

ELECTRONIC ARCHIVING OF PAPER ORIGINALS

Legal Framework for Electronic Archiving

Although some countries require certain types of documents to be kept and archived in their original paper form, for most categories of documents, including HR-related records, there is no such requirement, and it is generally acceptable to use electronic versions of paper records (i.e., scanned copies of paper originals) during most government agencies' inspections and audits or in court proceedings.



The evidential or probative value of electronic versions of paper records may be more easily challenged before a court than it would be for the originals. This is mainly because the original records could be tampered with or changed before being scanned, and,

unless proper technology has been used (e.g., encryption and timestamping), it may not be easy to detect such changes from a scanned copy. In specific situations, it may be good practice for employers to retain archives of paper originals in the event such originals would be requested by a specific investigator, auditor, judge or authority.

Are electronic scanned copies of paper originals legally valid?

Effective September 20, 2019, Law 13.874/2019, known as the Economic Freedom Act, modified a few bodies of law relating to creating and storing

documents electronically. Additional regulations will be issued by Brazil's Federal Government.

Under the new rules, it is the right of any person essential to the economic development and growth of Brazil to archive documents via microfilm to digital means. If the digitization is completed in accordance with the requirements established by the regulations, the electronically scanned copy will be considered to have equal value to the physical document.

Private documents can use any means to prove whether the authorship, integrity, and, confidentiality (if applicable) of an electronic document is valid. Note that all involved parties must agree, the document must be accepted by the individual against whom the record applies, or, regardless of the individual's acceptance, the digitization of the document used a Digital Certificate.

Law 12.682/2012 (as amended) sets specific procedures to create and store documents electronically. New digitization rules include that:

- Private and public documents can be stored in electronic, optical or equivalent form, composed of data or images (as long as all applicable laws are followed).
- Once the integrity of a digitized document has been verified, based on the requirements in the regulation, the original can be destroyed (unless the document is of historical value).



- The digital document and its copy, which has been created in accordance with the Law and related legislation, will have the same evidential value as the original document.
- Electronically stored documents can be deleted after the end of the relevant prescription period.
- Digital documents that have a mechanism to be authenticated and a mechanism to verify the integrity in a manner/technique defined by the market, can be reproduced in paper or other physical medium. The employer would be responsible for showing that integrity and authentication requirements are met.
- The process to digitize public documents must maintain the integrity, authenticity and, when applicable, the confidentiality of the digital document, with the use of a digital certificate issued under the Brazilian Public Key Infrastructure - ICP - Brazil.

Are there any legal requirements for electronic archiving systems (EAS)?

Electronic archiving systems should protect documents from unauthorized access, use,

alteration, reproduction, and destruction. In addition, minimum system requirements include the ability to:

- guarantee the preservation and reliability of records;
- retrieve and access records;
- index the location of records; and,
- verify each step that was used to create a scanned record.



HR Best Practices:

The Economic Freedom Act and recent modifications to existing laws will likely enable

employers to use more electronic records, provided that required procedures and certifications are complied with.

Last updated December 2020.

DISCLAIMER: The information contained in this form is for general information purposes only and is not intended to be a source for legal, or any other advice and should not be relied upon as such. This information is not intended to create, and the receipt of it by the reader does not constitute, an attorney-client relationship. Organizations or individuals receiving this document should always seek the advice of competent counsel in their home jurisdiction. Laws may change and The Ultimate Software Group, Inc. cannot guarantee that all the information in this form is current or correct. THE ULTIMATE SOFTWARE GROUP, INC. MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR CONTENT AND SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES INCLUDING BUT NOT LIMITED TO ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY, OR COMPLETENESS OF THIS INFORMATION. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER THE ULTIMATE SOFTWARE GROUP, INC., NOR ITS AGENTS, OFFICERS, EMPLOYEES, SUBSIDIARIES, OR AFFILIATES, ARE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE OR PROFITS, OR BUSINESS INTERRUPTION), EVEN IF THE ULTIMATE SOFTWARE GROUP, INC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT, ARISING IN ANY WAY OUT OF THE USE OF OR INABILITY TO USE THIS INFORMATION. This document and the content are proprietary and confidential information of The Ultimate Software Group, Inc. No part of this document or content may be reproduced in any form or distributed to any third party without the written consent of The Ultimate Software Group, Inc. © 2020 The Ultimate Software Group, Inc. All rights reserved.