

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?

Under Polish law, paper employee records are permitted to be scanned and stored electronically (Act on Amendment of Some Acts in Connection with Shortening the Period of Storage of Employee Files and Their Electronicisation, 2018). Scanned copies of paper originals must include either include an electronic seal from the employer or a qualified electronic signature from an employer-

authorized individual, verifying that the content matches that of the paper original. If records are migrated to an electronic format, employees must be informed of the change and given 30 days to collect the original record prior to the employer being allowed to destroy the original record. If the employee is dead, certain family members have the right to pick up the document (Labor Code, Art. 94).

Note that according to the Polish Accounting Act (Art. 73, item 1), accounting and inventory documents should be stored in their original form, i.e. if these documents are natively electronic they should be stored in the same form.

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

Employers are able to choose whether to keep a paper or electronic archive of employee documents. The basic requirements stipulate that both forms will need to have the characteristics of confidentiality, integrity, completeness and availability in conditions that do not damage or destroy the documents (Labor Code, Art. 94, item 9b).

The Regulation of the Minister of Family, Labor and Social Policy on employee documentation of December 10, 2018 (par. 9-12), sets detailed requirements for securing electronic records. The Regulation requires that electronically archived employee records are kept and stored in an IT system that:

- protects the record from damage, loss and unauthorized access;



- maintains the integrity of the record and metadata (i.e., prevents changes to the record unless the changes are part of an established and documented process);
- ensures that authorized individuals have permanent access to documentation;
- can identify which individuals have access to records and, tracks changes and metadata made by these individuals;
- allows the records to be effectively searched using metadata referred to in the details of the Regulation;
- allows issuing records, or parts of the record, in the manner specified in the Regulation including by electronic export; and,
- allows records to be printed.

Electronic records are considered secure if: (a) only authorized individuals can access the records; (b) the files are protected from destruction (both accidental and unauthorized; and, (c) the method and means used to protect the records are widely recognized as being effective.

Employee records should be protected through:

- systematic risk analysis;
- developing and applying procedures to secure the processing of documents and systems (including access, backup and storage procedures);

- applying adequate security measures to protect records from threats;
- ongoing monitoring of organizational and technical IT methods used to protect employee records, including periodically assessing the effectiveness of these methods; and,
- preparing for long term storage of records, including implementing plans for future transfers to new systems and data formats while ensuring uninterrupted access.

If a paper record must be attached to a preexisting electronic record, the employer (or representative) should make a digital copy of the paper document and add the employer's qualified electronic signature or seal. The record should then be added to the employee file in a manner that ensures legibility, access and consistency.



HR Best Practices:

When electronically archiving employee data in Poland, use technical solutions that ensure the

continued availability, usability and reliability of employee documents, at least until the record retention period expires.

Last updated January 2021.

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 © 2021 UKG Inc. All rights reserved.