ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Data Privacy and Risk Management, Collaboration is Key on Tackling Privacy Risks/Issues

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, USA

ABSTRACT

Data Privacy is relevant for majority of the firms conducting businesses in the international market today. Better privacy safeguards and implementations are one of the key contributors in driving business output, companies are reporting direct and indirect benefits as a result of privacy project related investments. To be compliant with the Privacy regulation landscape globally is the need of the hour, there have been significant business impacts in terms of both financial and reputational, as a result of noncompliance to privacy regulations. To manage these risks, it is imperative for the Privacy assessment teams, Legal teams and Risk management teams to work together and tackle these challenges.

This paper firstly aims at giving a perspective on global risk landscape and how the privacy regulations are gaining more traction every passing day, bringing in more states and countries into the fold. This article also narrates the approach or solution explaining how Risk management teams can partner with the relevant stakeholders in legal and privacy teams and guide the data privacy risks across firms, across business sectors. Through the risk management lifecycle thus remediating these risks, helping businesses prosper and at the same time safeguard individual interests.

***Corresponding author**

Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, USA.

Received: November 04, 2023; **Accepted:** November 14, 2023; **Published:** November 23, 2023

Keywords: Data Privacy, PII (Personally Identifiable Information), Risk management, Privacy Risks, GDPR

Introduction

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system [1].

Data Privacy: is the measure of control that people have over who can access their personal information [2].

Privacy acts and laws have been around since the late 1800s to safeguard public data and interest especially with the invention around newspapers and articles where information was printed without the individual's consent, the laws did go through a major overhaul in the later part of the year 1900s with the technology advances, computers and databases the privacy act of 1974 ensured that there are provisions and safeguards in place. In and around 1995, there was the Data protection act. Around 2016 GDPR, a very comprehensive set of regulations was brought into place to protect European citizens specifically, several other nations followed suit to protect their own population [2]. These laws ensured that PII data specifically is not misused, heavy fines were imposed on institutions that were non-compliant, and in the event of data breaches. From a Corporate standpoint, this means there are risks and controls that needs to be put in place.

Rationale for this Study

To help avoid organizations involved in data breaches and regulatory fines from accidental misuse or over collection of data, teams perform current state assessments, these assessments are targeted on products and companies to see if they comply with the various privacy regulations in place, they are assessed against those control frameworks.

Once the risks are identified, it becomes orphaned since privacy teams are responsible for identifying these risks and not to see through remediation, like any assessment team they would either move on to some other product for risk identification assessments or revisit this annually, if they have bandwidth.

Legal teams on the other hand don't have risk expertise, they have knowledge of various regulations and its impact so they can guide stakeholders on how to comply, nothing more, nothing less.

Risk leaders and managers have the expertise and can work with privacy and legal teams to get context on the regulation, requirement, controls, understand the risk through privacy teams and work with engineering teams on remediation of the risks identified. Thus Risk managers can play a crucial role of bridging the legal, privacy and engineering teams together to not only identify, analyze the risks but remediate them in due time to avoid

reputational and financial impact to the firms.

Literature Review

As per Veritas, an independent consulting firm, there is significant business impact, if a firm fails to protect its customer's personal data, there are additional risks such as risk of data breaches and legal repercussions [3].

As per IAPP, a privacy professionals membership, the five highest priority privacy risk domains identified by participants were data breaches, noncompliant third-party data processing, ineffective privacy by design implementation, inappropriate personal data management and insufficient privacy training for employees [4].

As per ISACA, professional membership of information security and compliance professionals, its best to create a Privacy risk framework and tackle these issues using the Privacy risk management approach, however this paper prescribes a better approach of bringing in the privacy risks into the firm's Risk management lifecycle instead of creating a whole new set of processes and approach just to manage privacy risks.

Data Privacy Regulation Landscape Across US and Globally

Figure 1: Privacy Regulation Landscape Across the Globe

In today's world and context, almost every nation especially if its conducting global transactions, has its own privacy law, some countries are working towards drafting one, if they don't have it at the moment, let's look at some of the major countries and a quick overview on their privacy laws
as per this article [5].

GDPR – Global Data Protection Regulation – European Union

This regulation aims to give consumers control over their own personal data by holding companies responsible for they way they handle and treat this information. This applies to all companies process personal data of subjects residing in the EU/EEA, regardless of company's location.

PIPL

The China Personal Information Protection Law (PIPL) is the new data privacy law in China, targeted at personal information protection and addressing the problems with personal data leakage. The PIPL is not only applicable to organizations and individuals who process personally identifiable information (PII) in China, but also those who process data of China citizens' PII outside of China.

DPDPA

India's Digital Personal Data Protection Act (DPDPA) 2023's primary focus is handling digital personal data within India, which includes both online and offline data. If processing includes providing Indians with products or services or profiling them, it also extends its authority to process personal data outside India. The bill seeks to create a safer and more secure digital environment for all stakeholders involved.

LPGD

The Brazilian General Data Protection Act (in Portuguese, LGPD, Lei Geral de Proteção de Dados) establishes rules on collecting, handling, storing and sharing of personal data managed by organizations. LPGD covers all companies that offer services or have operations involving data handling in Brazil.

There are many more countries or nations like Canada, Mexico and a few others who have their own nation specific privacy regulations.

United States being a federal body, states are given autonomy to an extent to draft their own privacy laws as such there are varying degrees of privacy laws drafted within the United States across different states some states like California have the CCPA (California Consumer Privacy Act) that considered to be the strictest amongst all states, CCPA, signed into law on June 8, 2018, and which went into effect on Jan. 1, 2020, establishes privacy rights and business requirements for collecting and selling Californians' personal information [6].

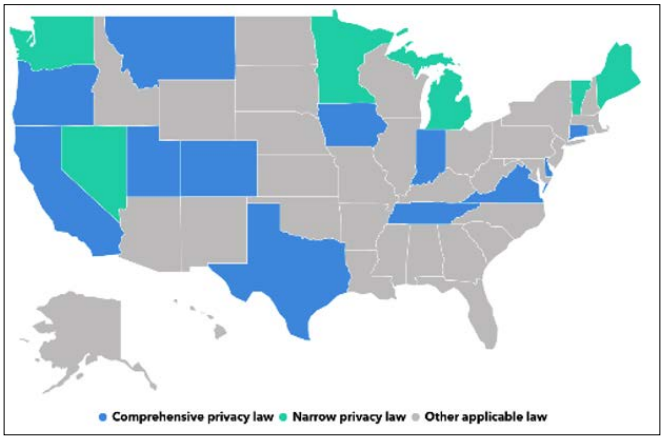

Figure 2: US Data Privacy Laws [6]

There are similar states like California that have enacted comprehensive and detailed privacy regulations, these states include Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia.

While there are other states like Nevada, Maine, Michigan, Minnesota, Vermont that have enacted tailored privacy regulations.

Adding to the above list there are some states like New York, New Jersey and a few more that have introduced privacy bills in 2023.

As we can see more and more states are coming into the fold to draft privacy regulations and protects the interests of their common citizens.

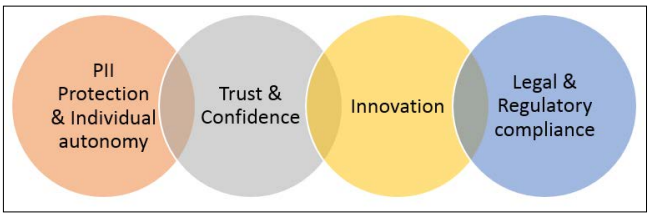

Figure 3: Importance of Data Privacy

Data privacy regulations are important for the following reasons; It safeguards PII/MNPI information from unauthorized access, these regulations direct the corporate firms on measures, safeguards that need to be in place, they also transfer the power back to the individual from the firm, people know exactly why their data is collected and how it will be used, also the controls that are put in place to protect the data [7].

It establishes trust and confidence between the parties involved, demonstrates the company's commitment to protect the said information.

These laws also fuel innovation since consent is asked prior to collecting information, firms now can analyze and gain valuable insights to create more efficient products but at the same time not compromising the privacy and security of information.

Compliance to these regulations are mandatory and noncompliance leads to heft fines that cause financial impact and at the same time there is a reputational impact that leads to loss of customer trust.

There is a very common misconception around Data privacy and data security, sometimes both are interchangeably used, best to clarify this concept here through a visual as described below.

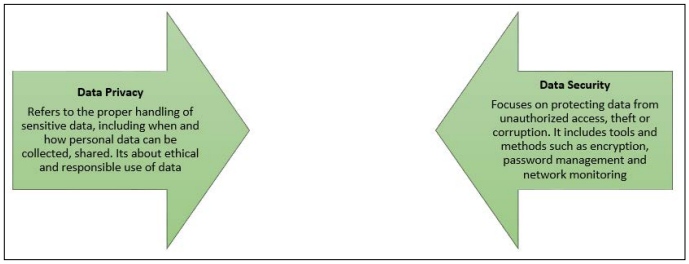

Figure 4: Data Privacy vs Data Security

Method

To identify privacy risks, many firms have specialized privacy teams who are certified in data privacy regulations, they conduct Privacy impact assessments against products starting with Data inventory that is trying to investigate the types of information collected from customers and for what purpose. There are also probing questions for example, are the engineering teams using the information for purposes mentioned in the contract?, external facing documents and to what extent?. Where are they being stored?, are there good encryption controls for sensitive information?. Who all have access to information etc. The results of these assessments are usually called as findings, which are then analyzed and rated for risk levels, and engineering teams are accountable for remediating these privacy findings which will end up being categorized as risks in the risk register later. The privacy teams usually don't have the bandwidth to track and monitor these towards completion.

Legal teams work with Engineering teams on drafting external facing documents sometimes called as Privacy sheets, different firms use different terminologies to name these documents but they essentially are stored on external facing sites to provide customers with information on how their data is being collected, what data is being collected? For what purpose and where is it stored, what are the controls in place to protect the said data etc.

Customers can reach out and opt out entirely or opt out of certain sections, if they wish to. Legal teams here play a crucial role of ensuring the engineering teams and dependent teams understand the privacy regulations, the extent to which they can stay compliant, what would noncompliance look like etc. Legal teams, however don't get involved once the risks are identified since they lack the expertise, they can act as collaborators with engineering on solving the issues and risks highlighted by the privacy teams.

Risk management teams if equipped with resources have the potential to see through the risks identified by the privacy teams, Risk leaders have the required background and expertise to handle privacy risks. They can work with legal teams to understand more context on the risks, effective remediation measures, and accordingly advise engineering teams on technical controls and solutions that can meet those said legal measures.

Risk teams can continuously have status check-ins with engineering to understand the roadblocks, once remediated, statuses can be reflected in the risk registers where these risk are documented, the risk reports circulated to senior management and leadership throughout the lifetime of the risk will help involved stakeholders on the risk posture stemming from these privacy risks.

Privacy teams can be kept in loop on updates thus communicating the information back to the assessment teams, closing the loop. These steps when followed ensure the privacy risks are identified, analyzed, appropriate response noted and finally remediated towards closure.

Discussion and Extended Use Cases

The afore mentioned method can easily be replicated across different companies, provided there are risk professionals with a background in both privacy and technology controls. The risk reporting mechanisms can be implemented in various firms. Privacy teams if not in place, Risk teams could front run those assessments with the help of legal teams thus saving capital on extra resources. Predefined cadence based governance forums can respond appropriately based on the criticality of the risks and controls that need to be in place. These are in practice in some of the financial firms with a matured Risk management framework, technology firms have recently adopted some techniques in the light of regulatory fines and proceedings by the government.

Conclusion

Privacy risks if not seen through towards completion can result in major repercussions to companies, this approach here helps Senior management and leadership to get a grip on these items through the risk reports run by the Risk teams. Risk Managers in partnership with Legal and Privacy teams can help identify risks, track and monitor them towards completion.

It's also important to involve legal teams as much as we can since these teams are the subject matter experts when it comes to not only identifying risks but also suggesting remediation measures. Privacy related context is very complex since depending

on location; where the firms are operating out of, depending on the country or state the person belongs to, there are nuances that normal practioners or professionals might fail to understand and capture. This collaborative process listed in this paper can help not only firms but also individuals who have allowed their information to be collected [8-12].

References

1. Risk Tolerance - Glossary | CSRC. NIST https://csrc.nist.gov/glossary/term/risk_management.
2. (2023) General Data Protection Regulation (GDPR) Compliance Guidelines. GDPR.EU https://gdpr.eu.
3. (2023) The Importance of Data Privacy and Compliance: A Comprehensive Guide. Veritas https://www.veritas.com/information-center/data-privacy.
4. (2023) Privacy Risk Study 2023 – Executive Summary. IAPP https://iapp.org/resources/article/privacy-risk-study-summary/.
5. International Privacy Laws | Office of Ethics. UC Berkeley https://ethics.berkeley.edu/privacy/international-privacy-laws.
6. Legal intelligence and insights powered by expert analysts. Bloomberg Law https://pro.bloomberglaw.com/insights/.
7. Tobin D (2023)What is Data Privacy—and Why Is It Important? Integrate.io https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/#:~:text=Preserving%20Individual%20Autonomy%3A%20Data%20privacy.
8. Nyambura Kiarie (2023) 2023 Updates to U.S. State Data Privacy Laws: What You Need to Know. Auditboard https://www.auditboard.com/blog/updates-to-us-state-data-privacy-laws/.
9. Murray C (2023) U.S. Data Privacy Protection Laws: A Comprehensive Guide. Forbes https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/?sh=7bb8f74f5f92.
10. Ramirez N (2019) What You Need to Know About Data Privacy Laws. Osano https://www.osano.com/articles/data-privacy-laws.
11. (2022) Data Privacy in America. SENATE RPC https://www.rpc.senate.gov/policy-papers/data-privacy-in-america.
12. U.S. Privacy Laws. EPIC - Electronic Privacy Information Center https://epic.org/issues/privacy-laws/united-states/.