GUARDING THE THREADS: DATA PROTECTION CHALLENGES AND STRATEGIES IN AFRICAN FASHION

I. INTRODUCTION

Data is the oil of the digital era.[1] In computing, data is information that has been translated into a form that is efficient for movement or processing.[2] With the digital era arose the need for businesses to collect and process data which in turn birthed the need to protect the data that were being collected. The fashion industry is no exception. The shift from traditional brick-and-mortar stores to the use of e-commerce websites and applications to display fashion products and reach consumers was welcomed. During the pandemic in 2020, the online marketplace was set abuzz characterized by heavy reliance on the internet by businesses to reach their consumers and stay afloat. Fashion brands such as Grass-fields and Kai Collective utilised this platform to make more sales and expand their business operations. "Fashion companies that have harnessed the power of data to strengthen e-commerce experiences have grown digital sales by 30 and 50 per cent." [3]Thus, it is evident that data collection and utilization is a catalyst for improved value in a fashion brand's e-commerce sales as well as physical sales.

A. THE PURPOSE AND SCOPE OF THE CONTENT

This publication seeks to highlight some of the challenges faced in the protection of Data collected from consumers by fashion brands and to explore the different strategies that can be adopted by Fashion brands in Africa to provide efficient and reliable security for the data of business.

B. COMPLYING WITH DATA PROTECTION LAW

---

[1] The Economist, 'The World's Most Valuable Resource is no Longer Oil, but Data' Economist (6 May 2017) https://www.economist.com/leaders/2017/05/06/the-worls-most-valuable-resource-is-no-longer-oil-but-data accessed 22August 2023

[2] Jack Vaughan, 'Data Management' Tech Target (July 2019) https://www.techtarget.com/searchdatamanagement/definition/data

[3] Sardine Devillard, Holger Harreis, Nicholas Landry, and Carlos Sanchez Altable, 'Jumpstarting Value Creation with Data Analytics in Fashion and Luxury' (Mckinsey, 14 October 2021) https://www.mckinsey.com/industries/retail/our-insights/jumpstarting-value-creation.with-data-analytics-in-fashion-and-luxury accessed 22 August 2023

OVERVIEW OF DATA PROTECTION LAWS IN AFRICA

The European Union's General Data Protection Regulation (GDPR) presented an opportunity for African countries to recognize the need for the protection of personal data of citizenry since the emergence of the Internet and the need for citizens to submit their data on various Internet platforms including social media, website and many more. [4] Over 30 out of 54 African countries have put in place Legislation to regulate the protection of personal data in their countries and only sixteen countries have signed the African Union Convention on Cyber Security and Personal Data Protection adopted on 27th June 2014 (" Makabo Convention") out of which thirteen countries have ratified it. The interest in creating Data Protection Laws for a 21st–century digital Landscape extends far beyond the African Union, to countries as diverse as Japan, Israel, Canada, Brazil and India. [5] This is because of the wide recognition of the growing risks Data subjects are continually exposed to which includes personal data breach, exploitation of child data privacy and many more which creates the need to protect collated personal data and to regulate the processing of personal data.

C. DATA BREACH MANAGEMENT AND RESPONSE

Data breach refers to a situation whereby unauthorized individuals gain access to sensitive or confidential information, such as personal data (e.g., Social Security numbers, bank account details, healthcare records) and corporate data (e.g., customer records, intellectual property, financial information). [6] Data breach management, therefore, can easily be defined as how well data breach incidents can be handled to create effective responses to combat the consequences of the breach incident at hand.

From the above, it can be deciphered that data breach management is an essential concept that all fashion brands must possess to ensure that their works receive due

---

[4] Dalberg Advisors Strategy, GDPR: The implications for Africa, https://dalberg.com/our-ideas/gdpr-implications-africa/ may 29 2018

[5] Brian Daigle, "Data protection Laws in Africa: A Pan-African Survey and Noted Trends" Journal of International Commerce and Economics, February 2021. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjp6-qJhomBAxVJiVwKHRypCQQQFnoECBMQAQ&url=https%3A%2F%2Fwww.usitc.gov%2Fpublications%2F332%2Fjournals%2Fjice_africa_data_protection_laws.pdf&usg=AOvVaw0NYny1R8h7e3P1ex7s_KLB&opi=89978449 Accessed on 23rd August,2023

[6] IBM, 'What is a data breach?'(IBM) https://www.ibm.com/topics/data-breach accessed 8 August 2023.

protection and can bounce back even when data breach incidents occur. It is important to note however that data breach management can prove futile if it is ineffective, therefore every fashion brand must possess a strong data breach management field put in place to fully serve its function.

When dealing with data breach management, the question of how to prepare for data breach incidents will erupt. Essentially, you want to have a data breach response plan which is a document that entails how an organization would respond to a data breach. [7]To prepare, and create a comprehensive data breach response plan through risk assessment, defining response teams, and establishing a contact list for authorities and third-party companies. Develop a flexible communications plan with prepared statements for customers, staff, and media to initiate incident response if a breach occurs. [8]

Another way to prepare for data breach incidents is by conducting data breach drills and simulations such as; Tabletop exercises which are in a low-stress setting to identify and resolve problems, and drill tests which help specific functions realistically. Functional exercises which are fully simulated tests of organizational capabilities as well as field exercises which simulate real events on a smaller scale can be used to effectively prepare for data breach incidents alongside generally educating staff on breach incidents. [9]

Preparation goes a long way in data breach management, however, how well you apply such preparation determines how thorough your ability to solve the problem will be. Therefore, it is essential to know how to respond to data breaches when they have occurred. In light of a breach, you must first and foremost examine the extent and scope of which damage has occurred to know what response plan to activate. This must be done thoroughly by a team of experts while duly strengthening data security and privacy control. Another key way to respond to a data breach is by ensuring any potential evidence is not destroyed while regularly communicating with law enforcement agencies, One may also consult a legal

---

[7] Rob Shapland, 'How to develop a data breach response plan: 5 steps' (TechTarget, July 2022) https://www.techtarget.com/searchsecurity/feature/How-to-develop-a-data-breach-response-plan-5-steps accessed 8 August 2023

[8] Ibid

[9] UNDDR, 'conducting simulation exercises' (Prevention Web) https://www.preventionweb.net/conducting-simuFederalTradeCommissionProtectingAmerica'sConsumer's, 'Data Breach Response: A guide for business'

counsel to be aware of one's rights and seek redress for any damage that occurred. [10]

Once a data breach has occurred certain prevention steps that can be taken to ensure your data is protected and not prone to the same or any other data breach include; restricting access and limiting the number of people with data access, strengthening the general security with firewalls, VPNs, and updates. Training employees on data security best practices and common threats and continuously auditing and updating security measures to adapt to evolving risks.[11]

In Conclusion, for data protection in African fashion, emphasis needs to be placed on data breach management's crucial role. Robust response plans, simulations, and timely actions protect sensitive data, and reputation, and foster trust must be put in place to safeguard customer information and intellectual property while ensuring resilience against cyber threats, and in essence a safer digital landscape for African fashion brands.

II. DATA PROTECTION CHALLENGES IN AFRICAN FASHION

A. DATA COLLECTION AND USAGE

As the African fashion Industry becomes more data-driven, it necessitates data collection to make informed business decisions. [12] Data needs to be handled properly through every process of collection, use and disposal to avoid data breaches or unlawful transfers which could lead to lawsuits. Section 25 of the Nigeria Data Protection Act (NDPA) provides that the lawful basis for data processing shall be where the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed.

[10] (IdentityTheft.gov, February 2021) https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business accessed 8 August 2023.lation-exercises accessed 8 August 2023.

[11] Nate Nead, 'How To Prevent A Data Breach in Your Company', (Forbes, 30 July 2021) https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=aaaeffb18da7 accessed 8 August 2023.

[12] Adi Bhat, 'Data Collection: What it is, Methods &Tools +Examples (Question Pro) https://www.questionpro.com/blog/datacollection/:~:text=Put%20simply%2C%20data%20collection%20is,how%20we%20will%20collect%20it accessed 22 August 2023

Section 2 of the Eswatini Data Protection Act recognises Consent as explicit and implicit. While Implicit consent means consent which is inferred from signs, actions, facts or by inaction or silence, explicit consent on the other hand is voluntarily expressed by spoken or written words clearly given by a data subject.

Although, the Data Protection Laws of African countries provide that where the data subject is a child or a person lacking in legal capacity to give consent, data controllers are expected to obtain the consent of their parents or legal guardians.[13] However, this raises the issue of properly adopting adequate mechanisms to verify age and consent. This shifts the onus on the data processor to provide extensive research to verify the age and the consent obtained.

African Fashion businesses such as Ruff 'n' Tumble (Nigeria) or JenniDezigns in South Africa must ensure that necessary steps are taken to secure the data of their under-aged consumers. For instance, any information given must be obtained through the children's parents or their *In loco parentis.* In the instance where it is obtained but consent is retrieved or not given at all, they must immediately delete such to avoid any legal consequence.

One provision that is similar across the Data Protection Law in Africa establishes the requirement of transparency which requires that before a data controller collects personal data from a data subject, the data controller shall inform the data subject of the scope and extent of use and transfer of such data. Thus, fashion businesses participating in data collection and use must first jump the hurdle of procuring consent and be transparent in their dealings with consumer data to avoid breaching the law and facing arduous lawsuits. In 2022, Shein was fined 1.9 million dollars by the New York Government for failing to inform its users of the data breach of their personal data which occurred in 2018.

Furthermore, data collected to predict consumer behaviour and trends may not always be accurate as consumer needs are ever-evolving. These wrongful predictions may lead to profit losses and inventory wastage. Data may also be lost if not properly stored leading to a waste of valuable time and resources.

[13] Nigeria Data Protection Act 2023, s 31

B. DATA SECURITY AND PRIVACY RISKS

Difficulties arise in the protection of consumer data due to the increase of cybercrimes in today's digital era. "The first quarter of 2020 experienced a higher record of consumer data breaches, with over 8 billion records exposed". [14] Fashion brands have also not been exempted from cybercrime considering that the majority of fashion brands are now either tech-enabled or tech-driven characterised by a very active digital presence. In 2018, Shein suffered a cyber-security attack that resulted in the theft of 39 million Shein account credentials including those of over 375,000 New York residents which prompted the Attorney General's office in New York to sanction an investigation into the extent of the breach that revealed the negligent manner in which the aftermath of the breach was handled. [15]

Section 39 of the NDPA provides that a data processor and data controller adopt appropriate technical measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control. [16] To this effect, a data controller is mandated to implement technical measures to protect against accidental or unlawful destruction, loss, misuse, alteration and unauthorised disclosure or access. [17]

The adoption of measures for data protection births further challenges for fashion brands. Remediation of a cyber-attack costs money which the brand, especially in its formative stages may be unable to afford. 60% of small brands that suffer data compromise close down in six months taking into consideration only the loss of consumer confidence in such a brand. [18] Therefore, it is a dilemma mostly faced by small brands that are at a higher risk of cyber-attacks because they do not have the cash reserves to pursue sophisticated data protection measures. It is expensive to

---

[14] Nicole Reader, 'Fashion +Tech + Security: Cyber Beware (LinkedIn, 21 July 2020) https://www.linkedin.com/pulse/fashiontechsecurity-cyber-beware-nicole-reader accessed 22 August 2023

[15] Rita Liao, 'Shein owner fined $1.9M for Failing to Notify 39m users of data breach' (Tech Crunch, 13 October 2022) https://techcrunch.com/2022/10/13/shein-zeotop-fined-1.9m-data-breach/amp/ accessed 23 August 2023

[16] Nigeria Data Protection Act 2023, s 39(1)

[17] Ibid 16

[18] Dakota Murphey, 'Why the Fashion Industry Should Tighten its Belt on Cybersecurity' (Interline, 2022) https://www.theinterline.com/2022/05/09/why-the-fashion-industry-should-tighten-its-belt-on-cybersecurity/amp/ accessed 22 August 2023

put cyber security measures in place and the absence of these measures exposes fashion brands to higher risks of data breaches. Where these breaches occur, it is far more expensive to counter them.

The fashion industry is built on brand and as such heavy on its intellectual property. With the disruption of technology in the fashion sector, most fashion brands digitize their product lines which exposes them to the risk of cyber-attacks in the digital space. This in turn creates a unique cyber security challenge for fashion brands. [19]

Procuring the services of a professional is expensive as there is a shortage of personnel with the right technical skill sets to prevent and tackle cyber security issues.[20]

C. INADEQUATE SENSITIZATION ON DATA PROTECTION

Therefore, not all fashion businesses in Africa are aware of its existence, much less its scope and provisions. Data controllers who process an insurmountable volume of data daily do not fully understand their respective obligations under the extant laws.

Therefore, there is a lacuna in the knowledge of these persons affected by data protection adherence and enforcement. Fashion companies alike especially those on a small scale may not be aware of the relevant data protection laws and how they apply to them thereby exposing them to the risk of breaching the stipulations of the law and suffering the accompanying penalties.

D. CROSS BORDER DATA TRANSFER

In a fashion company's international relations, it is pertinent to take into consideration the position of the law on cross border transfer of personal data. Section 41 of the Nigeria Data Protection Act provides that companies cannot transfer personal data from Nigeria to another country except the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code

[19] Ibid 13
[20] Ibid

of conduct or certification mechanism that allows for an adequate level of protection of personal data. Furthermore, where the transfer is compatible with acceptable grounds for transfer of personal data under the Act such as transparency and consent, then cross-border transfer is permitted.

However, Section 31 of the Eswatini Data Protection Act (EDPA) provides the transfer of personal information within the South African Development Community member states which include 16 Member States; Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic Tanzania, Zambia and Zimbabwe. Section 33 of the EDPA provides for the transfer of personal data to non-member states only when a maximum level of adequate security is ensured in such country. This brings the question- what is the standard of adequacy for each non-member state?

However, Article 15 of the Egypt Personal Data Protection Law[21] (EPDPL) provides for exceptions to the provision made in Article 14 of EPDPL some of which will help in the fashion industry. The provision includes;

i. To conclude or perform an agreement entered into by the person responsible for processing the personal data and third party, which shall be in favour of the concerned data subject. There is a legal necessity or obligation to protect the public interest.
ii. To transfer money to another country under the laws in force of that country.
iii. If the transfer or circulation is under a bilateral or multilateral agreement, to which the Arab Republic of Egypt is a party

This raises the challenge of regulatory compliance. The multiplicity of laws makes regulatory compliance more daunting for fashion brands that may be at risk of suffering penalties for non-compliance. Where such brands do not have a sound compliance team that understands the regulations relevant to fashion brands, they are prone to breaching the provisions of the law and may get sanctioned, have lawsuits instituted against them and suffer brand dilution.

III. DATA PROTECTION STRATEGIES FOR AFRICAN FASHION BRANDS

A. COMPETENT REGULATORY COMPLIANCE TEAM

[21]Personal Data Protection Law No.151 of 2020 (the "Law")

It is trite that compliance is the bedrock of a business's longevity. Penalties are detrimental to growth and expansion. Furthermore, notoriety for non-compliance attaches a bad reputation to a brand and leads to a negative dilution in brand image which in turn impacts its longevity.

Thus, fashion brands should invest in a competent and qualified regulatory compliance team who have a thorough understanding of the law governing data protection and therefore ensure that they comply with the legal conditions for data protection, prevent breach of the law and avoid accompanying penalties.

B. **TECHNICAL AUDITS**

To completely comprehend an organization's data, hardware, devices, systems and personnel, regular audits should be conducted. Fashion businesses should always look for their weaknesses.

C. Organisations should review their supply chain to consider what measures key suppliers have taken. Designated incident management teams and a practical response plan should be established. There should be policies and procedures which cover data and system security, regulatory and compliance issues.

D. Each incident is an opportunity to learn what practices to limit harm the next time. Evaluate whether a team responded appropriately and whether additional resources are needed.

E. There should be policies and procedures which cover data and system security, regulatory and compliance issues.

CONCLUSION

The concept of Data protection although relatively new, poses an enormous obligation on fashion companies in Africa at large. Data has been defined as one of the most expensive 21st-century 'mineral. The collection of Customers can help improve the marketing strategy of a company. The management of consumers' data will determine the place of a fashion company locally and internationally as well as in the digital market. Although data is an important tool of a company, it however springs up many challenges because of it fragile nature. Fashion companies must

create strategies to ensure ultimum protection of its customers' data of the many and most effective ways is to comply with the extant provision Data Protection Laws.