

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?

While Denmark does not have a specific law relating to electronic archiving of paper originals for private individuals or legal persons, the Danish IT Security Council created guidelines

based on legislation and case law in 1999. "It is the opinion of the Council that an organisation that follows the guidelines will generally be able to produce evidence for the content of a digital document (authenticity and integrity). The level of security outlined in the guidelines should be sufficient for most organisations."¹

In other words, scanned copies of paper documents are legally valid and may be presented as evidence if the validity of the record



can be proven through an assessment appropriate to the situation. In order to use a digitized record of a paper original, organizations should be able to prove that the content of the digital version is identical to the original.

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

While there aren't specific legal requirements in the GDPR or in the Data Protection Act relating to archiving systems, there are a number of factors to take into consideration, such as:

- separating duties and functions relating to digital document management (i.e. one person/team shouldn't be controlling the whole process);
- implementing technical security measures (such as preventing unauthorized access, safeguarding against data loss/corruption and ensuring availability);
- implementing archive management practices (the records should be searchable, etc.);

¹ 2013. "Digital Documents – the Weight of Evidence." *Ministry of Higher Education and Science*. June 18. Accessed January 29, 2018. <https://ufm.dk/en/publications/1999/digital-documents-the-weight-of-evidence?searchterm=it%20security>.

- ensuring the quality of a scanned document so data is not lost;
- logging records to create an audit trail (including date/time stamps, the I.D. of the scanning operator, document number, etc.) and filing records in a secure, non-erasable system;
- systematically testing scanning and filing processes to ensure quality;
- determining a rescanning process (i.e. who can rescan records and under what conditions documents should be rescanned);
- verifying the authenticity of a document prior to scanning;
- ensuring the integrity and maintenance of the document management system (including back-ups);
- determining when documents can be shredded and when paper originals should be maintained; and,
- printing guidelines (i.e. determining how documents can be printed and how authenticity/integrity can be ensured).

In addition, electronic archiving systems must comply with security requirements as outlined in

Article 32 of the General Data Protection Regulation. The Danish Data Protection Agency requires that companies prepare an Article 32 document describing implemented technical and organizational measures. When external IT-providers are used, a data processing agreement should be entered into between the parties (when the external provider is acting as a data processor).



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.

Last updated May 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.