CHANGE OF OUTLOOK FOR MODERN DATA PROTECTION PRACTICES

- **Abstract**

The regulations adopted by several countries relating to data protection have become kind of onerous on the companies as they struggle to ensure that their practices do not land them on the wrong side of the law. However, some of the major reasons to become data protection law compliant as claimed by the companies are to support company's values; meet customer or third party expectations rather than the fear of fines or class action litigation against the companies. But is it true that the data regulation compliances are not because of the fear of fines when they can be to the tune of 4 percent of company's global revenue or 20 million Euros whichever is greater as in the case of GDPR? Companies are realising slowly that it is not just an Information technology issue to comply with these regulations but one that affects various other operations in the company such as the sales and marketing especially. Companies are required to be constantly reviewing and adjusting their processes and systems to ensure effective personal data protection and protect the right of privacy of its customer and third party. One of the problems with these data protection regulations are the ambiguous requirements for example, how much effort and level of protection is reasonable? How does one assess the "likelihood of risk to rights and freedoms"? Thus the author discusses the difficulties faced by the companies in effective implementation of such laws.

Keywords: *GDPR, Data protection, data privacy, personal data, difficulties in compliance*

- **Introduction**

Various developed countries have already adopted Data protection regulations and some of the countries such as India are on the anvil of adopting such laws. One of the most talked about across all kind of stakeholders is the European Union's General Data Protection Regulation (EU GDPR). To comply with these regulations has become a necessary condition for all businesses especially those having any connect or reach to the EU. The businesses want to ensure that they are following the right approach and practice so that their actions or pursuit does not violate any of these regulations.

It is interesting to note that in one of the independent research, conducted by Dimensional Research on behalf of TrustArc, reports that some of the major reasons to become data protection law compliant as claimed by the companies are to support company's values; meet customer or third party expectations rather than the fear of fines or class action litigation against the companies.[1] But is it true that the data regulation compliances are not because of the fear of fines when they can be to the tune of 4 percent of company's global revenue or 20 million Euros whichever is greater as in the case of GDPR?

Companies are realising slowly that it is not just an Information technology issue to comply with these regulations but one that affects various other operations in the company such as the sales and marketing especially. Companies are required to be constantly

[1]*GDPR Compliance Status: A Comparison of US, UK and EU Companies*, TRUSTARC [Accessed 15 Jul. 2018].

reviewing and adjusting their processes and systems to ensure effective personal data protection and protect the right of privacy of its customer and third party. One of the problems with these data protection regulations are the ambiguous requirements for example, how much effort and level of protection is reasonable? How does one assess the "likelihood of risk to rights and freedoms"? Thus the authors discuss the difficulties faced by the companies in effective implementation of such laws. Also one of the other objectives of this research paper is to provide a roadmap for effective implementation of data protection laws.

- **Are the companies complying with data protection rules due to fear of fines?**

As mentioned in the introduction one of the researches carried out by Dimensional Research for TrustArc suggests that there are other reasons for the companies to comply with data protection rules and the fear of fines is not one of the main considerations. The research team surveyed 600 Information Technology, legal, and privacy professionals from the region of US, UK and other EU countries. Also the respondents were from all size companies, small, medium and large, representing major industry sectors. This research report portrays that the companies complied with the data protection laws mostly to meet customer expectations, support their company values or meet third party requirements. The fear of fines or class action lawsuits was not the main motivator to comply with the data privacy regulations.

The number of fines imposed in EU since July 2018 has progressively increased. One of the databases shows that until November 2020, 395 times the fines were imposed summing up to € 245,792,094. It is interesting to note the violations for which the fines have been imposed maximum number of times. Some of them being: 169 times the fines were imposed for insufficient legal basis for data processing; 88 times the fines were levied for insufficient technical and organisational measures to warrant information security; 70 times fines charged for not complying with general data processing principles.[2]

The sectors in which the highest fines were levied in are as follows:

(i) Media, Telecom and Broadcasting
(ii) Industry and Commerce
(iii) Transportation and Energy
(iv) Accommodation and hospitality
(v) Insurance, Finance and Consultation
(vi) Education and Public Sector
(vii) Healthcare
(viii) Private Entities, Individuals and others[3]

The initial months of GDPR enforcement witnessed that most European Data Regulators in countries worked with preliminary investigations, general recommendation and applied small amount of fines. Later towards the end of 2018, big social media companies such as

[2]Enforcementtracker.com. (2018). *GDPR Enforcement Tracker - list of GDPR fines*. [online] Available at: https://www.enforcementtracker.com/?insights [Accessed 19 Dec. 2020].

[3]*Ibid.*

the Facebook and Twitter and other internet companies like Google faced huge penalties for not being transparent about the process of personal data collection for advertising. It is elusive to think that the data protection regulations are focused on large businesses and corporations as evidence shows that even small and medium size businesses have been levied fines for failure to comply with the law.[4]

Given the scenario hardly any business would like to take chance of not complying with such stringent regulations such as the GDPR whose primary goal of heavy sanctions is to have a deterrent effect. Though currently, there is huge criticism that the Irish Data Protection Authority has failed to act against the US Tech giants in the matters of Data Protection.[5] However, most companies knowing that the fines could have a huge impact on their bottom line prefer prevention over cure. While the companies have to spend on complying with the new data protection regimes, they are looking at it as an opportunity rather than a threat, displaying a positive attitude, which is good for all stakeholders in the long run. The opportunity on one hand is in terms of stepping up their own data security protocols and methods and on the other hand to portray that they are data privacy compliant company and believe in protecting privacy of consumers. The crux of matter is that the companies view data protection and privacy compliance not only as an information technology issue alone, but also are considering its strategic value in operations, sales and marketing.

Establishing the fact that the companies are willing to comply with the data protection regulations for one reason or other, and understanding that they are required to review and modify their procedures and systems to provide for effective and efficient mechanism for data protection and right of privacy of customer and third party, the omnipotent problem is the ambiguity in data protection laws.

- **Ambiguities in the data protection laws**

In one of the studies the authors examined the legal grounds for processing data, that is 'when can one collect and use data?' according to the GDPR. This study also addresses the provisions relating to profiling (which may be by automated or non-automated means). The authors contend that due to the ambiguity in Article 22 of the GDPR, many profiling activities may fall outside the scope of Article 22. The authors state that the vagueness and subjectivity of various relevant GDPR provisions can weaken legal certainty.[6]

In an ethnographic study conducted in Sweden, from January 2017 to April 2017, by Alison Cool, the findings regarding the GDPR were that the data law was complex, maybe flawed, but definitely not unknowable.

---

[4]Kovalenko, I. (2019). *One Year After GDPR: The Lessons Digital Businesses Have Learned*. [online] dzone.com. Available at: https://dzone.com/articles/one-year-after-gdpr-the-lessons-digital-businesses [Accessed 07 Jun. 2019].

[5]Voss, W. Gregory & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL [Accessed 2020].

[6]Elena Gil González & Paul de Hert, *Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data - An analysis of GDPR Provisions and Principles*, 19(4) ERA FORUM 597-621 [Accessed 2019]

An interesting perspective of the ambiguity in data protection law was where the researchers saw it as a part of its strength and flexibility. If the law was ambiguous or vague and difficult to interpret, it was attributed not to the failure of law, but the unruliness and instability of technology. On one hand the technical researchers find the law as inexplicable, on the other hand legal experts see technology as the reason of uncertainty. Nonetheless, question remains: What does the provision mean? What is one expected to do?[7]

In yet another important study conducted by two authors using the adversarial case study of more than 150 businesses, demonstrated that the legal ambiguity relating to the provisions on 'Right of Access' may be abused by social engineers. The findings state that many businesses do not utilise sufficient safeguards against the abuse of Right of Access, which leads to risking sensitive information. [8]

The ambiguities may be inevitable in such technology neutral data protection laws and regulation as there are constant transformations in the field that is subject matter of governance. Probably it needs to be vague and use broader terms so that the law need not be amended time and again as the technology transforms.

- **Difficulties faced by companies in effective implementation of data protection law**

The GDPR became applicable in EU from 2018 and the companies were given a two year time to become GDPR compliant.[9] Some of the most important challenges that the companies have faced in becoming complaint to data protection laws such as the GDPR is the complexity of the regulation, shortage of qualified personnel and privacy experts required to deal with the complexities, efficiently protecting the data subjects' rights, and carrying out impact assessments.

McKinsey's research portray that some businesses feel fully complaint, the remaining feel a bit unprepared for GDPR and are using temporary controls and processes to comply till they will be able to implement more lasting solutions. Further as per the report there is an increase in requests from data subjects to access personal records and the challenge of keeping data secure is growing rapidly. Thus the businesses have to pay attention to security controls, management of data and automation.[10]

---

[7]Alison Cool, *Impossible, Unknowable, Accountable: Dramas and Dilemmas of Data Law*, 49(4) SOCIAL STUDIES OF SCIENCE, 503-530 (2019)

[8]Pavur, J. and Knerr, C. (2019). *GDPArrrrr: Using Privacy Laws to Steal Identities*. [online] arXiv.org. Available at: https://arxiv.org/abs/1912.00731 [Accessed 19 Dec. 2020].

[9]Bindu Ronald et al., *GDPR:Legal Impact on Extra-territorial Commercial Pressure on Indian Business, Trade and Investment*, Conference Proceedings – Seventh International Conference on *The Next Seven Years of The European Union*, 45 (2019)

[10]Mikkelsen, D., Henning Soller, Malin Strandell-Jansson and Wahlers, M. (2019). *GDPR compliance since May 2018: A continuing challenge*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge [Accessed 19 Dec. 2020].

One of the challenges in complying with data protection regulation is that the businesses are expected to have taken consent to use the data of the data subject. The consent needs to be a positive affirmative action rather than a negative action such as neglect of taking decision against. Thus the consent needs to get recorded in such a way that it is auditable. Further while seeking consent the information provided must not be misleading or intimidating.[11] The data subjects could be the employees of the business too. There is a requirement to take proper consent from them as well in case of processing their personal data. For example in July 2019, PwC was fined € 150,000 by the Greek Data Protection Authority (GDPA) for unlawful processing of its' employees personal data. The GDPA found that the company had processed the personal data in an unfair and non-transparent manner. The legal basis claimed by the company for using their data was consent. However consent did not seem to be reasonable legal basis as consent may not be considered free in an employer-employee relationship where employer seems to be in a power position. The data was being actually used for a different legal basis for which the employees were never informed. The legal basis under which the data was being used was either performance of contract, compliance with a legal obligation or legitimate interest.[12]

Further the data protection laws provide the data subjects with the right to erasure also known as the right to be forgotten, by way of which the data subject can initiate a request with the data controller to remove any data relating to that data subject that the business may be holding in any form (on paper or online). To comply with this requirement the businesses need to ensure that the personal data of the data subject is deleted in all forms and from backups and archives. Ensuring that the data is deleted from all possible storages and archives can be a daunting task. As far as one's own organisation or business set up is concerned one can be sure of that it has been deleted. But what if such personal data was shared with third party? How is one to ensure that the third party will erase such data on request? These are the complexities in terms of fulfilling the obligations under the data protection regulations.

In any given business set up, a few personnel understand the data protection law and its requirements and the severity of not complying with it. Does every other employee who deals with the personal data of data subjects take seriously the rights of data subjects? Are these employees made aware of the repercussions on the business of the failure to protect the data subjects' rights? The accountability principle is difficult to fulfil unless the employees are sufficiently trained, made aware and responsible for the actions in regard to handling data. The protocols established must be rigorously followed while trying to bring an attitudinal change in the employees who will respect each one's data as if their own.

Strengthening the data protection regime is often at crossroad with other regulatory necessity for example regulations requiring sharing of scientific data and promoting open

---

[11]Northdoor. (2017). *Five Common Challenges Organisations Face with GDPR | Northdoor*. [online] Available at: https://www.northdoor.co.uk/five-key-challenges-around-gdpr [Accessed 19 Dec. 2020].

[12]THE GREEK DATA PROTECTION AUTHORITY ISSUES A GDPR FINE AGAINST PWC FOR UNLAWFUL PROCESSING OF PERSONAL DATA OF ITS EMPLOYEES. (n.d.). [online] Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/08/greek-dpa-fines-pwc-for-unlawfully-processing-the-personal-data-of-its-employees.pdf [Accessed 19 Dec. 2020].

data frameworks.[13] Research companies and organisations that deal with EU scientists to share data are required to sign contracts that guarantee safeguarding of the data. Standard contracts require that European companies must audit the data systems and also require submission to the jurisdiction of EU courts. This is not acceptable to many non-EU companies and research organisations.[14]

The compliances of GDPR or any other data protection regulation gets even tougher for the Small and Medium Enterprises (SMEs). In Europe more than 99% of all businesses are SMEs, which means having less than 250 employees. Complying with GDPR can be a costly affair for them. And the chances that the enterprise does not follow GDPR can become evident anytime as anyone can complain.

- **Roadmap for effective implementation**

One of the mistakes businesses make is misinterpreting the requirements under the data protection laws. Example in the case of Google, it faced action as it did not centralise the process of user data collection on a single page. It required users to perform multiple actions. And even after completing these actions the users were not aware about the extent to which their personal data would be put to use. As per the GDPR, a separate consent form is required for each data processing goal.[15]

Following are some of the important take away for businesses wanting to be data protection compliant and for the companies to review their existing compliance:

(i) Ensure proper documentation required by the law - for example in the case of GDPR documents such as:

- ✓ Privacy Policy,
- ✓ Privacy Notice (Articles 12, 13 and 14),
- ✓ Cookie Policy, Disclaimer on cookie processing,
- ✓ Clear and concise consent form from Data Subjects (Articles 6,7 and 9)
- ✓ Personal Data Protection Policy (Article 24),
- ✓ Data Retention Policy (Articles 5, 13, 17 and 30) and Data Retention Schedule (Article 30)
- ✓ Parental Consent Form (Article 8)
- ✓ Data Protection Impact Assessment (Article 35)
- ✓ Supplier Data Processing Agreement (Articles 28, 32 and 82)
- ✓ Response to Data Breach and Procedure for Notification (Articles 4, 33 and 34)
- ✓ Data Breach to be notified to all data subjects (Article 34)

[13]Jane Kaye, *The Tension Between Data Sharing and The Protection of Privacy in Genomics Research*, 13 ANNUAL REVIEW OF GENOMICS AND HUMAN GENETICS 415-431 (2012).

[14]Rabesandratana, T. (2019). Researchers sound alarm on European data law. *Science*, [online] 366(6468), pp.936–936. Available at: https://inb-elixir.es/sites/default/files/news/20191122_Science_Researchers_sound_alarm_on_European_data_law.pdf [Accessed 22 Nov. 2019].

[15]*Supra* note 4.

There are many other documents which may be required under certain conditions and there are best practices of maintaining certain non-mandatory documents as well, a list of which can be referred at the website of EU GDPR Academy.[16]

(ii) One of the expectations of the Data Protection Authorities is that the data controllers must provide in their privacy notices, references to the specific provisions of the data protection laws of the relevant countries rather than generically mentioning compliance to EU GDPR. Also the Data Controllers are expected to use unambiguous explanations and provide clear and detailed information on the following aspects[17]:

- ✓ Identity of the data controller and their representative
- ✓ Purpose of processing data
- ✓ Third parties to whom data may be transferred and purpose of such transfer
- ✓ Legal grounds and the processes applied for data collection
- ✓ Data subject rights

(iii) Need careful consideration on storing and managing consent related documents in a secure and efficient system. There may be multiple parties (employees, vendors, suppliers, marketing agencies etc) from whom consent is received. In such a case centralised system for secure receiving, storage and retrieval of such consent related information would be ideal.

(iv) Automated systems designed to deal with requests relating to erasure of personal data, affecting the erasure from all internal and external storage and confirming to the data subject about erasure, all to be carried out in a timely manner. Also such automation should be able to ensure that personal data which may have been shared with any third parties also is erased by the third party in efficient manner.

(v) The business entity must conduct regular training of all employees handling or processing any personal data whether of employees, third party or consumers to ensure accountability at all levels in the business entity.

---

[16]Dejan kosutic, EUGDPRAcademy. (2020). *GDPR documentation requirements: Policies and procedures*. [online] Available at: https://advisera.com/eugdpracademy/knowledgebase/list-of-mandatory-documents-required-by-eu-gdpr/ [Accessed 19 Dec. 2020].

[17]İlay Yılmaz, Can Sozer and Dilşad Sağlam (2019). *Data Protection Authority Addresses GDPR Based Privacy Notices*. [online] Lexology.com. Available at: https://www.lexology.com/library/detail.aspx?g=20b01f92-b81a-46bc-b456-020b51a153de [Accessed 19 Dec. 2020].