



Digital Data Protection and Literacy for Ghana's Digital Transformation Initiative: A Case Study of the E-Tax System

Faustina K. Barfi 

UniMAC- Institute of Journalism Ghana
ORCID: [0000-0001-6477-5866](https://orcid.org/0000-0001-6477-5866)

Angela Achiaa Aikins 

University of Development Studies, Ghana
ORCID: [0000-0002-5664-4177](https://orcid.org/0000-0002-5664-4177)

Presented at the Department of Information Studies International Conference on Information Behaviour and Digital Data Literacy in Africa

DOI: <https://doi.org/10.4314/glj.v30i2.7>

Abstract

This study assessed digital data protection strategies and modalities for user support using the Ghana Revenue Authority (GRA) e-tax system as a case study. The community element of the Activity Theory guided the study. The study employed a qualitative research approach; hence, face-to-face key informant interviews and observation were used to gather the data. Purposive sampling was employed to sample three key informants as participants. The data was analysed using thematic analysis. Our findings show that GRA has recently seen a tremendous level of integration with other government agencies. Data generated for use and protection by GRA- include domestic tax, import taxes, tax identification, contracts, property tax and rates, and corporate tax data. The Authority uses a lock icon as an intervention on its website. Using security icons (security padlock and alert icon) helps users manage appropriate authentication credentials and preview updates on security and protection from cyber-attacks. We also found the client's privacy policy, SSL certificate, secure cookies, login authentication, disclaimer alert, compliance with data protection, firewall security intervention, and protocols to validate form input in place to protect user data. However, they did not have a guide to support users, guided solutions on data recovery, and procedures to inform the community of alerts and updates. The Authority uses training, orientation, and social media campaigns to sensitise the community on digital data protection. The subscription to ISO standards readiness certification and the application of data loss prevention initiatives such as two-factor authentication, encryption, and data anonymisation were identified as best practices to improve security for clients using the e-portal platform. To enhance information security culture, our participants stated that the involvement of civil society actors could serve as translators on tax information and facilitate training to support tax literacy. Participants also suggested that resource availability would help increase awareness levels. Therefore, budgetary allocation for awareness and civic education should be made available to the Authority. They also recommended that dedicated content creators and human resources be engaged permanently to manage, create, and update social media platforms and the web portal. Therefore, the way forward is the call for digitally literate citizens as a cultural change and adoption guided by the community of practice initiative. Intensifying education, training, advocacy, and upskilling digital skills in data protection initiatives by collaborating with and engaging civil actors is imminent.

Keywords: Data protection, digital literacy, ethical concerns, digital transformation, e-tax system.

Introduction

The rapid evolution of Africa's digital landscape has led to the widespread adoption and integration of information and communication technology (ICT) into public administration, governance, and social service delivery. Ghana is no exception to this trend. Like other countries, it is actively pursuing digital transformation, implementing diverse innovations and projects to accelerate government functions' automation and digitising public records and payment platforms. These initiatives leverage shared data infrastructure to enhance Ghana's e-government system. Some government agencies have become interoperable with payment platform enablers. Examples include the National Identification Authority database, which is used for verification for business registration at the Registrar General's Department and integration with the National Health Insurance Scheme and the Ghana Revenue Authority (GRA), among others (Ministry of Communication & World Bank, 2020).

These conscious efforts of transitioning government services from paper formats to digital platforms have generated large volumes of digital data. While the availability of data presents opportunities for collaborative data sharing, improved revenue mobilisation, and enhanced decision making and resource allocation, it also presents numerous challenges relating to managing, curating, and ethically distributing data, data privacy, and safeguarding individual human rights. It is, therefore, crucial to ensure the available digital data is appropriately secured and its credibility maintained to connect people, transact business, and provide verification services for e-government service engagements (Apleni & Smuts, 2020; Verkijika & De Wet, 2018; Tchao et al., 2017). The protection of generated digital data is paramount for e-government systems in this digital transformation era. Therefore, designed digital service platforms must have systems and modalities in place to secure data (Shareef, 2017).

This study assessed digital data protection strategies and modalities for user support using the GRA e-tax system as a case study. The study was guided by the community element of the Activity Theory, which previews it as a beneficiary of systems that improve lifestyles. The GRA e-tax system is an electronic service that allows taxpayers to register, file taxes, and make online payments. GRA's e-tax system aims to enhance efficiency and widen revenue mobilisation coverage and service delivery to citizens through a digitalised transformation system (Ministry

of Communication, 2018). The generated wide range of data such as personal, business data, royalties, company data, levies, financial data, electronic invoices, etc. (Institute for Fiscal Studies, 2023) warrant viable strategies to curate and protect them to build user trust, address ethical concerns, and make data readily available for use (Pasha, 2022; Shareef, 2017).

The electronic tax administration initiative by the GRA requires a community of digitally literate citizens to utilise its digital platform and remain safe. Pasha (2022) recommends that citizens be digitally literate on basic data security tips so they can utilise digital service platforms safely. Digital literacy has, therefore, become a requisite skill that the citizenry needs. Hence, inadequate education and data security awareness could hinder sufficient data protection and usage of digital service platforms. These could lead to loss of data, data infractions, identity theft, cyber risk, mobile bullying, social engineering, information breaches, and underutilisation of digital platforms, among others (Abusamhadana et al., 2021; Thiel, 2020; Koranteng & Adjei, 2018). Unfortunately, awareness creation to achieve optimum utilisation of the created platforms to embrace GRA's digital ecosystem is inadequate among citizens (taxpayers). There is, therefore, the call to intensify education and awareness on data protection, whether personal, government, or business (Opoku, 2020).

Nevertheless, there is a paucity of research on digital data protection mechanisms in Africa. The pace of Ghana's digital transformation should align with the digital literacy skills of its citizens, particularly in terms of their ability to fulfil civic responsibilities, such as paying taxes through the new e-tax system. There are few research findings on best practices to embrace this new order. As a result, there are minimal recommendations and theoretical guidelines, particularly on digital data protection for practitioners in the global southern countries, including Ghana (Thiel, 2020). Therefore, it is essential for a study to explore the digital data protection mechanisms of the GRA e-tax system. This study aims to identify best practices and key activities involved in digital data protection operations and literacy that will help taxpayers securely navigate online tax portals.

Literature review

E-tax system and awareness among community members

Tax payment is the responsibility of individuals, organisations, and businesses toward the nation.

Taxes are levied on one's generated earnings and are mandatory (Mbilla et al., 2020). Governments desire to provide convenient and user-friendly systems to facilitate easy payment of taxes (Solange et al., 2018). Complexity in the tax payment system may lead to non-compliance and non-payment of taxes (Odartey, 2022). These non-compliance and non-payment may be attributed to taxpayers' knowledge about the procedure of paying taxes, as Opoku (2020) reported, that tax complexity influences the level of tax knowledge.

Integrating information technology to automate the filing and payment of taxes reduces the burden associated with traditional payment systems (Salange et al., 2018). Implementing electronic taxation in some countries, like Zambia and Tanzania, resulted in significant improvement in tax collection as taxpayers perceived it as helpful, easy to use, and secure (Soneka & Phiri, 2019). The findings of Soneka and Phiri (2019) are consistent with the United Nations Economic Commission for Africa (2019) opinion, where they predicted that introducing e-tax would lead to improved tax revenue mobilisation. E-tax makes it relatively convenient for taxpayers to honour their tax obligations and enhances efficient mobilisation and monitoring of revenue collection. Rwanda's tax revenue generation increased by 6% due to the implementation of electronic taxation (United Nations Economic Commission for Africa, 2019). This implies that using digital technology to collect taxes significantly contributes to efficiency in revenue generation.

Regardless of the benefits that come with the implementation of electronic taxation, some taxpayers have not fully embraced it. For instance, the data leakage on Albania's e-government system discouraged citizens from using the system due to a breach of trust (Pasha, 2022). The study by Soneka and Phiri (2019) conducted in Zambia revealed that although most of their participants have adopted the country's e-tax system, a few still perceived e-tax systems as not user-friendly and secure. The study by Opoku (2020) revealed that a lack of education is one of the significant barriers to adopting Ghana's electronic tax payment system. The study recommended intensified tax education through workshops and awareness programs to improve taxpayers' knowledge.

This implies that creating intense awareness is needed to increase e-tax adoption. The level of awareness of intended users of any technological/digital system directly influences the adoption and

use of that particular technology. However, the level of users' awareness is also influenced by certain factors, such as the information the users are exposed to (Kashada, 2016). It can, therefore, be concluded taxpayers' awareness plays a significant role in the successful implementation of e-tax systems. In addition to facilitating taxpayers' understanding and usage of any digital platform, it also enhances the overall effectiveness of the tax administration. The creation of awareness does not only improve the knowledge and usage of the system but also contributes to the overall effectiveness of the tax administration.

Digital Literacy

Digital literacy is the application of cognitive and technical skills to find, evaluate, create, and communicate information using information and communication technology (Project New Yorker, 2024). Machin-Mastromatteo (2021) also explained digital literacy as the ability of an individual to successfully utilise information and communications technologies (ICT) and interact with digital information ecosystems. The study of Kabakus et al. (2023), which investigated the influence of digital literacy on the adoption and use of digital technology by administrative staff, found that digital literacy affects their intention to use digital technology. Digital literacy has become an integral part of successfully adopting new technology. However, digital literacy among taxpayers seems to be neglected. Incorporating technology into taxation systems can be a hurdle for taxpayers (Rukundo, 2020). It is, therefore, imperative for a country to ensure that expanded digital skills training is aligned with the evolution of ICT integration into government service delivery, including taxation. A key aspect of digital literacy is having a digital citizenry that has the capacity to manage and ethically use digital information while considering issues related to privacy, security, and digital rights. Although digital literacy is crucial to adopting and using the e-tax system, this can be impeded by several factors, such as the digital divide and security and privacy concerns. It is, therefore, crucial that the citizenry, particularly those with low digital literacy skills, be enlightened through awareness creation and other training channels to enable mass adoption and use of the e-tax system. Thus, a more educated population with digital capabilities can better manage and understand their taxes (Madunezim et al., 2024).

Digital data protection and privacy

Safeguarding taxpayer information in electronic tax systems is essential for ensuring transparency and accountability in the taxation process. It is also critical as protecting the taxpayers' sensitive information is a crucial component of tax governance and adoption of the tax system (Aidonojie, 2024). This includes data protection and privacy. To analyse whether the exchange of information complies with data protection safeguards, it is necessary to first look at the exact scope of the exchange of information. In the last decade, information relevant to tax assessment has not only been exchanged on request, but spontaneous and automatic exchange of information has become more popular (Wöhrer, 2018). Protecting data and the privacy of taxpayers is crucial in e-tax systems (Dabah, 2024). Safeguarding information and maintaining the trust of taxpayers are determined by several factors. These factors include the provision of strong cryptographic algorithms and secure key management practices employed at various levels, including applications, databases, and data transmission, to promote data protection and privacy (Dabah, 2024). Strong Identity and Access Management (IAM) policies can aid in user authentication and authorisation (Dabah, 2024; Koren, 2023). This can be achieved by following strict password policies, using Multi-Factor Authentication (MFA), and regularly rotating Application Programming Interface (API) keys and passwords (Dabah, 2024). Only individuals with appropriate identification and authorisation can access confidential information under IAM (Koren, 2023). Organisations, including GRA, should aim to provide the minimum level of access necessary for data protection against unauthorised and authorised disclosure. Regularly reviewing and updating access rights is essential to maintain this principle (Dabah, 2024). The presence of crucial databases and infrastructures for data storage and management should be ensured. A comprehensive Privileged Access Management (PAM) program can involve identifying and tracking privileged user sessions, utilising robust authentication methods, and employing a zero-trust approach to verify identity and access requests without exception (Koren, 2023).

Studies have shown that users of a technological system appreciate their digital privacy. They are cautious about protecting their data and are self-initiative about learning about digital privacy. However, their knowledge about digital privacy is not comprehensive and uniform, nor are their strategies for digital privacy

protection (Katavic et al., 2023). Katavic et al. (2023) also showed that 65% of participants would like to receive additional education on digital privacy (Katavic et al., 2023).

Digital data sources

The sources of data for governance vary (Thiel, 2020). Such data include biometric data, identification data, civil registration records, electoral voting records, health data, financial data, government publications, records on migrants, Memorandum of Understanding (MoUs), and other documents. Literature has revealed biometric identification data, health records, civil registration records, government publication, e-payroll records, e-commerce data, contracts, data on suppliers, tenders, MoUs, public institutional reports, property registration records, legislative data from parliamentary proceedings, tax identification records, financial data, records on business registration, records on drivers and vehicle licensing registration, legislative reports, records on migrants, database on schools among others call for protection (National Information Technology Agency, 2017). These and many more are some of the data generated for e-government services and operations in Ghana. Corroborating on the above, the 2020-2030 Digital Transformation Strategy for Africa enshrined the need for the development of digital ID and the protection of data as foundation pillars to guide a coordinated digitalisation agenda, enhance synergies, and avoid duplication of effort by the African Union (AU) Member States (AU, 2020).

According to the National Information Technology Agency (2017), these data are interoperable in harnessing electronic collaboration and the exchange of information between Ministries, Departments, and Agencies (MDAs) using metadata standards that conform to the Dublin Core Metadata element set. The standards aim to describe internet resources that aid in the discovery and interoperability of information exchange. Such basic elements include creator, title, date, subject, identifier, etc. Again, using these standards facilitates searching, classification, categorisation and retrieval of information, which serves as a catalogue of interoperable systems.

Theoretical Framework: Activity Theory

The Activity Theory has evolved and expanded with elements that result in coordinated actions. It resonates with interaction among instruments, subjects, objects, rules, division of labour and the community within which an activity is accomplished

(Helander et al., 2020). The community encompasses citizens, stakeholders, interest groups, and civil society utilising the system. Another element is the instrument, which connotes tools and applications. The third element refers to rules connoting guiding principles, standards, conventions, and policies on the use of the system. Examples include digital data policies, data recovery plans, compliance with ISO standards, metadata standards, etc. The Subject is the fourth element representing human capacity, skills, knowledge, expertise, and experience that utilise and apply rules, engage the community, division of labour, and instruments to accomplish a task. The subjects are people with technical knowledge of how to execute and implement data security interventions (Helander et al., 2020). Division of labour is another element that signifies the segmentation of roles, operations, techniques, and activities. Lastly, the object is described as digital data that drives the activity. This study focuses on the community element deemed as the beneficiary of the system. Among the digital transformation initiatives in Ghana is the e-tax system, which requires a digitally literate community to be able to fully embrace it. Whereas upskilling the digital skills of the citizenry is endorsed, identifying avenues that foster awareness and education to promote the ethical use of the system is commended. Several factors, including the digital divide and maintaining the pace of technological development, may impede the usage of a technological system (Madunezim et al., 2024). Therefore, it is crucial that the citizenry, through awareness creation and other training channels, is equipped with digital literacy skills to fully embrace the e-tax system.

Research Methodology

This study employed a qualitative research approach, utilizing a case study design to gain an in-depth understanding of participants' awareness, attitudes, beliefs, practices, and foresight regarding the varying digital data sources in GRA's e-transformation project. Case studies are particularly suitable as most e-government interventions are implemented in phases; thus this design allows for a holistic and in-depth investigation of the phenomenon (Norander & Brandhorst, 2017).

Data collection for this study was conducted using a triangulation approach, incorporating a Semi-Structured Interview guide and non-participant website observation techniques. The semi-structured interview guide, informed by the Community element of Activity

Theory, was used to inform the design of the interview guide. The interviews were conducted face-to-face to ensure clarity, engagement, and the opportunity for follow-up questions. The study population was staff of the GRA. GRA was selected because it is among the government's digital transformation functionalities that have advanced in the automation of its operations. GRA is also responsible for the e-tax system in Ghana. As part of its e-transformation pursuit, it has provided online portals where taxpayers can file and pay taxes via an online payment system, which warrants trust, data privacy, and guaranteed online security. Three participants were purposively selected: a project manager, a technical officer, and a key stakeholder informant (system end-user). The purposive sampling technique was most appropriate as it permitted the researchers to recruit participants who, based on their role in GRA's digital transformation agenda, could provide rich insights into the study (Polit & Beck, 2014). The system's end-user was also necessary to obtain valuable insight and feedback about GRA's system. It is important to note that the depth and richness of the data collected are often more important in qualitative research than the number of respondents. It is important to note that the depth and richness of the data collected are often more important in qualitative research than the number of participants. Therefore, the three participants could provide valuable insights for a narrow case study like this. The key questions explored included: What are the sources and available digital data for protection? What are some of the data protection assessment indicators that inform best practices? What activities and data protection cultures can be embraced to improve digital literacy?

In employing the non-participant observation, the researchers employed content analysis of GRA's website to examine online support initiatives that enable taxpayers to access e-tax services securely. Observations were guided by predetermined ISO 27001 security standards and Sen's (2024) security checklist. The focus was evaluating the website's functionalities supporting e-tax services and security measures ensuring privacy and trust in online transactions.

Participants provided informed consent before engaging in the study. To ensure confidentiality, no identifiable personal information was reported. The study prioritized data integrity and accuracy, maintaining a rigorous approach to research.

Data analysis

The researchers subjected the gathered data to two major analyses: thematic and content analysis. The data from interviews were transcribed and subjected to thematic analysis, identifying recurring patterns and themes related to digital literacy, sources of data clients, data protection measures, and user engagement. Data was transcribed, and codes were developed from key responses and categorized under major themes. This was done manually using Excel. The thematic analysis was guided by the six steps of the proposed thematic analysis by Xu and Zammit (2020): familiarisation with data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. The deduced themes and patterns were triangulated with content analysis from the GRA website.

Study findings

GRA digital transformation initiative and interoperability

The researchers investigated participants' understanding of digital transformation for Ghana's taxation system. It was discovered that the integration of Information Communication Technology to manage the operations of GRA's tax services encompasses activities such as digitisation of records, online payment, verification using electronic identity system, data interoperability, digitalisation, interconnection of the public sector and paperless way of delivering services to citizens (Participant 1 & 2). It was uncovered that there had been some interoperability interventions among government functionaries regarding shared data and payment platforms. "The Ghana Revenue Authority (GRA) before 2021 had a data silo system where one system was not necessarily integrated into another internally and externally. For example, the Registrar Generals Department was not integrated, and data were managed on different platforms. There is now an improvement in the interoperability of data sharing among functionaries. Presently, the Registrar Generals Department, the National Identification Authority, the Ministry of Finance, the Public Procurement Authority, and the GRA are integrated" (Participant 1). Participants also acknowledged GRA's digital transformation initiative yielding some benefits, including improvement in revenue mobilisation, social inclusion, resource allocation, effective decision-making, and delivery of remote access services. Overall, the participants of the study affirmed that GRA's digital transformation has

been successful.

Sources and available data for use and protection

The sources and available data for protection identified were civil data such as tax identification records, data on companies, contracts, reports, financial data, invoices, etc. A study of GRA's website showed that GRA provides a range of services electronically, implying GRA has records (digital data) on all these services. The researchers found that the data generated by GRA were on domestic tax, import taxes, tax identification, awarding of contracts, property tax and rates, and corporate tax amongst others.

Digital data protection mechanisms

The study discovered that the Authority hosts its data centre and operates a centralised data architecture system deploying ICT networks to connect across the country. It also has a backup storage, which serves as a recovery site. Access management, data loss prevention, firewall, backup, encryption, secure parameters, and access control were mentioned by participants 1 & 2. Also, data anonymisation, data masking, data exchange infrastructure, application data interface, and real-time vulnerability assessment were identified as mechanisms to protect data. All participants pointed to taxpayers' role in protecting usernames, passwords, and information on ID cards for online payment. Participant 2 indicated that some of the data protection measures instituted by GRA also address ethical concerns, such as trust, citizens' confidentiality to use the system, as well as privacy and the integrity of data.

Digital data security indicators to inform best practice

The researchers inquired if GRA subscribes to any data standard, such as International Organization for Standardization (ISO) standards for data security. Participant 1 attested, "Yes. we subscribe to the ISO data standard and the Data Protection Act of Ghana Data Protection Authority to conform to local and international standards". Extracts from the content analysis as part of the data collection method espoused the checklist of the ISO 27001 standard (2022). The study also observed and applied indicators of other websites on best practices applicable to secure a website (Sen, 2024) by triangulating with the GRA's sites. Findings discovered the under-listed (Table 1) on the Authority's website as security indicators. These indicators guarantee integrity on website use and data

transverse purposes. Participant 3 attested that using the online portal is convenient, and using the Ghana card and password, I can sign on at any time.

Table 1: GRA's website security checklist

Critical questions	Findings	Remarks
Is there a client's privacy policy in place	Yes	Protect reputation
Are there lock icons	Yes	To prevent defacement and vulnerability exploits
Is there an SSL certificate in place	Yes	Stay on top of expiration and trust (allows for pop-up warning to Authority)
Are there secure cookies	Yes	Aid in tracking information about a user's browsing session and history
Any login authentication format	Yes	Require a username and password to safeguard personal login account
Any user guide to support users	No	Provide specific, quick, and easy instructions on the features and conditions of use of the website
Any disclaimer alert	Yes	Protect the reputation of the service provider
Any guide on compliance with data protection	Yes	Users are preview to compliance policies and standards the Authority subscribes to
Any guided solutions on data recovery	No	To prevent or track data
Is there any firewall security intervention	Yes	Prevent automated attacks
Any protocols observed to validate form input	Yes	Allows user input to be validated before storing on the system
Are there procedures in place to inform the community of alerts and updates	No	No alerts/warnings to users

Digital literacy and user engagement

The researchers also investigated the activities and data protection culture to be embraced to improve digital literacy. Participants 1 & 2 indicated that due to the varied levels of illiteracy, education, and awareness, intensifying digital literacy skills is imminent. This will, in a way, not delay the benefit expected from the digitalization agenda. Awareness on digital data security literacy and personal data protection is for citizens (Participants 1 & 2). Intensifying education on best practices to embrace data protection culture being it on the website, personal data such as usernames and passwords, IDs, tokens, and electronic receipts, is key (Participant 1).

Discussion

GRA digital transformation initiative and interoperability

GRA has seen a recent tremendous level of internal and external integration with other government agencies such as the National Identification Authority, the Registrar Generals Department, the Ministry of Finance, and the Public Procurement Authority, among others. To enable the e-government agenda to materialise hitherto, the e-tax system serves as a one-stop shop for clients. The study found that access to data among GRA subsidiaries has now become real-time. This was confirmed in the statement of Participant 3,

who attested that clients in the comfort of their homes could transact and engage the e-services tax portal to make payments and file taxes, among other services. This finding is consistent with the findings of Salange et al. (2018), who stated that the automation of filing and tax payments reduces stress for clients. This may contribute to increased tax revenue generation, as in Zambia and Tanzania (Soneka & Phiri, 2019).

Sources and available data for use and protection

The sources of data identified require absolute protection as they could lead to loss, data infractions, identity theft, social engineering, and information breaches, as opined by Abusamhadana et al. (2021) and Thiel (2020). The study also revealed that the volume of digital data generated has resulted in a digital data interoperability infrastructure for global engagement with citizens, businesses, governments, and employees. It has promoted shared data infrastructure, collaboration, cyberspace engagements, improved efficiency, simplified administration, reengineered workflow, and digital transactions within the Ghanaian Public Sector.

Digital data protection mechanisms

The Authority practiced backup and storage on data recovery sites to safeguard data. Notable best practices discovered also included data loss prevention, firewall application, encryption, secure parameters, and access control. Other mechanisms practiced were data anonymisation, data masking, data exchange infrastructure, application data interface, and real-time vulnerability assessment. This corroborated the findings of Shareef (2017) and Pasha (2022) regarding the recommendations to secure data and Albania's e-government system, respectively. Data protection has become a human rights issue, according to the African Union, which requires collaborative effort on the part of citizens and institutions providing the services (African Union, 2022).

Digital data security indicators to guarantee integrity

The study evaluated the security measures enshrined in GRA's website to secure generated digital data. This evaluation was guided by the ISO 27001 standard for site security checklist and recommended checklist by Sen (2024). Following ISO 27001, a company security policy is identified as being meant to harden and increase the resiliency of one's website. The security checklists recommended by Sen (2024) focus on improving website privacy by protecting its

data from impersonation, hacking, port scans, social engineering, cyberattacks, traffic sniffers, and data miners. Table 1 presents the findings from the GRA's website for security measures provided to protect the digital data of its users. From Table 1, GRA's website had most of the recommended security checklists. Security recommendations on GRA's website are necessary to secure information such as usernames and passwords, download and upload documents, and exchange data with other platforms. However, some of the recommended checklists were not present. These include a user guide, data recovery guide, and procedural guide to inform the community of alerts and updates (Table 1). The researchers found these findings to be interesting as the absence of, for instance, a user guide, which is meant to provide quick and easy instructions on the features and conditions of use of the website, was not made readily available to users. According to Rukundo (2020), the absence of these features may negatively influence the adoption and usability of GRA's electronic tax system. It is, therefore, of the essence that GRA clients be previewed for data security interventions to gain their confidence, guaranteed privacy, and trust. The study discovered the lock icon as an intervention on the Authority's website and other interventions.

Security icons help users manage appropriate authentication credentials, preview updates on security, and protection from cyberattacks. Figures 1 and 2 are examples of security icons discovered on GRA's website. An icon such as the security padlock (Figure 1) signifies that the site is secured with a digital certificate. The alert icon (Figure 2) indicates a warning or the appearance of an error to users (Yamagishi & Fujii, 2024). Yamagishi and Fujii (2024) echoed education on information security to deepen users' understanding. The presence of these icons enables easy navigation of the site and strengthens security. Table 1 highlights other interventions integrated to enhance security at the Authority's site.



Figure 1: Lock Icon



Figure 2: Alert Icon

Digital literacy and user engagement

The study discovered the Authority's website as a major channel to enlighten citizens about data protection initiatives. Unfortunately, GRA does not actively use other social media handles for such purpose. Le al et. (2022), however, recommends using live chat, podcasts, blogs, chatbots, video chats, and web calling to deliver digital data protection initiatives to users. This is because online social networking tools serve as a cheaper way to engage the community and is suitable where resources are limited.

Organisational structures and commitments in place to sensitise the community on the protection of digital data

The study elicited some commitment from the GRA to sensitise the community on measures to protect data. Training, orientation, and social media channels were identified. The study discovered other measures, such as technology and real-time vulnerability assessment, from the interview, to identify risks and areas that informed security resilience. The subscription to ISO standards readiness certification and the application of data loss prevention initiatives such as two-factor authentication, encryption, and data anonymisation are identified as best practices that improve security for clients to use the e-portal platform. Rahman (2010) proposal on strategic communications to engage stakeholders on tax reform pointed to the application of robust systems and portals in this digital era and the extensive level of literacy on the part of the community.

Cultural intervention that impacts activities to protect data

Education, training, and awareness creation were interventions being practiced to impact the protection of data by the Authority. Another intervention Uden and Mustapha (2011) recommended is the initiative of the community of practice (CoP) encapsulated in the activity theory concept as a community, which focuses on social and cultural change and adoption where tacit knowledge sharing becomes easy. The CoP plays a crucial role in implementing reforms. The community of practice contextualises situated learning where practitioners, knowledge producers, and policy processes address a phenomenon. Zondiros (2008) corroborated the CoP as an approach for engaging people in knowledge sharing, organisational change, and reforms using systems and how people understand

such systems. The findings of a study by Boogaard et al. (2022) on strengthening taxpayer engagement identified radio, television, community associations, social media, WhatsApp groups, SMS and door-to-door education as mediums of communication to enhance citizens awareness. The community association connotes the community of practice where citizenry shall be segmented based on varied literacy gaps to educate them.

How can information security culture be improved?

The website was discovered to be a notable channel used to promote awareness of e-services with few highlights on data protection and security alerts. Boogaard et al. (2022) opined to engage taxpayers through forums, education, and dialogue. The use of civil society actors was identified to serve as translators of tax information and trainers to support tax literacy. Another channel underscored to improve information security culture among citizens on social change programs aimed at addressing social gaps is the community of practice. Other countries practice this advocacy channel to promote tax education. Bahar (2022) opined on the adoption of a community of practice initiative by tax professionals in Malaysia to address the educational gap. The study also pointed to CoP as a method to communicate knowledge among the tax community in Malaysia. Whereas periodic changes to tax laws and budgets are inevitable, continuous education among various parties such as the Ministry of Finance, tax associations, academicians, and other professionals was recommended. Identifying the targeted audience using the CoP lenses was commended. Boogaard et al. (2022) corroborated on community of practice as a concept to promote knowledge of the tax system and education on data protection. They describe a community as a target audience where platforms are created to share ideas on data security to support citizenry understanding, adoption, and best practices on social reforms.

Resources required to intensify awareness creation

It was deduced from the interview that budgetary allocation on awareness and civic education was minimal and ought to be widened. Utilisation of dedicated social media platforms to roll out literacy programmes. Content creators, visualization skills, and dedicated human resources were commended to manage, create, and update social media platforms and web portals. It was also discovered that enhanced collaboration among government agencies to invest

in citizen education on basic digital literacy skills was laudable. Finally, commitment from heads of institutions and support services from the local media organisations and the National Commission for Civic Education is commended.

Conclusion and recommendations

The various sources and available digital data for use and protection have yielded data interoperability infrastructure for global engagement with citizens, businesses, governments, and employees that guarantee secure digital platforms to boost citizens' privacy, integrity, and trust. Guided by the ISO checklist for site security, outlined some criteria to improve the resilience of the Authority's site, such as the use of security icons, for example, the lock icon, login authentication, use of secure cookies, privacy policy, protocols observed to validate form input among others, disclaimer, etc. The delivery channels of digital data protection initiatives for the e-tax system commended were website, live chat, podcast, blogs, chatbots, video chats, and web calling. Training, orientation, intensified social media engagements, and awareness creation were some organisational structures and commitments in place to sensitise the community to protect digital data. Others included subscription to ISO standards readiness certification and the application of data loss prevention initiatives such as encryption and data anonymisation. Other commitments and channels discovered were the community of practice (CoP) initiative, door-to-door education, radio, television, community associations, social media, WhatsApp groups, and SMS alerts to improve the information security culture of citizens.

The community subscription to digital security interventions is detrimental and largely depends on users' understanding and education on such interventions. The findings showed that GRA has most security interventions in place; however, users' understanding of its use was low. The envisioned digital transformation agenda for Ghanaians is gradually unfolding as it is practised in the global north. Therefore, a call for digitally literate citizens is the way forward. Intensifying education, training, advocacy, and upskilling digital skills on data protection initiatives is imminent. The study recommends that a user guide that will espouse digital literacy through manuals, video, audio, and flyers by segmenting the varied literacy groups to address them and data recovery procedures are made available to users. We anticipate these will increase the adoption rate and

reduce the risk of data abuse.

References

- Abusamhadana, G. O., Bakon, A. K. & Elias, N. F. (2021). E-government in Ghana: the benefits and challenges. *Asia-Pacific Journal of Information Technology & Multimedia*, 10(1): 124-140. DOI: <https://doi.org/10.17576/apjitm-2021-1001-11>
- African Union. (2020). The digital transformation strategy for Africa (2020-2030). Available: <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>.
- African Union (2022) Au Data Policy Framework. <https://au.int/sites/default/files/documents/42078-doc-data-policy-framework-2024-ENG-V2.pdf>
- Aidonojie, P. A., Majekodunmi, T. A., Eregbuonye, O., & Ogbemudia, I. O. (2024). Legal issues concerning of data security and privacy in automated income tax systems in Nigeria. *Hang Tuah Law Journal*, 8(1), 14–41. <https://doi.org/10.30649/htlj.v8i1.223>
- Apleni, A. & Smuts, H. (2020). An e-government implementation framework: a developing country case study. In *Responsible Design, Implementation & Use of Information & Communication Technology*. M. Hattingh. Proceedings Part II, 12067of 19th IFIP WG 6.11: Conference on e-Business, e-Services, & e-Society, I3E 2020. April 6–8, 2020. Skukuza, South Africa: 15–27. DOI: https://doi.org/10.1007/978-3-030-45002-1_2.
- Boogaard, V. D., Prichard, W., Beach, R., & Mohiuddin, F. (2022). Enabling tax bargaining: Supporting more meaningful tax transparency and taxpayer engagement in Ghana and Sierra Leone. *Development Policy Review*, 40(1), 1-22. DOI: 10.1111/dpr.12563
- Dabah, G. (2024, March 14). How to protect personally identifiable information: PII security best practices. Piiano Blog. <https://www.piiano.com/blog/pii-security-best-practices>
- Helander, N., Jussila, J., Bal, A., Sillanpää, V., Paunu, A., Ammirato, S., & Felicetti, A. (2020). Co-creating digital government service: An activity theory perspective. *Hawaii International Conference on System Sciences*. Proceedings of the 53rd Hawaii International Conference on System Sciences. <https://hdl.handle.net/10125/64002>
- ISO. (2022). Information security, cybersecurity and privacy protection. ISO/IEC 27001:2022. <https://>

- www.iso.org/standard/27001.
- Institute for Fiscal Studies Ministry of Finance, Ghana (2023) A survey of the Ghanaian tax system. www.mofep.gov.gh/sites/default/files/reports/revenue/SGTSUpdate_Mar2024_v2.pdf
- Kabakus, A. K., Bahçekapili, E., & Ayaz, A. (2023). The effect of digital literacy on technology acceptance: An evaluation on administrative staff in higher education. *Journal of Information Science*, 01655515231160028.
- Kashada, A., Li, H., & Kashadah, O. (2016). The Impact of User Awareness on Successful Adoption of Decision Support System DSS in Developing Countries: The Context of Libyan Higher Education Ministry. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 16(1), 334-345.
- Katavić, S. S., Ivanović, H., & Papić, A. (2023). Digital Privacy and Data Protection Knowledge and Skills of University Students in Croatia: Preliminary Findings. *Education for Information*, 39(4), 493-515. <https://doi.org/10.3233/EFI-230056>
- Koranteng, A.K. & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*. 20(2): 150-161. DOI: <https://doi.org/10.1108/FS-08-2017-0043>.
- Le Van, H., Maor, D. & McConney, A. (2022). The potential of social networking sites for continuing professional learning: investigating the experiences of teachers with limited resources. *Studies In Continuing Education*. 44(3), 546–562. <https://doi.org/10.1080/0158037X.2021.1932453>.
- Lilach Faerman Koren. (2023, September 11). Identity security's crucial role in safeguarding data privacy. *CyberArk Blog*. <https://www.cyberark.com/resources/blog/identity-securitys-crucial-role-in-safeguarding-data-privacy>
- Machin-Mastromatteo, J. D. (2021). Information and digital literacy initiatives. *Information Development*, 37(3), 329-333. <https://doi.org/10.1177/02666669211031695>
- Madunezim, C. J., Eze, C. C., & Oredu, J. N. (2024). Application of e-governance in service delivery: A study of Federal Inland Revenue Service. *Journal of Policy and Development Studies*, 14(2), 104–111. <https://doi.org/10.4314/jpds.v14i2.8>
- Mbilla, S. A. E., Nyeadu, J. D., & Akolgo, D. A. (2020). Tax compliance in Ghana: Evidence self-employed from Bawku West District. BP International. <https://doi.org/10.9734/bpi/mono/978-93-90149-18-6>
- Ministry of Communications & World Bank. (2020). E-transform newsletter for the first quarter of 2020. Accra: Ministry of Communication.
- National Information Technology Agency. (2017). E-government network infrastructure. Available: <https://nita.gov.gh/projects/jurong-logistics-hub/> [2021, June 15].
- Norander, S. & Brandhorst, J. (2017). Case Study. In A. Mike (Ed.), *The Sage encyclopaedia of communication research methods* (pp. 117-119). Sage. DOI: <https://doi.org/10.4135/9781483381411>.
- Odartey, E. L. (2022). Corruption perception and tax non-compliance among self-employed individuals in Ghana. [MPhil Thesis, University of Ghana] <http://ugspace.ug.edu.gh:8080/handle/123456789/40446>
- Opoku, A. (2020). Level of tax knowledge and technology adoption among small taxpayers in Ghana. [MPhil Thesis, University of Cape Town]. <http://hdl.handle.net/123456789/7355>
- Pasha, D. (2022). E-Governance and the Importance of Personal Data Protection in Albania. DCAF <https://www.dcaf.ch/sites/default/files/imce/ECA/D.Pasha-YoungFaces2022.pdf>
- Polit, D. F. & Beck, C. T. (2014). *Essentials of nursing research: appraising evidence for nursing research*. (8th ed.). Lippincott Williams & Wilkins Publishers.
- Project New Yorker. (2024, March 6). What Is Digital Literacy and Why Is It Important? <https://projectnewyorker.org/what-is-digital-literacy-and-why-is-it-important/>
- Rahman, S. (2010). Using strategic communications to engage stakeholders in tax reform. 59820 World Bank Publication <https://documents1.worldbank.org/curated/en/796441468328213861/df/598200NEWS01pu1ice120Communications.pdf>.
- Rukundo, S. (2020). Addressing the challenges of taxation of the digital economy: Lessons for African countries. The Institute of Development Studies and Partner Organisations. Report. <https://hdl.handle.net/20.500.12413/14990>
- Sen, K. (2024). Website security checklist. <https://www.upguard.com/blog/the-website-security-checklist>.
- Shareef, M. S. (2017). Security of e-government; risks,

- threats, and success factors. *Journal of Raparin University*, 4(10).
- Solange, U., Mulyungi, P., & Oluoch, O. (2018). Effect of electronic tax system on tax compliance among small and medium taxpayers in Rwanda: Case study of Nyarugenge Sector, *International Journal of Management and Commerce Innovations*, 6 (1).
- Soneka, P. N. & Phiri, J. (2019). A model for improving E-tax systems adoption in rural Zambia based on the TAM Model. *Open Journal of Business and Management*, 7(2), 10.4236/ojbm.2019.72062
- Tchao, E. T., Keelson, E., Aggor, C., & Amankwa, G. A. (2017). E-government services in Ghana - current state and future perspectives. 2017 International Conference on Computational Science & Computational Intelligence, (CSCI), Las Vegas, NV, USA, 2017, pp. 624-631. DOI: <https://doi.org/10.1109/CSCI.2017.108>.
- Thiel, A. (2020). Biometric identification technologies and the Ghanaian data revolution. *Journal of Modern African Studies*, 58(1), 115-136. DOI: <https://doi.org/10.1017/S0022278X19000600>.
- Uden, L. & Mustapha, S. (2011). Defining community of practice in the context of activity theory. Retrieved from <http://ur.aeu.edu>. My /id/ eprint/518.
- United Nations Economic Commission for Africa. (2019). Fiscal Policy for Financing Sustainable Development in Africa. <https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/2019LINK-Wednesday-Session1-A.pdf>
- Verkijika, S. F. & De Wet, L. (2018). E-government adoption in Sub-Saharan Africa. *Electronic Commerce Research & Applications*. 30(1), 83-93. DOI: <https://doi.org/10.1016/j.eierap>.
- Wöhrer, V. (2018). Data protection and taxpayers' rights: challenges created by automatic exchange of information. *European and International Tax Law and Policy Series*, 10. Institute for Austrian and International Tax Law. https://www.ibfd.org/sites/default/files/2021-12/18-066-Data-Protection-Taxpayers-Rights_final-web.pdf
- Xu, W., & Zammit, K. (2020). Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International Journal of Qualitative Methods*, 19, 1609406920918810.
- Yamagishi, R. & Fujii, S. (2024). Survey and analysis of user perception of security icons. In *European Interdisciplinary Cybersecurity Conference*. <https://DOI.org/10.1145/3655693.3661295>.
- Zondiros, D. (2008). Communities of practice, activity theory and distributed learning. *Readings in Education and Technology: Proceedings of ICICTE*. <http://www.icicte.org/> ICICTE2008 Proceedings/zondiros097.pdf. Bahar. <https://doi.org/10.3390/soc14020019>

Corresponding Author

Angela Aikins
aannor@uds.edu.gh