



# HR Electronic Records – Nigeria

## 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.



There is no specific legal or regulatory framework for electronic archiving under Nigerian Law, however, the Evidence (Amendment) Act 2023 (the "Evidence Act") recognizes the use of electronically generated documents as evidence in court provided such electronically generated documents comply with the requirements for admissibility under the Evidence Act .

That said, it is useful to note that certain legislation provides for rules that apply to storage of personal data. These provisions would

generally apply to storage of data regardless of whether such data is stored electronically or otherwise. For example the "Processing" of personal data under the Nigerian Data Protection Act (NDPA) 2023 is defined to mean any operation or set of operations which is performed on personal data , whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria.

While processing personal data, a data controller or processor is required to ensure that the personal data of the data subject is retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed ; and ensure that it is processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach .

In addition to the above, it is useful to note the provisions of the Nigerian Cybercrime (Prohibition, Prevention, ETC) Act (the "Cybercrimes Act") gives the Nigerian President the power (upon recommendation of the National

# UKG HR COMPLIANCE ASSIST

Security Adviser) to designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country as constituting Critical National Information Infrastructure . Pursuant to this, the President is empowered to prescribe minimum standards, guidelines, rules or procedure in respect of the storage or archiving of data or information which has been designated as critical national information infrastructure, amongst other things. We are not aware of instances where this has been effected against private entities however from the wordings of the Law private entities with information relevant for this purpose are not immune from being designated as Critical National Information Infrastructure. That said, in our view, it is unlikely that HR data would fall within the category of information that may be designated as Critical National Information Infrastructure.

## Are electronic scanned copies of paper originals legally valid?

Asides the provisions of the Evidence Act referenced above, currently, the only specific legislation regarding archiving in Nigeria is the National Archives Act 1992, which provides for the establishment of the National Archives of Nigeria as the agency statutorily responsible for maintaining all archives of the Nigerian government.

However, this law does not provide for electronic archiving for private establishments. As such, there is currently no legislation governing this system. However, it is customary for companies to take recourse to the provisions of the Evidence

Act and Notaries Public Act 1936 in determining the validity of electronically generated documents.

That said, it is useful to note that certain legislation provides for rules that apply to storage of personal data. These provisions would generally apply to storage of data regardless of whether such data is stored electronically or otherwise. For example the “Processing” of personal data under the, for example, **“Processing”** of personal data under the Nigerian Data Protection Act (NDPA) 2023 is defined to mean any operation or set of operations which is performed on personal data , whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria. A similar definition is found under the Nigeria Data Protection Regulation 2019 made pursuant to **National Information Technology Development Agency Act 2007 (“NITDA Act”)** is defined which defines **“Processing”** of personal data as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Furthermore, the NITDA has clarified severally that based on the above definition, all requirements under the Data Protection

# UKG HR COMPLIANCE ASSIST

Regulations which applies to processing of data would automatically apply to storage of data.

While processing personal data, a data controller or processor is required to ensure that the personal data of the data subject is retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed ; and ensure that it is processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach .

processed in a fair, lawful and transparent manner;

collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;

adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;

accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed; and

processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach.

In addition to the above, it is useful to note the provisions of the Nigerian Cybercrime

(Prohibition, Prevention, ETC) Act (the “Cybercrimes Act”) gives the Nigerian President the power (upon recommendation of the National Security Adviser) to designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country as constituting Critical National Information Infrastructure . Pursuant to this, the President is empowered to prescribe minimum standards, guidelines, rules or procedure in respect of the storage or archiving of data or information which has been designated as critical national information infrastructure, amongst other things. We are not aware of instances where this has been effected against private entities however from the wordings of the Law private entities with information relevant for this purpose are not immune from being designated as Critical National Information Infrastructure. That said, in our view, it is unlikely that HR data would fall within the category of information that may be designated as Critical National Information Infrastructure

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

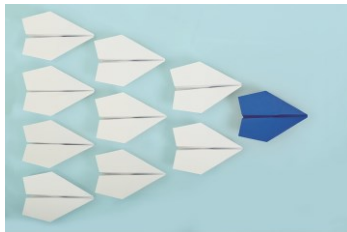
Outside of the National Archives Act, which only applies the Nigerian government agencies, there is no legislation specific to electronic archiving systems. Most companies follow the provisions in the Evidence Act and the Notaries Public Act to determine the validity of documents that have been generated in electronic form.

# UKG HR COMPLIANCE ASSIST

## 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. When scanned documents are used in Nigeria (excluding

evidence in Nigeria's courts or submission to a regulatory authority), the scanned record is generally presumed to have the same value as the original if the record has been certified by the courts or notarized by a notary public.



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.