Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

Cite this article as:

MS. NANDINI TRIPATHY, "*Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR",* Vol.3 & Issue 3, Law Audience Journal (e-ISSN: 2581-6705), Pages 302 to 306 (5th February 2022), available at ***https://www.lawaudience.com/big-data-privacy-and-data-protection-a-case-study-analysis-under-gdpr/***.

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

Publisher Details Are Available At:

https://www.lawaudience.com/publisher-details/

Editorial Board Members Details Are Available At:

https://www.lawaudience.com/editorial-board-members/

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

ABSTRACT:

"Big data is proven to be a valuable asset for many businesses, allowing for greater processes and business opportunities. Big data, on either hand, has given a lot of people more access to sensitive information that, when handled, could endanger people's privacy and violate data protection. As a result, data controllers may face serious penalties, even bankruptcy, if they really do not conform. The volume of data processed, saved, and gathered is increasing rapidly as even more devices access the internet and each other, posing new data security problems[1]".

I. CHALLENGE OF BIG DATA AND SECURITY:

When dealing with ***"big data",*** solutions do not meet the standards for ensuring security and privacy. Big data solutions frequently rely on traditional firewalls or application layer execution to limit access to information, but firewalls transport security layers; data source can be unknown, and anonymised data can be re-identified. For any of these reasons, advanced techniques are being introduced to verify, secure, and monitor huge amounts of data in areas such as infrastructure, security, and management.[2] According to the ***National Institute of Standards and Technology***, cloud computing is a paradigm for providing internet connectivity to a pool of computing investments ***(e.g., networks, servers, storage, applications, and services)*** that can be quickly supplied and released with very little proper coordination or provider affiliation ***(NIST).***

II. DATA PROTECTION:

A system typically contains a large volume of personal data or information that corporations can use to gain a competitive advantage. As a result, we should consider where the limit for the usage of such information is. So, in order to use data securely while also protecting privacy, we must first comprehend the privacy dangers connected with big data. While big data has many advantages for businesses of all kinds, it also poses a number of severe privacy issues,

[1] ISACA: Privacy and Big Data (2013). http://www.isaca.org (last accessed on 27th November 2021).
[2] World Economic Forum: Personal Data: The Emergence of a New Asset Class (2011), www.weforum.org/reports/personal-dataemergence-new-asset-class (last accessed on 27th November 2021).

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

including: ***(1). Data Breach (2), Data Brokerage (3), and Data Discrimination*** are all examples of data breaches.[3]

III. REGULATORY FRAMEWORK IN INDIA:

The Information Technology Act of 2000 ("IT Act"), as well as the rules enacted under it, provides legal principles for data protection, covering data collection, storage, disclosure, and transfer. ***The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "SPDI Rules")*** necessitate whatever organisation that processes, deals with, stores, or handles sensitive personal information in a computer system that it owns, controls, or operates to obey procedures and measures. Several other Indian laws, in addition to the IT Act and the SPDI Rules, can apply to data protection, depending on the entity collecting the data and the type of data collected.[4]

IV. REGULATORY FRAMEWORK IN THE EU:

The mere fact that a browser is available in the EU is inadequate to expose the business to GDPR; nevertheless, other evidence of a company's intent to offer goods or services in the EU may be relevant. Companies that are not based in the EU but are subject to GDPR must appoint an EU representative for GDPR compliance reasons in written. Small-scale, non-sensitive processing of data on a routine basis is exceptions to the general rule.

The European Data Protection Board (EDPB) is an independent European organization charged with ensuring that data protection rules are applied uniformly across the EU. ***"The EDPB is established by the General Data Protection Regulation (GDPR) (GDPR)".*** The European Data Protection Supervisor or national data protection authorities from EU/EEA countries are included on the EDPB. The European Commission engages in the operations and

[3] Katal, A., Wazid, M.: Big data: issues, challenges, tools and good practices. In: IEEE 6th International Conference on Contemporary Computing (IC3). Department of CSE, Graphic Era University, Dehradun, India (2013) (last accessed on 27th November 2021).

[4] Abid, M., Iynkaran, N., Yong, X.: Protection of big data privacy. IEEE Access **4**, 1821–1834 (2016). https://doi.org/10.1109/ACCESS.2016.2558446 (last accessed on 27th November 2021).

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

meetings of a Board but does not have a vote. The EDPS supplies the secretariat again for EDPB. The secretariat implements the Chair of the Board's orders to the code. Personal data processed by an admin who has never had any units in the EU but has an organization in a nation in which the EU Member State's public rules apply.

OECD Privacy Principle 3- Purpose Specification:

Personal data collection objectives should be specified no later than the time of collection, and future usage should be limited to achieving those goals or additional goals that are not incompatible with the primary purposes.[5]

OECD Privacy Principle 4: Use Limitation:

Personal data shall not be shared, made available, or used for purposes other than those mentioned in paragraph 9 of the OECD recommendation unless: ***a) with the consent of the data subject; or b) with legal authorisation (which would be related to the OECD privacy principle 3 – Purpose Specification).***

OECD Privacy Principle 5:

Security Measures Loss or unauthorized access to private data, including its removal, usage, alteration, or publication, should all be safeguarded by adequate security safeguards.

OECD Privacy Principle 6: Openness:

It is necessary to implement a broad policy of accountability for personal data developments, procedures, and rules. The ability to show the existence and nature of private information, as well as the primary purposes for which it is used, as well as the identity and usual residency of the data controller, should all be made public.

OECD Privacy Principle 7: Individual Participation:

Individuals must be able to: ***a) obtain verification from a data principal, or other, that the data processor holds personal details concerning them. b) to have data on them communicated to them in the following manner: i. in a reasonable amount of time; ii. for a***

[5] Pierre-Luc, D.: Privacy and social media in the Age of Big Data. House of Commons, Canada (2012) (last accessed on 27th November 2021).

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

reasonable fee, if applicable; iii. in a reasonable manner; and iv. in a format that they can understand. c) to receive notification of the reasons for the demand.

V. BIG DATA INTEROPERABILITY FRAMEWORK:

On June 19, 2013, ***the NIST Big Data Public Working Group was established. (NBD-PWG)***. A Working Group's goal is to create a common Big Data framework ***(also known as the "NIST Big Data Interoperability Framework")***. The NIST Big Data Interoperability Framework consists of seven documents ***(referred to as "volumes")*** that cover core Big Data concerns and were prepared by five NBD-PWG subgroups. The NIST Big Data volumes are still in written form and are directed largely at US businesses.[6]

The NIST approach must be evaluated against by the European Data Protection Strategy, that may have consequences for how privacy is managed. Security and Privacy Subgroup The NIST Big Data Security & Privacy Subgroup released the final draft of Volume 6 on Security and Privacy in September 2015, and it covers, among many other things, the following topics. Security and Privacy Taxonomies; NIST Big Data Reference Architecture Security and Privacy Fabric (NBDRA).[7]

VI. BIG DATA GOVERNANCE:

Information and communication technology advancements are fast connecting the surrounding environment with massive amounts of data. As a result of this occurrence, advanced data technology has emerged among scientists and engineers all over the world, especially in the study of big data. The importance of adhering to business standards and older industry laws grows as data technology progresses. To undertake impact analysis, a robust governance

[6] Hasan, O., Habegger, B., Brunie, L., Bennani, N., Damiani, E.: A discussion of privacy challenges in user profiling with big data techniques: the EEXCESS use case. In: 2013 IEEE International Congress on Big Data, Santa Clara, CA (2013) (last accessed on 27th November 2021).

[7] Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M.: Privacy issues and data protection in big data: a case study analysis under GDPR. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 5027–5033. IEEE (2018) (last accessed on 27th November 2021).

Law Audience Journal, Volume 3 & Issue 3, 5th February 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 302 to 306,

Title: "Big Data Privacy and Data Protection: A Case Study Analysis Under GDPR", Authored By: Ms. Nandini Tripathy (LL.M), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, Email Id: nandini.tripathy121@gmail.com.

system must be able to audit additional data modifications, detect data offspring, and allow role-based data access.[8]

VII. CONCLUSION:

Big Data Analytics carries weight. Not only for companies, but also for politicians, regulators, and customers, Big Data Analytics has become more prominent. As a consequence, Big Data Analytics does have a lot of potential for both firms and customers. The new EU Regulation is a significant step forward in terms of allowing business innovation via Big Data Analytics. However, we believe that incorporating privacy and data protection principles into Big Data Analytics systems and projects from the start will enable businesses to not only fully exploit the capabilities of Big Data Analytics, but also to distinguish themselves from competitors who may face complaints and potential sanctions.[9]

As a result, in order to boost company efficiency and innovation, institutions must follow the ***'important privacy & data protection principles,'*** as well as provide GDPR-compliant privacy and data protection, as well as user-friendly Big Data Analytics solutions, by properly applying controls. Continuously developing and constructing privacy and data protection controls. As a result, businesses must set up a privacy and data protection (risk) management system to identify, mitigate, and manage associated risks in line with their risk appetite. To accomplish this goal, new, innovative, and efficient solutions for securing personal data processed in the context of Big Data Analytics must be considered. To build solutions, legal and technological tools should be used in unison.

[8] Ng, W.S., Wu, H., Wu, W., Xiang, S., Tan, K.L.: Privacy preservation in streaming data collection. In: IEEE 18th International Conference on Parallel and Distributed Systems. Institute for Infocomm Research, A*STAR, Singapore (2012) (last accessed on 27th November 2021).

[9] Bachlechner, D., La Fors, K., Sears, A.M.: The role of privacy-preserving technologies in the age of big data. In: WISP 2018 Proceedings, vol. 28 (2018) https://aisel.aisnet.org/wisp2018/28 (last accessed on 27th November 2021).