EFFECTIVE DATA PRIVACY NORMS FOR A FIRM: A NEED OF HOUR

- **Abstract**

Defining appropriate company policies in the realm of data protection is key, given that a flawed company policy impacts data subject's rights and the firm thus becoming liable for severe financial penalties under General Data Protection Regulation (GDPR), as apparent from the recent fine levied on H & M. With the current global pandemic, more work is being executed online than ever before and this has resulted in more exposure of private data. Understanding the data privacy laws and implementation of technical and organizational measures by firms to ensure compliance is no longer a luxury.

The objective of this paper is to recommend how company policies need to be revamped to address contemporary data protection legislations like EU GDPR, and on the anvil, Indian Personal Data Protection Bill 2019, in the context of changing work patterns like Bring Your Own Device and Work From Home.

The purpose of this paper is not only for the top management of firms but also aims to percolate this urgent imperative to the grassroot level. While it is a given that it is virtually impossible to ensure that millions of peoples' private data may never be compromised again, this paper is a step towards this virtual reality, focusing on the base of the organization's pyramid.

Keywords: *Information Security, Data Protection, Data Privacy, Personal Data, GDPR, Data Protection officer (DPO), Technical Measures, Data Protection & Security – Imperative for Firms*

- **Introduction To Data Protection & Security Imperative For Firms**

Protection of personal data has assumed greater prominence in recent years with the proliferation of health data breaches caused by cyberattacks and ransomware attacks on the custodians, in most cases, firms. It has been resulted in enactment of several regulations that provides data privacy and security provisions for safeguarding personal information have been promulgated, the gold standard being EU GDPR. These regulation has imposed several liabilities on the firms, lack of robust data protection measures could result in negative impact to a firm's reputation and could result in steep fines imposed by regulators. The GDPR Enforcement Tracker, 2020 provided below demonstrates type of Violation and Quantum of Fines imposed by the regulators (ref. Table 1).

	Violation	Sum of Fines
	Insufficient legal basis for data processing	**€ 164,364,648** (at 162 fines)
	Insufficient technical and organisational measures to ensure information security	**€ 152,787,807** (at 85 fines)
	Non-compliance with general data processing principles	**€ 17,574,465** (at 66 fines)
	Insufficient fulfilment of data subjects rights	**€ 9,534,225** (at 42 fines)

	Violation	Sum of Fines
	Insufficient fulfilment of information obligations	**€ 568,305** (at 20 fines)

Table 1 GDPR: Type of Violation and Quantum of Fines[1]

When GDPR was introduced in 2018, little did the firms realized the impact of the regulation and the rigor of enforcement. More than 330 Million Euro fines have been levied till date for the violation of the GDPR principles and rights of data subjects. Firms provide products and services that handle personal information and must have security features in place to ensure compliance.

The requirements to be considered by firms for ensuring compliance to GDPR and similar data privacy regulations must serve an input for formulating firm level policies, procedures and organization roles relating to data privacy and protection. The challenges to firms (Diagram 1) and a recommended approach for ensuring a proactive response by firms is depicted in Diagram 2

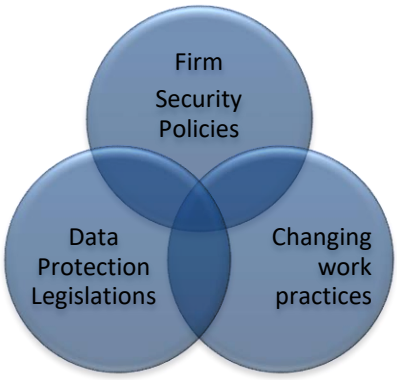
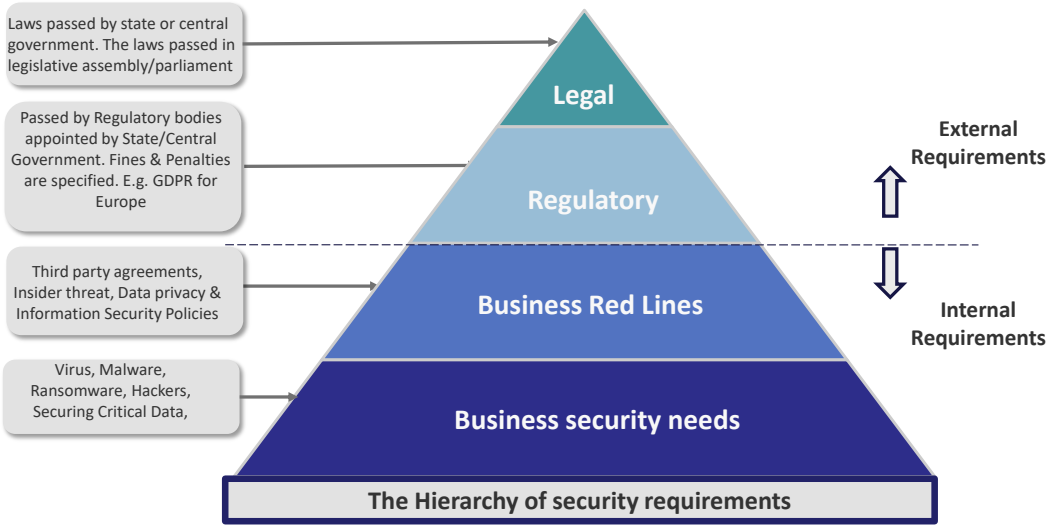


Diagram 1: The challenges to the Firm



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

Diagram 2: Firm's techno-legal response framework

1. TOP INCIDENTS, ROOT CAUSES AND RECOMMENDATIONS:

Top 4 violations (Table 2),[2] their respective root causes and possible firm level actions that are required for compliance in similar incidences and thus avoiding such fines are further analyzed in this Section.

#	Controller	Country	Fine in Euros	Type of Violation	Date
1.	Marriott International, Inc	UNITED KINGDOM	110 million	Insufficient technical & organisational measures to ensure information security	09 Jul 2019
2.	Google Inc.	FRANCE	50 million	Insufficient legal basis for data processing	21 Jan 2019
3.	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	GERMANY	35.2 million	Insufficient legal basis for data processing	01 Oct 2020
4.	TIM (telecom operator)	ITALY	27.8 million	Insufficient legal basis for data processing	15 Jan 2020

Table 2 GDPR: Analysis of the 4 largest corporate fines[3]

2.1 Marriot International [4](Violation of Article 5 of GDPR):

2.1.1 **The incident** – Sensitive data of almost 500 million guests of Starwood Hotel were hacked after a merger with Marriot International. After an internal investigation, they found out that the security tool had actually raised alerts of unusual database queries within the Starwood reservation system. This attack had been undetected since 2014, making the impact worse. Hackers had used Remote Access Trojan (RAT) and Mimikatz to break in.

2.1.2 **Root Cause** – Marriot did not perform sufficient due diligence on Starwood's IT security infrastructure during the merger process, which was a deal worth around 10 Billion Euro.

2.1.3 **Recommendations to avoid similar incident** - Conduct due diligence and thorough checks before adopting an acquired company's IT system. Implement appropriate software tools that can flag such activities at an

[2]*Supra* note 62

[3]*Id.*

[4]Article (5) of GDPR

earlier stage, backed by active monitoring of warnings to potential breaches. Check the legal requirements.

2.2 H&M Hennes and Mauritz Online Shop A.B. and Co. (Violation of Article 6 of GDPR):

2.2.1 **The Incident** – H&M had been creating highly inappropriate profiles of some of its employees for at least 5 years. They stored it on a database that up to 50 managers had access to.

2.2.2 **Root Cause** – Unauthorized collection of personal data from employees violates GDPR. Data like religious beliefs could be used to be biased during promotions and project assignment.

2.2.3 **Recommendationsto avoid similar incident** – While collecting data, employees should be made aware as to why this data has to be known by the HR department. The consent of the employee should be taken. If the employee doesn't want to share any such information, his/her right to privacy must be respected. Adequate technical security to data should be provided.

2.3 TIM[5] Telecommunications operator (Violation of Article 6 of GDPR)[6]

2.3.1 **The Incident** – Reported of promotional calls without proper consent. Further investigation pointed the failure in responding to data subjects' requests. The rights provided to subjects of the data under GDPR were disregarded.

2.3.2 **Root Cause** – The call center firms that were commissioned by TIM placed millions of calls to non-customers, without suitable legal basis or explicit consent.

2.3.3 **Recommendationsto avoid similar incident** – Need to have proper management of the contact details of data subjects for commercial campaigns, ensuring contacting only those who opted. More importantly, a foolproof mechanism to avoid calling those data subjects who wished to be omitted or those who have not provided explicit consent. It is of vital importance that firms update these lists frequently to bridge the gap in accuracy. Firms should refrain from storing data beyond the time allowed by the regulations of the country they operate in.

2.4 Google Inc. (Violation of Article 6 of GDPR)[7]:

[5]Article (6) of GDPR

[6]Data Privacy Manager. (2020). *€27,8 million GDPR fine for Italian Telecom -TIM – Data Privacy Manager*. [online] Available at: https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/ [Accessed 19 Dec. 2020].

2.4.1 **The incident** – In January 2019, CNIL (French Data Protection Authority) imposed a fine of 50 million Euros on Google. Inc under GDPR for lack of transparency and failure to obtain consent for ad targeting.

2.4.2 **Root Cause** – Forcing users to accept privacy policy (no valid consent). Did not have legal basis to process personal data.[8]

2.4.3 **Recommendationsto avoid similar incident**–Provide notice in clear and plain language when collecting persona data. Being transparent and using opt-in checkboxes instead of opt-out. Making disclosures accessible easily.

2. NEW NORMAL AND THE IMPACT ON FIRMS:

a. **Bring Your Own Device:**

Challenges – Exposure to a wide variety of security risks and potential data protection compliance issues, coupled with challenges in effective monitoring are the fundamental challenges faced by the firms.

Company policy that could alleviate – Detailed policies for BYOD devices, Encryption of sensitive data and Ensuring that company's information doesn't mix with employee's personal data can minimize the impacts on the first.

b. **Work from Home:**

Challenges – Manipulation of **VPN, weaponizing** of data are possible due to work from home policy.

Company policy that could alleviate – Having endpoint integrity checking and strong authentication in place once the VPN is active, educating employees to not download malicious applications or documents can reduce the problem.

- **CORPORATE ACTIONS TO ADDRESS DATA PROTECTION CHALENGES**

Appointing a competent Data Protection Officer (DPO)[9]

---

[7]Lydia (2019). *Case study: Google's €50 million GDPR fine - Golden Data - Medium*. [online] Medium. Available at: https://medium.com/golden-data/case-study-googles-50-milliion-gdpr-fine-5e43946793c2 [Accessed 19 May. 2019].

[8]Digital Guardian. (2019). *Google Fined $57M by Data Protection Watchdog Over GDPR Violations*. [online] Available at: https://digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations [Accessed 17 Sept. 2020].

[9]Digital Guardian. (2017). *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019*. [online] Available at: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance [Accessed 06 Oct. 2020].

1. Primary role:

DPO is meant to ensure that the company processes the personal data of its staff, customers, and providers, in compliance with applicable data protection principles.

2. Position of the DPO:

The position is of high responsibility in the firm's organization hierarchy and it is required that the DPO reports on a regular basis to top management regarding compliance to data protection regulations. To ensue independence, the DPO should not be an actor in the processing activities. The role must be supported by the firms to enable his/her smooth functioning, with provision of adequate staff and resources, to carry out the required activities. DPO must be vested with the authority to investigate data compliance incidents at his/her discretion.

2.1 Responsibilities of the DPO:

The role of Data Protection Office (DPO) is a key one, in the new normal. DPO

- Ensuring that data subjects are educated about their rights;[10]
- Advising the firm, especially the interpretation of data protection rules;
- Handling queries or complaints relating to matters of data privacy;
- Drawing the company's attention to any failures or potential risks ;
- Ensuring the firm's compliance to the applicable data protection regulations

2.2 Ensuring apt Data Protection Agreements (DPAs) with 3rd Parties and ensuring changes to these agreements are controlled:

Due diligence is required when firm's establish contracts with business associates (Controllers and Processors), especially for data intensive engagements. Normally, there is a need for a separate data protection agreement, in addition to the regular commercial contract. Key factors to be considered in the DPA include the insertion of clauses that ensure sharing of liability with business associates. It must also be verified that business associates establish Technical & Organization Measures aligned to the firm's needs, especially in cases where the firm plays the role of Data Controller. DPAs help in reducing the risk of non-compliance and shares the liability in case of data breaches.

2.3 Establishing a framework for Technical and Organizational Measures:

ISO 27001 is an international standard for establishing an Information Security Management System (ISMS). This is a widely adopted framework and includes security controls that ensure data protection by design. Benefits of ISO 27001 include a focus on confidentiality, integrity and availability of a firm's information systems.

Deployment of the standard involves \mapping of the information related critical assets, documenting the relevant processes, enhancing risk responses and planning for business

[10] Article 37 of GDPR

resilience. Certification improves business partner and customer confidence in the firm. This standard has become a hygiene factor and a firm's basic qualification in doing business.

2.4 Conducting a Data Protection Impact Analysis (DPIA) and updating it regularly:[11]

Data Protection Impact Analysis is a firm's procedure that is used to evaluate the activities that are specifically related to the processing of personal data. It is a legal requirement especially in cases wherein a firm acting as data controller anticipates a processing activity that is "likely to result in a high risk to the rights and freedoms of natural persons (Article 35 of GDPR)". Firms playing the role of data processor too would benefit from a DPIA, primarily de-risking their operations.

DPIA involves collaboration amongst the firm's stakeholders in walking though the data flows in the firm and identifying risks. The exercise could highlight privacy related risks that need to be addressed through appropriate mitigation – typically implementation of policies, procedures and information security controls.

Firms must conduct a DPIA once they consider in a new data processing activity or major changes in existing activities. It is important to revisit the DPIA especially in case of major changes e.g. in contractors, location, tools or data processing methods.

2.5 Establishing a Forensic Cell:

Interesting, as per NCRB data the conviction rate for cyber-crimes ranges from 2-5%. Hence, focus on internal investigation and establishing a forensic cell is key for effective enforcement. This team would support the DPO and the technical team in effectively ensuring compliance and producing robust audit trails, when required.

A forensic unit within a firm would help assist the management and where applicable, the authorities in the investigations pertaining to cyber crimes and help in making related court cases stronger, thus enhancing convictions and thus deterring cybercrimes.

2.6 Ameliorating Insider Threats:[12]

There are several types of insider threats. While malicious insiders have legitimate access to a firm's network and have malicious intentions, the accidental insider is an employee or associate who makes an honest mistake that could result in a data breach.

---

[11]Data Privacy Manager. (2020). *What is a DPIA and how to conduct it? [Video & Infographics] – Data Privacy Manager*. [online] Available at: https://dataprivacymanager.net/what-is-dpia-a-data-protection-impact-assesment/ [Accessed 24 Sept. 2020].

[12]Kedrosky, E. (2019). *6 AppSec Lessons from the SolarWinds and FireEye Breach*. [online] Security Boulevard. Available at: https://securityboulevard.com/2019/07/how-to-prevent-insider-data-breaches-at-your-business/ [Accessed 15 Jul. 2019].

To tackle the enemy within, the firm would need to identify the firm's sensitive data and ensure adequate controls. Simple actions of deploying strong passwords and enforcing strict access control, with periodic review of user accounts and privileged access rights would go a long way in reducing the threat levels. Verifying that ex-employees and short-term consultants or contractors do not continue to have access to firm information after they have left the company is a basic expectation from the firm's Human Resource Exit Process.

- **Conclusion**

In this ever-evolving field of cyber-security and data protection, it is imperative to be compliant with the law of the land. Clearly, the challenges ahead of firms (Diagram 1) need a framework (Diagram 2) and robust strategy (Diagram 3).

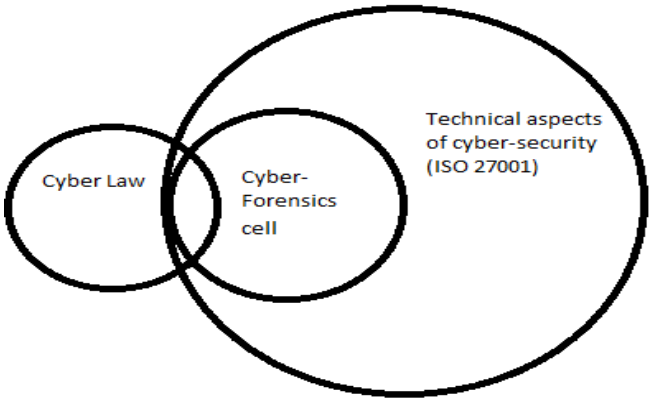


Diagram 3

The strategy must include a combination of techno-legal skills, constant upgrade of information security controls, and a contemporary organization structure that includes a DPO and a Cyber-forensics Cell. A combination of compliance experts and technical experts focusing on risk management and effective deployment of security processes within the firm is clearly the key differentiation that would enable a firm's business viability.

Bibliography

1. CMS, GDPR Enforcement Tracker, 2020, (17th Apr, 2020, 15:30 IST) https://enforcementtracker.com/

2. Dan Swinhoe, The 15 biggest data breaches of the 21st century, (17th Apr, 2020, 15:30 IST) https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

3. Lydia F de la torre, Case study: Google's 50 million Euro GDPR Fine (19th May, 2019), https://medium.com/golden-data/case-study-googles-50-milliion-gdpr-fine-5e43946793c2

4. Dan baker, How to prevent Insider Data Breaches at your Business,(15th July, 2019), https://securityboulevard.com/2019/07/how-to-prevent-insider-data-breaches-at-your-business/

5. GDPR (4th Feb, 2020) https://advisera.com/eugdpracademy/gdpr/

6. 27.8 million Euro GDPR Fine for Italian Telecom – TIM (4th Feb, 2020) https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/

7. What is a DPIA and how to conduct it (24th Sept, 2020), https://dataprivacymanager.net/what-is-dpia-a-data-protection-impact-assesment/

8. Chris Brook, Google Fined $57M by Data protection watchdog Over GDPR Violations(17th Sept, 2020), https://digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations

9. Victoria Hudgins, What Ever Happened to the proposed GDPR Fines Against Marriot, British Airways(27th July, 2020 10:30) https://www.law.com/legaltechnews/2020/07/27/what-ever-happened-to-the-proposed-gdpr-fines-against-marriott-british-airways/?slreturn=20200919000007#:~:text=The%20breach%20exposed%20the%20personal,due%20to%20system%20security%20shortfalls.

10. Nate Lord, What is a Data Protection Officer(DPO)? Learn About the New Role Required for GDPR Compliance in 2019(6th October, 2020), https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance

Legislation

1. General Data Protection Regulation, 2018