in the classification scheme. A registration system is a method for assigning a unique identifier to each created record, linked to its identity and integrity metadata. Recordkeeping access privileges refer to the authority to classify, annotate, read, retrieve, transfer, and/or destroy records in the recordkeeping system, granted to officers and employees by the organization based on job duties and business needs. Typically, the access to records for purpose of classification, transfer and destruction is given only to the record officer (records manager or archivist) of the organization. A recordkeeping retrieval system is a set of rules governing the searching and finding of records and/or information about records in a recordkeeping system, and the tools and mechanisms used to implement these rules. Recordkeeping technological requirements include the hardware and software specifications for the recordkeeping system. The procedures for maintaining authentic records are the procedures designed to ensure that the identity and integrity of the records in the recordkeeping system are protected.

An organization should include in its records management policy that it is the record keeper's responsibility to manage the recordkeeping system. The role of the record keeper is that of a trusted custodian who should have the qualification for trusted custodian stated in the principle C8.

A recordkeeping system that complies with the above requirements and procedures in its design and management is capable of ensuring the authenticity of records after their creation, since these requirements and procedures establish the maximum degree of control with regard to the maintenance and use of the records.

The existence of a trustworthy recordkeeping system allows the preserver to presume the authenticity of the records under its control when assessing it in the course of appraisal. Preservers must then determine the feasibility of preserving them as authentic records. More precisely, they must decide whether the digital components embodying the essential elements that confer identity and are essential to the integrity of the records can be preserved, given the preserver's current and anticipated capabilities. This would include the state of preservation knowledge, hardware and software capabilities, staff expertise, and financial resources. The preserver must monitor records that have been appraised. The activities associated with doing so are necessary to ensure the continuing preservation of the

appraised authentic records. The monitoring activity occurs after an appraisal decision is made and before disposition is undertaken. Appraisal decisions need to be reviewed to ensure that the information about the appraised records is still valid, that changes to the records and their context have not adversely affected their identity or integrity, and that the details of the process of carrying out disposition are still workable and applicable to the records.

Archival description of a fonds emerges from the comprehensive analysis of the various relationships interwoven in the course of records' formation and accumulation, and therefore is the most reliable means of establishing the continued authenticity of a body of interrelated records. While the authenticity of individual records can be in part established through their metadata, the authenticity of aggregations of records, i.e., file, series, or fonds, can only be proved through archival description. In fact, as original records disappear and an interminable chain of non-identical reproductions follows them, the researchers looking at the last of those reproductions cannot find in it any information regarding provenance, authority, context, or authenticity. The authentication function of archival description is different from that of a certificate of authenticity, because it isn't simply an attestation of the authenticity of individual records, but a collective attestation of the authenticity of the records of a fond and of all their interrelationships as made explicit by their administrative, custodial and technological history, the scope and content, and the hierarchical representation of the records aggregates. And, it is different both from the identity and integrity metadata attached to individual records, which are part of the record itself and are reproduced time after time with it, and from the additional metadata attached to records aggregations (e.g. file, series) identifying them and documenting their technological transformation. The unique function of archival description is to provide an historical view of the records and of their becoming while presenting them as a universality in which each member's individuality is subject to the bond of a common provenance and destination.

[C7] Preservation considerations should be embedded in all activities involved in record creation and maintenance if a creator wishes to maintain and preserve authentic records beyond its operational business need.

[P7] Preservation considerations should be embedded in all activities involved in each phase of the records lifecycle if their continuing authentic existence over the long term is to be ensured.

The concept of the record lifecycle in archival science refers to the theory that records go through distinct phases, including creation, use and maintenance, and disposition (i.e.

destruction or permanent preservation).

It is essential for organizations dealing with records in digital form to understand that, differently from what is the case with traditional records, preservation is a continuous process that begins with the creation of the records. This notion requires that preservation considerations be incorporated and manifested in the design of record-making and keeping systems. Each aggregation of records appraised for preservation should be identified in accordance with classification plans and records retention schedules established by the organization, and this identification should be indicated in the records metadata. The records so identified should be monitored throughout their lifecycle so that appraisal decisions and preservation considerations can be updated and/or modified to accommodate any possible changes occurring after they are first made. In order to monitor and implement appraisal decisions and preservation considerations, the designated preserver should be given access to the organization's recordkeeping system. Policies and procedures should be established to facilitate constant interaction between the organization and its designated preserver.

[C8] A trusted custodian should be designated as the preserver of the creator's records.

[P1] A designated record preserver fulfills the role of trusted custodian.

The designated preserver of an organization's records is the entity responsible for taking physical and legal custody of, and preserving (i.e., protecting and ensuring continuous access to) the organization's records. Be it an outside organization or an in-house unit, the role of the designated preserver should be that of a trusted custodian. To be considered as a trusted custodian, the preserver must

- act as a neutral third party, i.e., demonstrate that it has no stake in the content of the records and no reason to alter records under its custody, and that it will not allow anybody to alter the records either accidentally or on purpose,
- be equipped with the knowledge and skills necessary to fulfil its responsibilities, which should be acquired through formal education in records and archives administration, and
- establish a trusted preservation system that is capable of ensuring that accurate and authentic copies of the creator's records are acquired and preserved.

As long as the organization's records are maintained by the organization in its recordkeeping system, they are operational records, although under the responsibility of a trusted record keeper. A record custodian trusted by the organization should maintain records that have been removed from the recordkeeping system for long-term or indefinite preservation. The preserver, after having assessed the authenticity of the records, produces an authentic copy

of them from the creator's recordkeeping system. Records acquired this way are authentic copies of the operational records of the creator identified for long-term preservation because they are made by the designated trusted custodian. The authentic copies of the creator's records are then kept by the trusted custodian in a trusted preservation system, which should include in its design a descriptive and a retrieval system, and rules and procedures for the ongoing production of authentic copies as the technology is upgraded and the existing one becomes obsolete.

It should be noted that the simple fact of reproduction of records in the preserver's preservation system does not make of its result an authentic copy. Such designation must be provided by the preserver's authority. It should also be recognized that a sustainable preservation strategy requires close collaboration between a records creator and its designated trusted custodian, and it is the preserver's responsibility to take the initiative in collaborating with the creator to establish acquisition and preservation procedures and in advising records creators in any records management activities essential to the preserver's acquisition and preservation activities.

This trusted custodian will establish and maintain a preservation system to receive and preserve the organization's digital records. This involves ensuring that the authenticity of the records received from the organization is assessed and maintained. Within the context of the preservation system, the preserver identifies appropriate preservation strategies and procedures, drawing on expertise from various disciplines, including archival science, computer science and law. The preservation procedures are implemented within the preservation system.

[C9] All business processes that contribute to the creation and/or use of the same records should be explicitly documented.

[P10] Archival appraisal should identify and analyze all the business processes that contribute to the creation and/or use of the same records.

Records created in the course of carrying out one business function or one business process are often also used in the course of conducting other business functions or processes. In cases like this, records resulting from different activities may be mixed together in the organization's record-making system or in stand alone applications or systems. This practice creates difficulties for the organization in identifying records classes for accountability purposes, and for its designated preservers in conducting appraisal and preservation activities. It is therefore recommended that policies and procedures be established that require detailed documentations of all business processes contributing to the creation and use of the same records in the

system(s). Procedural manuals with such descriptions are effective in increasing the awareness of the impact of record making and keeping on the management of an organization.

Any appraisal decision should consider all uses of the record and be aware of the business processes behind them. This is necessary in order to make an informed decision about what to preserve, as well as to be able to dispose effectively of all possible copies of the records that have not been selected for preservation.

The use of records or information within records by different business processes may be desirable from the creator's standpoint in terms of providing a degree of interoperability among the creator's information and record systems. In such situations, the preserver should advise the creator that metadata attached to records used by many business processes must identify each relevant business process. This is critical for the creator because it ensures the authenticity of the records by establishing their identity and integrity in each context. It is also critical for the preserver who must understand all contexts in which the records were used in order to effectively undertake appraisal and also to meet the baseline requirements for maintaining authenticity for any records acquired into the preservation system.

[C10] Third-party intellectual property rights attached to the creator's records should be explicitly identified and managed in the record-making and recordkeeping systems.

[P8] Third-party intellectual property rights attached to the creator's records should be explicitly identified and managed in the preservation system.

Every organization should realize that the records that it creates or are under its control or custody contain information covered by intellectual property legislation. But it should also be aware that in some cases the intellectual property rights and copyright linked to a record may belong to a party other than the author and addressee.

All intellectual property rights attached to a record need to be documented in the metadata accompanying such record at the time that it is made or received and set aside. Intellectual property issues can significantly influence the reproduction of records, which is central to the processes of refreshing, converting and migrating records for either continuous use or preservation purposes. Subject to variations in different legislative environments, reproductions of records with intellectual property rights and copyrights held by third parties may violate legislation that protects such rights. These issues must be identified and addressed at the stage of designing the record making and keeping systems. In the case of records identified for long-term preservation, long-term clearance of such rights should be addressed explicitly in the organization's policy.

Preservers know that records under records creators' control usually contain information covered by intellectual property legislation. Because records preservation in a digital environment means to reproduce the creator's records and to preserve authentic copies of those records, intellectual property rights and copyright have become an issue for the preserver. It is the preserver's responsibility, first, to advise the creator on how to address intellectual property and copyright issues in its record making and keeping systems, and, second, to ensure that intellectual property and copyright issues are addressed in the design of the preservation system. In particular, any issue relevant to third-party intellectual property rights and copyright should be cleared before the transfer of records to be preserved from the creator to the preserver occurs. The latter must consider these issues as a part of the assessment of feasibility of preservation.

[C11] Privacy rights and obligations attached to the creator's records should be explicitly identified and protected in the record-making and recordkeeping systems.
[P9] Privacy rights and obligations attached to the creator's records should be explicitly identified and protected in the preservation system.

Privacy legislation protects the rights of individuals in terms of both how the organization collecting their personal data may use it and the rights of access to personal data by the individuals to whom the information pertains.

Metadata schemas that note and administer the use of personal information contained within the records must be embedded in record-making and keeping systems. This will enable the protection of personal information through the establishment of system-wide access privileges. In cases where records are to be preserved indefinitely, privacy issues relating to access to records must be expressly resolved, i.e., explicit permissions must be sought from the individuals concerned, ideally prior to record creation. Record policies must establish that the designated preserver of the organization, as a trusted custodian, be given access to records containing personal information in order to perform preservation activities.

Archival processing of personal information for preservation purposes is different from the use of it for research or business purposes. Regardless of the legislative framework, the creator and the preserver should be able to demonstrate that archival processing of records containing personal information does not put such information at risk of unauthorized access. Preservers should also insist that responsibility for processing records containing personal data for preservation purposes must reside with the records creator and its legitimate successors. Contracting out preservation functions to specialized commercial operators

puts at risk the privacy of the data in the records and consequently the ability to obtain permission to process personal information for preservation purposes.

In the case of records that are not yet designated for permanent preservation, appraisal decisions should be taken before the initial mandate for processing personal information has expired, in that the legality of retaining such records may expire.

[C12] Procedures for sharing records across different jurisdictions should be established on the basis of the legal requirements under which the records are created.
[P13] Procedures for providing access to records created in one jurisdiction to users in other jurisdictions should be established on the basis of the legal environment in which the records were created.

Organizations with branches in jurisdictionally separate areas, i.e., areas which are covered by different legislation, must be aware that different access, privacy, and intellectual property laws may have an impact on their records sharing activities. Such sharing activities include records exchanging within the same organization or with outside organizations, such as governments or business partners. The fact that records are freely accessible in one jurisdiction does not imply that they can be accessed in the same way in other jurisdictions. The records creating organization must investigate such issues and address them in their policies. This includes providing records to a trusted preserver, where the latter operates in a separate juridical environment from the organization. Also preservers who are a unit of a record creator (e.g., in-house archival programs or archives) that has geographically separated branches falling under different jurisdictions, and therefore legislation, must be aware of the impact of such diverse legal contexts on their records sharing activities. This would affect access policies relevant to both internal and external sharing activities.

[C13] Reproductions of a record made by the creator in its usual and ordinary course of business and for its purposes and use, as part of its recordkeeping activities, have the same effects of its first created manifestation and each is to be considered at any given time the record of the creator.
[P3] Reproductions of a creator's records made for purposes of preservation by their trusted custodian are authentic copies of the creator's records.

In the digital environment, the first manifestation of a record, be it a draft, an original or a copy, only exists when first composed in the organization's record making system, if it is an internal record, or when first received, if it is transmitted from the outside. When the record

is closed and saved into the making or receiving system, its first manifestation technically disappears as the saving action decomposes it into its digital components. Any later representation of the digital record is a re-production resulting from an assembly of its digital components. Conceptually, however, organizations use the reproduction of the first manifestation as if it were the record first manifestation because it is made in the usual and ordinary course of carrying out business activities and for the purpose of such activities. This also means that each reproduction in sequence has the same admissibility in court as the first manifestation and will be given same weight.

In order to establish that a record is reproduced in the usual and ordinary course of business, it is necessary to set out routine procedures in writing. In effect, if accurate and reliable records have been generated in a trusted record making system and their authenticity has been maintained together with that of the received records in the organization's recordkeeping system, then all records will have the same effects as their first manifestation.

Reproductions of a creator's records for preservation purposes rather than in response to an operational business need are considered authentic copies of the records of the creator because they are never used in their present manifestation for action or reference by the creator itself. The creator's records and their authentic copies are the same records, but at a different phase in their lifecycle and thus at a different state of transmission. The former are used by their creator to achieve business goals, while the latter are made by the preservers for preservation purposes.

Copies of records in the preserver's preservation system may not be designated authentic if the preserver has made them for purposes other than preservation; for example, an imitative copy or a simple copy from which personal identifiers are removed may be made for access purposes. Ultimately, only the preserver has the authority to designate a copy as authentic.

This framework of principles will be much more understandable and useful if read in its complete version and in conjunction with all the other documents resulting from InterPARES research, especially the final reports of the research teams, which will be soon available on the InterPARES website. Thus, stay tuned…