DATA PRIVACY AND DATA PROTECTION: THE RIGHT OF USER'S AND THE RESPONSIBILITY OF COMPANIES IN THE DIGITAL WORLD.

*Alafaa Princess Uche-Awaji**

ABSTRACT

With the continuous advancement in technology and massive increase in internet usage, the concepts of data privacy and data protection is a hugely debated topic. This is because, the service providers who manage the websites, applications and social media platforms often collect and store user's personal data with the objective of providing adequate services to best suit each user's preference. Usually, these digital service companies are saddled with the responsibility of protecting the personal data of the users from unauthorised access and against all vulnerabilities. However, instances arise where these platforms fail to adequately place safeguards to protect the data collected and this results to a data breach and exposure of users sensitive data to unauthorised parties who can use the personal data to defraud and harass the users or to send unwanted adverts without the users consent. Thus, infringing on the users' fundamental right of privacy and freedom to freely express themselves. Hence, the need for companies to adopt defensive mechanisms to ensure an adequate protection of users' personal data and also awareness by the users that they have a right of control over which personal data to share and with whom it is shared. This paper is divided into three parts with the first discussing the rights of users and responsibilities of companies as well as the established regulations in the protection of data. The second part of this work considers the issues surrounding data privacy and data protection and the challenges faced in ensuring the safety of users' personal data. Finally, the last part offers a series of recommendations and conclusion.

Key words: Data Privacy, Data Protection, User, Data Breach, Privacy Policy, General Data Protection Regulation (GDPR), Nigerian Data Protection Regulation (NDPR), California Consumer Privacy Act (CCPA).

INTRODUCTION

Data privacy and data protection is of immense importance both to the users and the companies respectively. The concept of privacy has been considered a fundamental human right of individuals in several jurisdictions as privacy is essential to a free society. Data privacy is deemed to be the right of individuals to determine who has access to their personal information, what personal information is shared and the protection of these information from unauthorised parties who should not have access to them.[1] Data protection on the other hand is considered to be the responsibility of companies in protecting its users personal information from unauthorised use. It involves the enforcement of polices to prevent misuse or unauthorised access to user's personal information and the application of defensive mechanisms against all vulnerabilities to their data collection and storage system.[2] Companies also owe users an explanation on the steps taken with regard to the protection of data from hacks and sales and any form of data intrusion in their privacy policies. The privacy policies are to be on the company's websites explaining to its users the kind of personal information collected, how it is used, with whom it is shared to and how it is secured. Such transparency on how the user's data is collected, whom it is shared with and managed proves to the users that the company can be trusted to handle their personal data with care.

Similarly, the users have a right to give consent to the collection of their personal information and should be given an opportunity to exercise such rights, such as the use of cookies and an option to either consent or disable such cookies on the websites.[3] Users consent is essential in discussing data privacy and data protection. This is because, although a company has ensured that restrictions and other safety measures are placed to accessing user's personal information and such personal information was collected without the users consent such company would still be guilty of breaching a data privacy law. Various countries have now established regulations and policies to protect their citizens personal information. Data privacy laws and regulations are important in enabling individuals freely exercise their fundamental rights of privacy. Privacy entails the right

---

* Bar Aspirant at the Nigerian Law School, 2021/2022 Academic Session.

[1] "What is data privacy?" Available at https://www.cloudfare.com/learning/privacy/what-is-data-privacy/ accessed 30th October, 2021.

[2] "Data privacy vs. Data protection: Understanding the distinction in defending your data" by Expert panel, Forbes Technology Council, 19th December, 2018, 7:00am Est. Available at https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protectionunderstandingthe-distinction-in-defending-yourdata/?shz65d57f4d50c9/ accessed 30th October, 2021.

[3] "Data privacy Laws: what you need to know in 2021" by Angelique Carson, 20th July, 2021. Available at https://www.osano.com/articles/data-privacylaws/ accessed 30th October, 2021.

of an individual to freely exist in one's space without uninvited monitoring. Data protection is an important way in ensuring that companies comply with the laws and also guarantee the privacy of users' personal information.

LEGAL FRAMEWORKS ON DATA PRIVACY AND DATA PROTECTION IN NOTABLE JURISDICTIONS.

The General Data Protection Regulation (EU) 2016/679 (GDPR)

The General Data Protection Regulation (GDPR) has been described as the most essential and comprehensive privacy and protection legislation in the world. This regulation was established by the European Parliament and Council of the European Union on April 14th, 2016 to repeal the Data Protection Directive 95/46/EC. The GDPR took effect on May 25th, 2018 and is established to be the major law regulating the conduct of companies and businesses within or outside the EU in protecting the personal information of EU citizens and residents with regard to the processing and free movement of such data. This regulation applies to all member states of the European Union in order to create a uniform data protection law among EU countries. Companies either with a digital or physical presence which collects or processes the personal data of EU residents and citizens are mandated to comply with the GDPR and a default to this regulation attracts strict penalties and fines.[4]This regulation became a model for several national laws on data privacy and security across the world. By virtue of Article 8(3) of the EU Charter of Fundamental Rights,[5] data privacy and protection are two rights explicitly enshrined in the Charter. Under this provision, EU citizens have a fundamental right to the protection of their personal data.[6] In the same vein, the General Data Protection Regulation (GDPR) has been established to protect the fundamental right of data privacy and protection of EU citizens.

The GDPR comprises of 11 chapters, 99 articles and 173 recitals relating to general privacy principles, rights of data subjects(users'), duties of data controllers, transfer of users' data, liabilities and remedies for breach of rights and other miscellaneous provisions. This regulation

[4] "What is the GDPR? Understanding and complying with GDPR requirements in 2019" by Juliana De Groot, 30th September, 2020. Available at https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection/ accessed 4th November, 2021.
[5] "Charter of Fundamental Rights of the European Union" Official Journal of the European Union C83, vol. 53, European Union, 2010, p. 380.
[6] "Data Protection", available at https://edps.europa.eu/data-protection_en/ accessed 14th November, 2021.

does not apply to the processing of personal information for law enforcement or national security activities of EU member states. Also, where the data is processed for personal or household activities and not for any commercial or economic purposes, the regulation is inapplicable.[7] Salient provisions on data privacy and protection in the regulation include, right of data subjects to withdraw consent at any time,[8] provision of legal basis in which users' personal data can be processed,[9] right of users to transparent information regarding personal data,[10] right of users to access personal information, how it is acquired and processed, the purpose and with whom it is shared,[11] right of erasure which entails right to be forgotten without undue delay,[12] users' right of control and ability to easily transfer their personal data between service providers,[13] right of individuals to object to the processing of personal information for marketing or non-service related purposes,[14] maintenance of reasonable data protection measures by design or default in the company's development and processing setup,[15] swift data breach notification to users' where their rights are at risk because of the breach,[16] requirement of a data protection officer to ensure company compliance with the regulation,[17] and penalties for non-compliance with the regulation.[18]

As contained in the regulation, consent by data subjects must be specific, freely given and a plain-worded affirmation and not through a consent option with an opt-out selection by default structure.[19] Also, as provided in Article 27, non-EU organisations are required to appoint a representative based in one of the EU member states.[20]Another important provision of the GDPR, is the anonymity of the personal data collected to ensure adequate protection and privacy through pseudonymisation as an alternative.[21] Pseudonymisation can be defined as a technology that

[7] Recital 18 of the General Data Protection Regulation (EU) 2016/679 (GDPR).
[8] The General Data Protection Regulation (EU) 2016/679 (GDPR) Article 7(3) (conditions for consent).
[9] *Ibid,* Article 6(1) (Lawfulness of processing). This provision lists six legal grounds for processing personal data, consent, contractual obligation, users' vital interest, public interest, legitimate interest of data controller or third party and compliance with data controller's legal obligation.
[10] *Ibid,* Article 12(Transparent information, communication and modalities for the exercise of data subjects' rights).
[11] *Ibid,* Article 15(Right of access by the data subject).
[12] *Ibid,* Article 17(right of erasure).
[13] *Ibid,* Article 20(right of portability).
[14] *Ibid,* Article 21(Right to object).
[15] *Ibid,* Article 25(Data protection by design and by default).
[16] *Ibid,* Article 34(Communication of a personal data breach to the data subject).
[17] *Ibid,* Article 37(Designation of a data protection officer).
[18] *Ibid,* Article 83(Conditions for imposing administrative fines).
[19] *Ibid,* Recital 32(Conditions for consent).
[20] *Ibid,* Article 27(Representatives of controllers or processors not established in the Union).
[21] *Ibid,* Recital 28(Introduction to pseudonymisation).

enhances privacy and as stated in the General Data Protection Regulation (GDPR), it is the means of processing personal data in a manner that such data can no longer be attributed to a specific data subject without the use of additional information and this additional information is kept separately and subject to technical and organisational measures. [22] It is a useful method in reducing the risks of unauthorised access to the personal data of data subjects and this in turn helps the data controllers and processors fulfil their data protection obligation. Two examples of pseudonymisation are, encryption and tokenisation. Encryption is the process in which an original data is unable to be accessed and it cannot be reversed without the correct decryption key, while tokenisation is a form of data protection which replaces sensitive data with non-sensitive substitutes known as tokens so that the sensitive data is hidden and invisible for processing.[23]

Although the General Data Protection Regulation (GDPR) has been argued to be an effective regulation, there exists some challenges with regard to the compliance of certain requirements of the regulation. Such as the huge cost incurred by companies in order to meet up certain requirements of data mapping, cross-border transfer of data and other data processing activities, these all require a lot of financial commitment to be made. Many companies find it difficult to easily provide or delete data subject's personal information on request and so rely on the GDPR compliance software which discovers and classifies such information. Arguments have also been made regarding how small businesses would cope in adequately complying with the GDPR as they might not have the financial resources to do so. Similarly, arguments have been made that there exists an unclear understanding of the compliance measure of the regulation as well as its effective implementation with regard to blockchain systems. Some international websites in a bid to avoid compliance with the GDPR did block EU users entirely and some others redirected them to lower versions of their services.

Despite the challenges, several companies have complied with the General Data Protection Regulation (GDPR) and made changes to their privacy policies and settings. Also, with the implementation of this regulation, a large percentage of users globally have increased knowledge and awareness on the issue of data privacy and protection as well as their rights and thus affects users' decision-making process on how they use several internet service platforms and websites.

[22] *Ibid,* Article 4(5) (Definitions).
[23] *Ibid,* Recital 28(Introduction to pseudonymisation).

Thereby resulting in a competitive quality for companies which provide these services to comply with the regulations in fulfilling their legal obligation of ensuring adequate data protection on their websites and in their privacy policies and settings.

The California Consumer Privacy Act of 2018 (CCPA).

The California Consumer Privacy Act (CCPA) is a state legislation signed into law on June 28th, 2018.[24] This law was amended on September 13th, 2018 and on October 11th, 2019. The CCPA came into effect on January 1st, 2020[25] although the California Privacy Rights Act was passed later in November 2020 to expand the CCPA.[26] The CCPA is established to protect the personal information of all consumers who falls into the definition of a California resident as provided in the Act.[27] This means that any business[28] which collects or sells the personal data of California residents are subject to this law. The physical location of a business is not regarded and this does not absolve it from complying with the act. This Act contains certain key components such as users right of access and knowledge of all their personal data which a company collects from them,[29] purpose behind the collection and selling of the information,[30] right to choose whether their information be sold to third parties(right to opt-out at any time to the selling of their personal information), categories of third parties a business shares the information with[31] and right to request complete erasure of data[32] etc . The California Consumer Privacy Act (CCPA) has been said to exist on three important principles, accountability, control and transparency.[33]

[24] California Legislative Information Bill Text. Available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 accessed 16th November, 2021.
[25] "2019 is the Year of …CCPA?" by Liisa M. Thomas, Craig Cardon, Brian D. Anderson, Rachel T. Hudson, Snehal Desai, 8th January, 2019. Available at https://www.natlawreview.com/article/2019-year-ccpa-infographic/ accessed 16th November, 2021.
[26] "Move over, CCPA: The California Privacy Rights Act gets the spotlight now" by Cynthia Cole, Matthew R. Baker and Katherine Burgess, 16th November, 2020. Available at https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now accessed 16th November, 2021.
[27] California Consumer Privacy Act of 2018. S. 1798.140 (i) (definition section).
[28] *Ibid* s. 1798.140 (d) paragraph (1)(2)(3).
[29] *Ibid* s. 1798.110(a).
[30] *Ibid* s. 1798.100(a) and s. 1798.115(a).
[31] *Ibid* s. 1798.110(a)
[32] *Ibid* s. 1798.105(a).
[33] "Basics of the California Consumer Privacy Act of 2018" by PrivacyPolicies.com Legal Writing Team, 15th November, 2021. Available at https://ww.privacypolicies.com/blog/california-consumer-privacy-act/ accessed 6th January, 2022.

A notable feature of the California Consumer Privacy Act (CCPA) is that it expanded the definition of personal information to include, geolocation data, personal identifiers, inferences about the users from any of the information identified made by the company to create a profile reflecting users preferences, behaviours and so on and the internet browsing and search history data of the user etc.[34] This Act provides that California residents have a right to bring their data to another service provider or have it deleted completely.[35] Also, under this Act, businesses are mandated to disclose important general information about their privacy practices in a privacy policy on their website and the business' privacy policy should be more transparent, containing in details how data is collected, why it is collected, who it is shared with and the users rights concerning the business practices. Businesses under this Act are mandated to display in their privacy policy a link titled "**Do Not Sell My Personal Information**"[36] and an opt-out option must be clearly displayed in the privacy policy of the business.[37] The California Consumer Privacy Act (CCPA) prohibits businesses from discriminating against users who choose to exercise any of their rights as provided in the Act.[38] Finally, the Act also provides penalties for non-compliance and California residents are permitted to file law suits for privacy losses without any proof of damages or loss of property or money.

In conclusion, it can be stated that the establishment of the California Consumer Privacy Act (CCPA) signifies the era of massive protection of sensitive personal data and guarantees the right of privacy of users and also empowers the users or consumers to an adequate control over the collection, use and sale of their personal data by companies who render such services and obtain their information.

The Nigerian Data Protection Regulation, (NDPR) 2019.

As data remains a critical component of the digital economy, the Nigerian government through its agency, the National Information and Technology Development Agency (NITDA) which is empowered by the NITDA Act, 2007 issued the Nigerian Data Protection Regulation (NDPR) in

[34] Supra note 27. S. 1798.140(v) paragraph 1(A-L).
[35] Supra note 31.
[36] Supra note 27. S. 1798.135(a)(1).
[37] Supra note 27. S. 1798.120.
[38] *Ibid* s. 1798.125(a).

2019[39] to address data privacy and protection in Nigeria. This regulation seeks to comprehensively regulate and control access to user's personal information in Nigeria. With regard to citizens right to privacy, there are several laws in Nigeria that impact data protection regulation.[40] Before the issuance of the Nigerian Data Protection Regulation (NDPR), there was no specific law limited to regulating data privacy and protection.[41] However, as is applicable in most jurisdictions, data privacy and protection stem from the grundnorm of the land, which in this case is the Nigerian Constitution.[42] By virtue of s. 37 of the Nigerian Constitution which protects the rights of citizens to their privacy, privacy of their homes, correspondence, telephone conversations and telegraphic communications as well as any personal information regarding such citizen, it can be said that this section lays the foundation for data privacy and protection rights in Nigeria. Data privacy and protection can thus be deemed to be extensions of a citizen's constitutional right to privacy. Therefore, in a case of breach of privacy whether physical or digital, the citizen or data subject can enforce such right in a court of law under the Fundamental Human Rights Enforcement Procedure (FREP) Rules.

This was held in the decision of the Ogun State High court in *Incorporated Trustees of Digital Rights Lawyers Initiative v L. T Solutions and Multimedia Limited*[43] where the court was of the view that a data subject's right as contained in Article 3.1 of the NDPR, may be enforced just as a constitutional right is enforced under FREP Rules. Similarly, in light of the judgment of the Court of Appeal in the recent case of *Digital Rights Lawyers Initiative v National Identity Management Commission*[44], the court recognised a data subject's right (data privacy and protection) as part of the fundamental right to privacy. Here the Court of Appeal stated that data protection under the NDPR is included under s. 37 of the CFRN and this right to privacy also includes the protection

[39] NDPR- A regulation made by the NITDA by virtue of s. 6 of the National Information and Technology Development Agency, Act (2007). Available at https://nitda-gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf/ accessed 20th December, 2021.
[40] Some of these laws include; The Nigerian Constitution (as amended) 1999, The National Information and Technology Development Agency Act, 2019, The Child Rights Act, Cybercrimes (Prohibition, Prevention Etc) Act, 2015, Central Bank of Nigeria Consumer Protection Framework, 2016, The Nigerian Communications (registration of Telephone Subscribers) Regulations 2011, Freedom of Information Act, 2011 etc.
[41] "Data Privacy and Protection under the Nigerian Law" by Francis Oloho (S.P.A. Ajibade and co.), 19th February, 2020. Available at https://www.mondaq.com/nigeria/privacy-protection/895320/data-privacy-and-protection-under-the-nigerian-law/ accessed 20th December, 2021.
[42] Constitution of the Federal Republic of Nigeria 1999(as amended) Act No. 24, 5th May, 1999.
[43] Suit No. HCT/262/2020.
[44] Suit No. CA/IB/291/2020.

of a person's personal information from others or persons unauthorised to have access to them. Therefore, every citizen has the right to ensure the privacy and protection of his or her data and such right is guaranteed under the Constitution.[45]

The Nigerian Data Protection Regulation (NDPR) is the most comprehensive legislation containing provisions which protects data privacy in Nigeria. This Regulation comprises of four (4) parts with part one focusing on the objectives of the regulation, scope of the regulation and definition sections. Article 2.1 contains the governing principles for data protection, which includes, the lawful collection and processing of personal data[46], consent obtained from the data subject before such collection and processing[47], the data subject has the right to withdraw consent at any time, consent must be obtained without fraud, coercion or undue influence, also any medium through which personal data is collected is required to display in a simple and understandable manner, their privacy policy.[48] Article 2.6 provides for some possible data protection measures[49] to include, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals etc[50], Article 2.8 provides for the right of a data subject to object to the processing of his data[51], the regulation also provides punishment for offenders[52], Article 3.1 contains the rights of a data subject, right to be informed of the appropriate measures adopted in safeguarding his data in a foreign country, right to data portability, right to request erasure of personal data etc. Article 4.2 provides for an administrative redress panel to investigate in a case of an allegation of breach of the regulation.[53]

Conclusively, the establishment of the National Information and Technology Development Agency Regulation and the Nigerian Data Protection Regulation (NDPR) is a commendable feat as it portrays a significant step in Nigeria towards being abreast with the digital revolution and

[45] "The Constitutionality of the Right to Data protection under Section 37 of the CFRN in Light of the Court of Appeal Judgment" by TechLaw Space.
[46] Nigerian Data Protection Regulation (NDPR), 2019. Article 2.2(Lawful Processing).
[47] *Ibid* Article 2.3 (Procuring consent).
[48] *Ibid* Article 2.5 (Publicity and Clarity of Privacy Policy).
[49] *Ibid* Article 2.6 (Data Securing).
[50] "Managing Data Privacy issues in Corporate Restructuring: Key Considerations for Investors" by Emmanuel Omoju and Patience Ajogbor, 1st December, 2020.
[51] Nigerian Data Protection Regulation (NDPR), 2019. Article 2.8 (Objections by the Data Subject).
[52] *Ibid* Article 2.10 (Penalty for Default).
[53] "Actions Beyond the Nigerian Data Protection Regulations (NDPR) 2019" by Gabriel Omoniyi, 30th December, 2020. Available at https://www.mondaq.com/nigeria/data-protection/1020784/actions-beyond-the-nigerian-data-protection-regulations-npdr-2019#_ftnref35/ accessed 6th January, 2022.

further emphasises the approval and value of safeguarding the digital rights of citizens within Nigeria. The establishment of this data privacy and protection legislation and the lauded decision in *Digital Rights Lawyers Initiative v National Identity Management Commission*[54] which aligns with the position that data protection is not a right provided for in the NDPR alone but it is a constitutional and fundamental right provided for in the Constitution therefore acknowledges the rights of persons to preserve their right of privacy as guaranteed under the Constitution.[55]

OVERVIEW OF CHALLENGES ENCOUNTERED IN DATA PRIVACY AND PROTECTION.

Data privacy and protection laws has been considered an amazing achievement, however there exists a lot of challenges with the protection of user's data.

1. Massive growth of data

Organisations are expected to adequately ensure the protection of user's personal information from any form of data breach and with the growing nature and volume of data in our technologically driven world it becomes overwhelming to handle the billions of data. Also considering the various data privacy legislations and the complexity of its rules, there is a doubt that absolute compliance is even possible.

2. Conflict of laws

With the existence of several legislations on data privacy and protection, the possibility of conflict between several laws could often pose a lot of challenge to organisations whose users cut across various continents and affect their ability to adequately comply with each countries data privacy laws. For example, in relation to the definition of certain terms like data privacy, data subjects' consent, withdrawal of consent, right of erasure etc, which may often differ among the laws of several countries and this sometimes affect organisations decision as to determine what data privacy law to apply to their users.

[54] Supra Note 35.
[55] "An Extensive Article on Data Privacy and Data Protection Law in Nigeria" by Uche Val Obi SAN, 9th September, 2020. Available at https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/ accessed 6th January, 2022.

3. Cost of maintaining data privacy and security

The cost of rectifying a data breach results in a huge loss of revenue to an organisation as such organisation faces intense regulatory penalties. Organisations are expected to adopt and take appropriate steps to ensure that adequate and specific security technologies are provided for, such as data backups and archiving in order for data to be safeguarded, recovered and restored.

4. Human Error complexities

Many data analysts have stated that human error is considered to be the biggest challenge in data privacy[56], for instance a lack of awareness by employees can significantly affect an organisations data privacy and protection system. This can occur through the use of weak passwords, falling for phishing scams etc and thus could result in user's data becoming vulnerable and lead to data loss.

RECOMMENDATIONS

To effectively ensure the privacy and protection of user's personal data, both the organisations collecting and processing the data as well as the users are to adopt appropriate and essential steps.

Organisations

1. Empowerment of employees to be aware of the need for data privacy and security through the creation of security awareness and training programs for old and new employees and thereby reducing the risk of data loss.
2. Implementation of data loss prevention and security tools to help prevent employees or users from leaking sensitive data and to reduce the risk of attack.
3. Ensuring the consistent monitoring of the organisations' network and systems in order to detect any suspicious activities or attacks early.
4. Implementation of zero trust models which would restrict access to the organisations network by outsiders or unauthorised third parties.
5. Ensuring that the policy enforcement and protection mechanism of the organisation is easily implemented by all users, devices, data and application irrespective of where the users are connected from.

[56] "The Five Biggest Challenges in Global Data privacy and Protection" https://cipher.com/blog/the-5-biggest-challenges-in-global-data-privacy-and-protection-/ accessed 6th January, 2022.

Users

1. Familiarizing themselves with privacy tools, such as password managers which is an encrypted virtual private network to protect the user's internet connection. A good password should be long, complex and as hard to guess as possible. The same password should not be used for all the users accounts.
2. Periodically scanning your device with trusted antivirus software to locate and remove any malicious threats to your device and backup your data often.
3. Be on guard for any strange request, flashing click bait content and things that may seem fake or suspicious. One way to prevent such phishing is to avoid entering your personal information on any site you did not visit, search or bookmark on your own.
4. Users are advised to only share their personal information with companies that are open and honest about their data privacy policies and who would not sell their information with the aim of accumulating massive rewards and are lax on protecting user's data.
5. Users are to be aware that a number of companies use and store their personal data, therefore they should avoid sharing a lot of their personal data as the users have a fundamental right to privacy of personal information.
6. Awareness of users of their legal rights to privacy and the legal responsibilities of organisations to ensure the adequate protection of their personal data.

CONCLUSION

Data privacy entails the right of an individual to freely exist in one's space without any unwanted surveillance and data protection is an important way of ensuring that organisations and companies both comply with the laws and also guarantees information privacy. Organisations have the responsibility of protecting the user's personal information and transparency by these organisations and companies on how user's data is collected, managed and when such information is shared builds trust in the users. Hence, data privacy and protection aim essentially not only to protect the users but also to ensure that the companies and organisations are entrusted with the responsibility of protecting user's personal data and are held liable for any data security breaches.