SECTION ON LEGAL PRACTICE

SECTION ON LEGAL PRACTICE LAW JOURNAL
(SLP LAW JOURNAL)

Volume 10 June 2024

ISSN: 2734 – 3464

A Publication of the Section on Legal Practice (SLP),
Nigerian Bar Association (NBA)

Article 7

VIRTUAL DATA ROOMS – A CURSORY LOOK AT THE EFFECT OF DATA PROTECTION LAWS; THE OBLIGATIONS AND LIABILITY OF THE DISCLOSER

By Favour D. Iremia* and Toluwase Oladele**

Abstract

Virtual Data Rooms (VDRs) have transformed the landscape of confidential information sharing, particularly within mergers and acquisitions (M&A) and financial transactions. VDRs offer enhanced accessibility, efficiency, and security compared to physical data rooms. However, they also pose inherent risks, particularly concerning data security and compliance with data protection laws. The onus lies on organizations to choose VDR providers with robust security infrastructure and adherence to data protection laws to avoid legal, financial, and reputational repercussions. The security and integrity of VDR systems is paramount to protect sensitive data and preserve trust in business dealings. This article examines VDRs, the effect of data protection laws on the usage of VDRs and the obligations of the disclosing parties arising under the data protection laws, as well as liability in the event of a VDR security breach.

Keywords: Virtual Data Rooms, Data Protection, Compliance, Disclosures, Confidentiality.

INTRODUCTION

The term "data room "dates back to the 1900s, an era when companies relied on printing physical documents and gathering them in secure rooms for investors and other potential partners to peruse.[1] M&A (mergers & acquisitions) gave birth to the first data rooms. This process, as we know it today, originated in the 19th century. This era, called "*The Great Merger Movement*", emphasized the importance of creating a physical data room to

* Favour D. Iremia - Associate, Commercial Team, TONBOFA Law Practice TONBOFA Law Practice, 51 Adeshiyan Street, Ilupeju, Lagos State. Info@tonbofa.com 07052223612, favour@tonbofa.com

** Toluwase Oladele – Senior Associate, Commercial Team, TONBOFA Law Practice, 08037394007, toluwase@tonbofa.com

[1] Justine, Moore, The Insider's Guide to Data Rooms: What to Know Before You Raise https://a16z.com/the-insiders-guide-to-data-rooms-what-to-know-before-you-raise/ Retrieved April 20, 2024

store sensitive documents on company information.[2] Dusty storage rooms in offices, filled shelves or cabinets with a massive volume of confidential information are known as Physical Data Rooms (PDRs). Highly restricted access controls entry to these storage rooms, requiring interested parties to be onsite and physically present at the disclosing party's offices to gain access. With the globalization and digitalization of business, data rooms have long since evolved from just physical rooms to online document storage and sharing systems.

Virtual Data Rooms (VDRs), on the other hand, have made it quite easy for investors and other interested parties anywhere in the world to have access to such confidential information without having to leave their offices. In 1984, Sony's introduction of the CD-ROM marked a watershed moment, signalling the dawn of a new era in data storage and accessibility. This pivotal step marked a profound transition from traditional physical storage mediums to the realm of digital solutions. Sony's ground-breaking introduction of the CD-ROM not only revolutionized the way data was stored but also paved the way for a myriad of technological advancements in the years to come. Sony's innovative CD-ROM technology boasted unparalleled storage capabilities, providing users with the ability to store massive volumes of data conveniently and reliably. The significance of this innovation cannot be overstated, as it ushered in a paradigm shift in the way information was managed and accessed. Gone were the days of cumbersome physical storage solutions; instead, users could now effortlessly store and retrieve vast amounts of data with unparalleled ease and efficiency.

Furthermore, the widespread adoption of CD-ROM technology spurred a wave of innovation across various industries, ranging from education and entertainment to business and beyond. Its impact extended far beyond mere storage solutions, serving as a catalyst for the digital revolution that continues to shape our world today. In essence, Sony's pioneering efforts in launching the CD-ROM in 1984 marked a seminal moment in the history of technology, propelling us into a new era of digital innovation and redefining the way we store, access, and interact with information.

---

[2] DiliTrust, Data Rooms: What is Their History and How Have They Evolved? https://www.dilitrust.com/data-rooms-what-is-their-history/ Retrieved April 20, 2024

Despite the advancements in storage solutions, inherent risks persisted, including the potential for physical data loss and corruption. Thus, it remained imperative to leverage ongoing technological progress to refine the storage of sensitive information. A significant milestone in this pursuit occurred in 1996 with the introduction of "Cloud Computing" by George Favaloro of Compaq Computers, revolutionizing data storage by enabling online accessibility. Approximately a decade after Favaloro's groundbreaking innovation, tech industry giants like Google propelled the concept of Cloud Computing into mainstream consciousness. Google's pivotal presentation on the topic in 2006 during a widely attended conference marked a pivotal moment, catalysing widespread adoption. Subsequently, other industry titans such as Microsoft, Amazon, and IBM swiftly embraced this novel technology, recognizing its transformative potential.

The advent of Cloud Computing ushered in a new era characterized by enhanced efficiency and security in data management. Notably, this technological evolution had a tangible positive impact on M&A (mergers and acquisitions) and other corporate finance transactions through the advent of VDRs. By streamlining transaction processes and bolstering the security of sensitive documents, Cloud Computing contributed to accelerated deal completion and heightened confidence among stakeholders.[3]

Data rooms stand as essential components within the operational frameworks of organizations spanning a multitude of sectors in the business realm. Whether in legal practice, mining enterprises, oil and gas ventures, construction projects, manufacturing facilities, or other domains, the utilization of data rooms underscores a fundamental aspect of modern business operations. The choice between PDRs and VDRs often hinges on a variety of factors, including the nature of the industry, the specific requirements of the organization, technological preferences, and the nature of the confidential information.

In the intricate landscape of mergers and acquisitions (M&A) and other corporate finance transactions, data rooms emerge as pivotal arenas during

[3] DiliTrust, Data Rooms: What is Their History and How Have They Evolved? https://www.dilitrust.com/data-rooms-what-is-their-history/ Retrieved April 20, 2024

the due diligence phase. Here, stakeholders engage in exhaustive assessments aimed at discerning and mitigating potential risks, whether they be of a legal, financial, or operational nature. The comprehensive nature of due diligence demands unfettered access to a trove of critical information housed within these data rooms, facilitating informed decision-making processes.

However, access to such sensitive data is not granted without stringent protocols in place. Prior to delving into the depths of the data rooms, parties involved typically formalize their commitment to confidentiality through the execution of a legally binding agreement. Known as a Confidentiality Agreement or Non-Disclosure Agreement (NDA), this document serves as a safeguard, ensuring that proprietary information remains protected, and that the integrity of the transactional process is maintained.

Furthermore, the advent of technological innovations continues to shape the landscape of data room functionalities. Virtual data rooms, in particular, have witnessed a surge in popularity, offering unparalleled convenience, accessibility, and security. These digital platforms not only streamline the due diligence process but also empower organizations to navigate the complexities of modern business transactions with greater agility and efficiency.

In addition to the confidentiality agreement, the disclosing party's legal team will also draw up a set of data room rules. These rules will govern access to the data room and are a further protection for the disclosing party (in that those accessing the data room are bound to a set of rules imposed by the disclosing party). The receiving party will either sign a hard copy of the rules or agree to them via a 'click through' on the platform hosting the VDR. The rules can be amended from time to time by the disclosing party giving notice to the receiving party. The rules will differ depending on the type of data room.[4]

At the due diligence stage of any finance transaction, contracts, agreements, or other confidential documents that contain personal data would be

[4] Lexis Nexis, Data rooms—share and asset purchases https://plus.lexis.com/uk/practical-guidance-uk/data-roomsshare-and-asset-purchases/?crid=c5f048a0-d497-4cd3-a626-b94ccf37e038 Retrieved April 20, 2024

disclosed. The disclosing party must be acquainted with the dangers of violating the relevant data protection provisions within its jurisdiction and take all necessary steps to implement proper safeguards for the distribution of such information, especially when a data room is used.

Exploring the Preference for Virtual Data Rooms (VDRs)

During a finance transaction, the disclosing party sets up VDRs, which are online (often cloud-based) repositories and document-sharing platforms, to give the receiving party and their advisers access to the documents and information they need to conduct their due diligence exercise in relation to the target company/business. A disclosing party typically engages a third-party service provider to set up the VDR, and then the disclosing party proceeds to get it ready for use by uploading documents and data onto the secure online document repository and data-sharing platform. With advances in technology and the number of third-party providers, VDRs are now broadly used.[5]A basic example of how virtual data room tools work is the Microsoft OneDrive used internally by teams within an organisation to collaborate and work on several tasks. One of the key features of this software being the ability to access the relevant documents and information needed for the progress of the task or project. Access to certain information can also be restricted to certain team members depending on their rankings within the organisation.

While tools like Google Drive and OneDrive are suitable tools for less confidential information and collaboration, it is different in the case of the Virtual Data Room tool, which has a number of important features and functions designed for the needs of financial advisors, law firms, company boards and financial entities. While VDR also works in the Software-as-a-Service (SaaS) model, it is distinguished from popular cloud tools by advanced functions such as traffic supervision in the Data Room, amongst others.[6] Free platforms such as SharePoint, or Dropbox may be converted

---

[5] Lexis Nexis, Data rooms—share and asset purchases https://plus.lexis.com/uk/practical-guidance-uk/data-roomsshare-and-asset-purchases/?crid=c5f048a0-d497-4cd3-a626-b94ccf37e038 Retrieved April 20, 2024

[6] Aleksandra, Prusator, Security: Can Microsoft One Drive or Google Drive replace VDR? https://fordatagroup.com/can-microsoft-one-drive-or-google-drive-replace-vdr/ Retrieved April 20, 2024.

and utilised as VDRs, however they provide limited functionality and may not meet all requirements compared to dedicated VDR software.[7]

Advantages of VDRs

The advantages of VDRs include:

1. Remote Accessibility: VDRs can be accessed at any time and at any location worldwide over a prescribed period. Documents are easily and efficiently reviewed electronically.
2. Saves time and costs: At the due diligence stage, remote access to the relevant documents saves time and costs that would have been expended in visiting the PDR at the disclosing party's offices and manually searching for and reviewing each document.
3. Highly attractive to international investors and other counterparties: The savings in costs and time in the use of a VDR significantly increase the number of potential investors or other counterparties to the financial transaction compared to a circumstance where only a PDR is employed.
4. Organizing documents easily: Regardless of the locations of the physical documents at the offices of the disclosing party, whether halfway across the world at branch offices or not, and notwithstanding the massive volume of documents, it is easier to scan, upload, and organize the documents within the VDR ecosystem compared to the sheer amount of manpower and time consumption required to do so in the PDR. At the request of the receiving party, the disclosing party can also easily update its archives and correct any errors in the accuracy of the confidential information.
5. Restrictions: It is quite easy to place restrictions on individual access to the VDRs. Persons who would be granted access to the VDRs are usually provided with secure usernames and passwords, which must

[7] Acquire Blog, What Is a Data Room and How Do You Use One During an Acquisition? https://blog.acquire.com/what-is-a-data-room-and-how-do-you-use-one-during-an-acquisition/#:~:text=watermarks%2C%20and%20encryption.-,Is%20SharePoint%20a%20Data%20Room%3F,sharing%20and%20managing%20confidential%20documents. Retrieved April 21, 2024.

be kept confidential at all times to avoid unauthorized third-party access. Further restrictions can also be placed, limiting actions such as downloading or printing the confidential information; copying and pasting of text might also be disabled, including any software to screen capture.

6. Security: Encryption software, multiple firewalls, virus detection and full administrator control over which folders and documents can be viewed by users, are a few of the security measures put in place by VDR providers to ensure the security of all information housed within the VDR systems.

Disadvantages of VDRs

1. Security Risks: Despite the various security measures, security guarantee is still not 100%. VDRs could, regardless of the security measures, become subject to cybersecurity attacks.

2. Confidentiality: Confidentiality may be compromised as persons with access might share the secured username and password with others in their organization, and the disclosing party may have no idea of who actually has access to the VDR. This risk is usually addressed in the NDA, by ensuring that a receiving party and other persons to whom it might disclose confidential information are all bound by the confidentiality clause of the NDA.

3. Copyright risks would also be taken into consideration in the event that third-party documents and intellectual property are shared.

Data Protection Laws and the consideration of Data Protection Principles in selecting a VDR

Companies are responsible for and must be able to demonstrate compliance with the data protection principles, which include processing personal data lawfully, fairly, and transparently in relation to the data subject, and fulfilling certain conditions, including:

- consent of the data subject must be obtained;
- the processing of the data must be requisite for the performance of a contract with the data subject;

- legal compliance obligations must be met;
- there must be protection of the data subject's vital interests; and
- the data processing should not be done in a prejudicial manner but in pursuit of legitimate interests and the data subject's interests or fundamental rights and freedoms.[8]

The Nigeria Data Protection Regulation (NDPR) 2019, Part 2 paragraph 2.1 spells out expressly the governing principles for data processing in Nigeria. It states that:

> *(I) In addition to the procedures laid down in this Regulation or any other instrument for the time being in force, Personal Data shall be:*
>
> *a. collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject; provided that:*
>
> *i. a further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest;*
>
> *ii. any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph shall not transfer any Personal Data to any person;*
>
> b. *adequate, accurate and without prejudice to the dignity of* human *person;*
>
> c. stored *only for the period within which it is reasonably* needed, and
>
> d. secured against *all foreseeable hazards and breaches such as* theft, cyberattack, *viral attack, dissemination, manipulations* of any *kind, damage by rain, fire or exposure to other* natural *elements.*

[8] Stavros, Pavlou, The 'dark' side of the data room: disclosure dangers in M&A and finance transactions https://chambers.com/articles/the-dark-side-of-the-data-room-disclosure-dangers-in-ma-and-finance-transactions Retrieved April 23, 2024.

(2) Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject owes a duty of care to the said Data Subject;

(3) Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in this Regulation.

A similar, albeit more detailed provision can be found in Nigeria Data Protection Act (NDPA) 2023, section 24. Homogeneously, the EU General Data Protection Regulation (GDPR), Article 5 provides that:

1. *Personal data shall be:*

   a. *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

   b. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

   c. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

   d. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

   e. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for*

> ***longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');***
>
> ***f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').***

Considering the above, data shown during M&A and financial transactions must be disclosed lawfully, fairly, and in a transparent manner. Both Parties, the disclosing party, and the receiving party, have the obligations to ensure that personal data shared at the due diligence stage is treated and handled in accordance with the various data protection laws as applicable in the relevant jurisdiction. Moreover, the use of a Virtual Data Room (VDR) raises additional areas of interest about the security and digital protection of the disclosed data during processing and transmission.

The nature of data contained in such documents and their virtual nature in the digital era may complicate matters further, as a virtual data room requires careful handling and supervision, including setting up access restrictions and limiting its contents to the perusal and review of the documents contained therein.[9]

Through advanced encryption and flexible internal security policies the security of VDRs is significantly strengthened. This prevents unauthorised individuals from stealing any data, personal or otherwise, from within a VDR.[10] The NDPR[11], NDPA[12] and GDPR respectively require

---

[9] Stavros, Pavlou, The 'dark' side of the data room: disclosure dangers in M&A and finance transactions https://chambers.com/articles/the-dark-side-of-the-data-room-disclosure-dangers-in-ma-and-finance-transactions Retrieved April 23, 2024.

[10] Cyber Management Alliance, Virtual Data Rooms and How They're Revolutionising Cyber Security https://www.cm-alliance.com/cybersecurity-blog/virtual-data-rooms-and-how-theyre-revolutionising-cyber-security Retrieved April 20,2024

organizations to implement appropriate technical and organizational measures for the security of personal data during and after processing. These security measures will include, *inter alia:*

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[13]

Neglecting VDR security is like rolling out the red carpet for trouble right into your digital home. Lack of adequate safeguards and appropriate security measures means that confidential data is left exposed to a myriad of threats. Cybercriminals will steal or tweak the information for malicious purposes. Competitors will acquire unfair advantages when it accesses confidential trade secrets, financial information or strategic plans. Consumers face equally grievous risks, which may include identity theft, breach of privacy and theft of financial information.

There are severe legal and financial fallouts which organisations may face because of data breaches. Organisations might also suffer interminable damages to its goodwill and reputation, which could less to the winding up of businesses. Hence, neglecting virtual data room security simply is not worth the risk[1415]

When choosing a VDR, whether on a free platform or a specialized VDR, organizations should carefully consider the security measures utilized by the provider and the relevant data protection laws. The choice should also take

---

[11] NDPR, Part 2 paragraph 2.6
[12] NDPA, Section 39
[13] GDPR, Article 32(1)
[15] Patrick, Spencer, Protecting Your Data: A Guide to Virtual Data Room Security https://www.kiteworks.com/secure-file-sharing/virtual-data-room-security/ Retrieved April 20, 2024

into consideration factors such as ease of use, scalability, cost-effectiveness, and compatibility with existing systems, among others.

Upon selecting and setting up the preferred VDR system, organizations should take steps to invest in training for members of staff and management on the security features and restrictions of the VDR system. This training will focus on data breaches, data security risks, and how to effectively and efficiently use the VDR system. Additionally, organizations should regularly assess and audit the security measures to ensure that the VDR system is up to date and meets the needs of the organization.

Finally, as technology advances and new threats emerge, it is vital that the chosen VDR solution is upgraded regularly to maintain its security efficacy. By blending these methods, the VDR security measures stay sturdy, dependable, and efficient in safeguarding confidential information.

Risks of VDR Breaches

A breach, leak, or compromise of a VDR would cause significant and lasting harm to various parties involved. For example, where unauthorized third parties gain access to confidential agreements stored in the VDR through authorized persons with access, it breaks trust and confidentiality rules. A breach of the VDR could also occur due to a cyberattack on the VDR system. Such breaches and subsequent leaks of confidential information and personal data could devalue a business, diminish its market share, affect investor returns, and erode its competitive edge.

In order to engage the services of a VDR provider and obtain access to its online software, prospective clients are required to enter into contractual agreements with the provider. These agreements extensively detail the terms and conditions governing the utilization of the VDR services, including the management of risks associated with unauthorized access.

Within these contractual arrangements, there exists a delineation of responsibilities regarding the security of the VDR. In some cases, the onus falls entirely upon the customer to ensure the protection of their passwords and sensitive data, as well as to actively monitor the activity occurring within the subscribed VDR platform. Additionally, customers are obligated to promptly report any instances of unauthorized access to the VDR service

provider, thereby facilitating swift action to mitigate potential risks and breaches.

Moreover, these contractual agreements necessitate the implementation of robust procedures by VDR customers. Such procedures are aimed at restricting access to the VDR, thereby safeguarding sensitive information from unauthorized parties. Furthermore, these protocols extend to post-transaction measures, requiring customers to enact mechanisms that limit access for parties once their involvement in the transaction has been concluded. These comprehensive procedures serve as vital safeguards, ensuring the integrity and security of the VDR environment throughout its utilization.

Additionally, certain VDR service providers may waive all warranties and demand acknowledgment regarding the potential compromise the security of its platform. Further, a VDR service provider often negotiates provisions to exempt themselves from liability for indirect damages to customers (e.g., damages caused by third parties) and to cap its liability for damages arising from providing VDR services. Lastly, in such agreements, a VDR service provider may limit its duty to indemnify the customer and instead require the customer to defend the provider against certain claims related to customer content stored in the VDR. While these provisions may not necessarily be unreasonable, they allocate a significant portion, if not all, of the risk of a data breach to the customer.[16]

However, regardless of any other person granted access to the VDR at the due diligence stage, only the disclosing party, being the party with whom the VDR provider has a service agreement, may have any claims against the VDR provider in the event of a data breach due to the inadequacy of the security of the VDR. The receiving party may only have claims against the disclosing party as agreed in the NDA.

The onus, therefore, is on the disclosing party utilizing a VDR at the due diligence stage to choose a VDR provider with the requisite security infrastructure and compliance with the relevant data protection laws.

---

[16] Van, Wiltz, Cybersecurity in the Cloud: Virtual Data Rooms—Part II https://casetext.com/analysis/cybersecurity-in-the-cloud-virtual-data-roomspart-ii Retrieved April 20, 2024

The liability of each party, the disclosing party, the receiving party or the VDR provider would be as defined and limited in the respective agreements executed and in accordance with the laws applicable.

Conclusion

In conclusion, the evolution of data rooms from their physical origins to the virtual realm has transformed the landscape of business transactions, particularly in the context of mergers and acquisitions and other corporate finance endeavours. Virtual Data Rooms (VDRs) have emerged as indispensable tools, offering enhanced accessibility, efficiency, and security compared to their physical predecessors.

However, alongside the myriad benefits of VDRs come inherent risks, particularly concerning data security and compliance with data protection laws. The consequences of a VDR breach can be profound, ranging from reputational damage to financial and legal liabilities for all parties involved. Thus, it is imperative for organizations to diligently evaluate and implement robust security measures and compliance protocols when utilizing VDRs.

The contractual agreements between VDR service providers and customers play a crucial role in allocating responsibilities and liabilities related to VDR security. Customers must be vigilant in safeguarding their passwords and monitoring VDR activity, while also implementing procedures to restrict access and mitigate risks. Meanwhile, VDR service providers often disclaim liability and impose limitations on indemnification, shifting significant risk onto the customer.

Ultimately, the onus lies on the disclosing party to choose a VDR provider with robust security infrastructure and adherence to data protection laws. Failure to do so could result in severe consequences, including legal and financial repercussions, reputational damage, and compromised transactions. As technology continues to evolve, organizations must remain vigilant in maintaining the security and integrity of their VDR systems, ensuring the protection of sensitive data and the preservation of trust in business dealings.