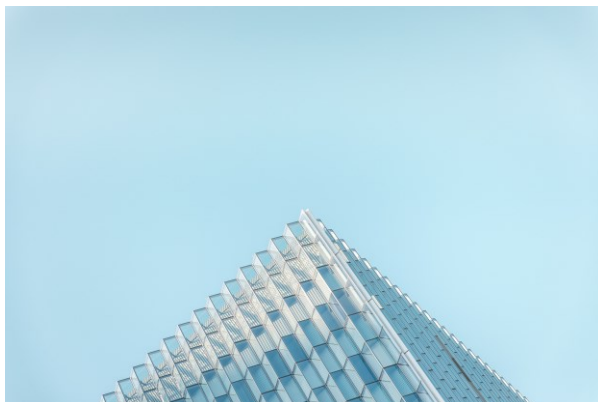


HR Electronic Records – Romania

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?

A scanned document that is intelligible and presents sufficient warranties to establish belief over its content and the identity of the person who has signed it, Romanian courts have interpreted such a document as having been signed by a simple electronic signature (as defined by the eIDAS Regulation). Therefore, subject to the condition of form required for a specific legal act, the document reproduced by a scanned copy will have the following probatory value:

- a) if the scanned copy reproduces a document for which written form is required only for ensuring proof of the agreement, the scanned copy will be deemed a commencement of proof in writing (Romanian: “inceput de dovada scrisa”) and may be used in court in correlation with other means of evidence (e.g., witnesses, presumptions) in order to prove the agreement between the parties.
- b) if written form is neither required as a validity nor a probative requirement, the scanned copy is sufficient and no additional methods of proof will

UKG HR COMPLIANCE ASSIST

be necessary. However, any party may require the original to compare it against the scanned copy. If the party invoking it will not be able to provide the original, the scanned copy will only be considered a commencement of proof.

If the scanned copy of the paper original is electronically archived per the requirements of the Electronic Archive Law, the manager of the electronic archive will need to certify the document per the provisions of Art. 7 of the Electronic Archive Law.

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

- According to the Electronic Archive Law, should an entity intend to manage and supervise an electronic archive, it has to be qualified as a manager of the electronic archive (the “Manager”). Alternatively, an entity can rely on an authorized provider of electronic archiving services.
- In order to obtain the status of Manager, the entity has to submit a notification to the Authority for the Digitalization of Romania (“ADR” or “Authority”) at least 30 days before beginning to archive. The notification must be submitted in the form provided in Annex 2 of Order 493/2009.
- Together with the notification, the entity shall submit all the information regarding the safety and preservation procedures used, as well as any other information required by the Authority. Annex 2 of Order 493/2009 indicates a list of documents (mostly related to functional and security requirements to keep the electronic archive in a good way) that the Manager must submit.
- Assuming all legal requirements are met, the Authority will issue an accreditation order, registers the Manager and assigns the Manager with an identification code. A database of authorized Managers is available on the official website of ADR – here.
- As per the provisions of Art. 7 of the Electronic Archive Law, in order to be legally, electronically archived, the document must comply with the following requirements:
 - a) signed by the person who holds the right to dispose of the document (the “Holder”), with an extended electronic signature;
 - b) the electronic signature shall be used within its validity term by the Holder;
 - c) submitted together with the encryption key for the encrypted documents that fall within the scope of the National Archives Law;
 - d) provided together with the information indicated in Art. 8 para. (2) of the Electronic Archive Law; If the document in electronic form was generated by transferring the information from analog to digital media (i.e., scanned copy of the original paper), the following additional information will be also necessary: references to the owner of the original, the location of the original, the transfer method used, and the hardware device and the computer program used.
- Note: The above rules appear to be more relevant where the Manager is different from the Holder of the documents. It is not clear to what extent these requirements would also apply where the Manager of the archive and the Holder of the documents are the same entity (i.e., where say the employer is an electronic archive Manager for its own documents).

UKG HR COMPLIANCE ASSIST

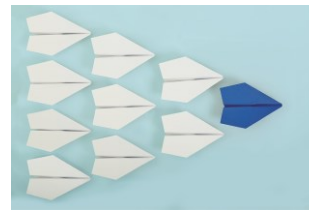
- The Manager must electronically sign all archived documents to certify the fact that the respective document has the same value of original or copy, according to the decision of the Holder.
- The Manager shall register and keep the record of all the documents submitted to the electronic archive, by keeping an electronic registry. Once registered, the content of the document cannot be modified. The Manager shall fill-in an electronic file for each document, including details on the regime of access to the document as established by the Holder, which will be archived separately from the document.
- The Electronic Archive Law also prescribes certain other obligations incumbent upon the Manager. Such obligations are mainly the following:
 - a) to keep the electronic archive in good condition;
 - b) to observe certain safety rules, in order to ensure the integrity, the security and the confidentiality of the archived documents;
 - c) to keep the source code of all programs used for construction and operation of the electronic archive and to submit to the National Archives a copy of the source code of all programs used to build and operate the electronic archive;
 - d) to ensure the display of any archived document;
 - e) to ensure the destruction of any document upon the expiry of the archiving period;
 - f) to ensure financial resources to cover the damages that it could cause during the electronic archiving activities. The insurance modality is established by decision of the Authority.
- g) to notify the Authority, with at least 60 days in advance, on the intention to cease the archiving activities, except for the cases of force majeure.
- The electronic document management system must automatically generate an audit record, in which are recorded, without the possibility of modification, all decisions and actions that occur on a document from the moment of registration and until its destruction or transfer to the National Archives.
- In case of classified documents, additional requirements may apply since the electronic archiving process will comply with Law no. 182/2002 and standards for the protection of classified information.
- Any natural or legal person may benefit from electronic document archiving services. In order to submit a document in the electronic archive, the beneficiary must meet both the established conditions by the provisions of Art. 7 of the Electronic Archive Law, as well as to have a valid qualified digital certificate for the electronic signature used for signing electronic documents stored in the electronic archive and to communicate to the Manager the information necessary to verify the validity.
- Electronic archives are stored in data centers that are subject to a prior authorization by the ADR. In order to receive such an authorization, the data center must prove it complies with a series of technical criteria that ensure: (i) the integrity and security of the electronic documents; (ii) the security and integrity of the space where the equipment

UKG HR COMPLIANCE ASSIST

storing the electronic archive are located; and (iii) the retrieval of information in case of natural disaster, according to the law. The authorization of the Manager is different from the authorization on the data center (see Order 489/2009).

- Employee-related electronic documents may be stored informally. Informal, electronic storage does not need to comply with the Electronic Archive Law (see response to Questions 1 and 4 in the Electronic Records Word Document). If stored informally, the employer is only required to observe the general data protection principles (e.g., data minimization, accuracy, storage limitation, integrity and confidentiality). However, informal, electronic storage does not equate to the electronic storage for archiving purposes according to the Electronic Archive Law.
- The risk with informal archiving is that the probative value of the document decreases. For example, if the written form/wet ink form is a condition of validity and the document is only in electronic form or there is no original written document, the electronic version stored informally can be considered at most a commencement of written proof. On the other hand, if the electronic version of the document was archived in compliance with the Electronic Archive Law, the manager of the electronic archive could certify the electronic document as an original in lieu of the written/wet ink version.
-

As regards to storage in the cloud there are no specific local provisions or guidance, but as long as the documents will also be kept in the form required by the law (e.g., the paper records), as the case may be, the client could also store the electronic records in cloud. In addition, we highlight that from a data protection perspective, if the service cloud provider is a third party, the



client has to ensure that such third party provides sufficient guarantees to implement appropriate technical

and organizational masters so that the processing will meet the requirements of data protection, with the observance of the provisions of Article 28 of GDPR.

HR Best Practices: The full electronic archiving era is approaching, but for now it is not possible to guarantee that all paper documents can be destroyed. Indeed, the acceptance of digital copies remains subject to the discretion of the judge.

Similar to the electronic signature, electronic archiving will probably also develop to a three-level structure: simple, advanced and certified archiving. Over time, this means that certified electronic archiving will make the burden of proof fall under the responsibility of the challenging party.

UKG HR COMPLIANCE ASSIST

Last update: February 2024.

DISCLAIMER: The information contained in this document is for general information purposes only and is not intended to be a source for legal, tax, or any other professional 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. All legal or tax questions or concerns should be directed to your legal counsel or tax consultant. Laws and regulations may change and UKG Inc. ("UKG") cannot guarantee that all the information in this document is accurate, current or complete. UKG MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR THE INFORMATION OR CONTENT CONTAINED HEREIN 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 UKG, 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 UKG 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 UKG. No part of this document or its content may be reproduced in any form, or by any means, or distributed to any third party without the prior written consent of UKG © 2022 UKG Inc. All rights reserved.