Roman Hanson

B=2

Day: M T W T F S

Date: __/__/20__

Social Media and Data Privacy: How global Regulations are shaping the future of Online Privacy.

Outline:

1. Introduction:

Global regulations are shaping the future of online privacy by enacting various laws like the European Union's General Data Protection Regulation (GDPR). These laws have shaped the online privacy through enhanced transparency and improved data security.

2. How Global Regulations are shaping the future of online privacy.

2.1 General Data Protection Regulation (GDPR) of European Union sets a high standard for data privacy rights

2.2 Singapore's Personal Data Protection Act covers data breach standards

2.3 Asia Pacific Economic Corridor (APEC), cross border Privacy Rules system fosters

Date: __/__/20

interoperability between different national models

2.4 The California Consumer Privacy Act (CCPA) mirrors some GDPR provisions

3. Challenges in Implementing Data Privacy Laws:

3.1 Rules often fail to keep pace with evolving technologies like Artificial Intelligence

3.2 Differing cultural attitudes towards privacy protection

3.3 Fastest growing data needs fastest regulations

3.4 Cross-border data flows needs comprehensive regulations

4 Way forward to Overcome the challenges:

4.1 Implement holistic regulatory compliance programs

4.2 Establish clear data governance frameworks

Day: M T W T F S
Date: / /20

4.3 Conduct continuous employee training

4.4 Implement technology driven compliance solutions

5. Conclusion

By implementing above discussed measures data privacy can be ensured.

Date: __/__/20

Data privacy compliance has become the requirement of businesses and the importance of data privacy and compliance with regulations has never been more significant. The regulatory landscape surrounding data privacy is multifaceted with various laws and standards governing how organizations handle and protect personal information. From the General Data Protection Regulation in Europe to the California's Consumer Privacy Act in United States, businesses must navigate a complex maze to ensure compliance. As technology continues to advance, so do the challenges associated with protecting sensitive information. Rules often fail to keep pace with the evolving technologies and differently cultural values do are the most frequent challenges. However, cross border data transmission requires a comprehensive regulatory framework. These challenges can be overcomed by certain measures like implement holistic systems.

Day: M T W T F S
Date: __/__/20

for compliance and establish clear data governance frameworks in this regard. By implementing these measures in true letter and spirit we can overcome the challenges and the online data privacy can be ensured.

General Data Protection Regulation (GDPR) by European Union (EU) is a welcoming step to regulate the social media. It is one of the most comprehensive and data stringent protection laws in the world. It applies to any organisation that possesses the personal data of EU citizens, regardless of where the company situated. Its key provisions which are shaping the future of online privacy are consent and right to access. Organisations must obtain explicit consent before collecting or processing personal data and individuals have the right to access their personal data held by an organisation. Lastly, companies must notify regulators

Day: M T W T F S
Date: __/__/20

of a data breach within 72 hours. fines for non-compliance can reach upto 4% of global annual revenue. Therefore, these provisions will shape the future of online privacy.

Singapore's personal Data Protection Act covers the baseline standards of it a comprehensive law that governs the collection, use, disclosure and care of data in Singapore. Its key provisions are access, accuracy, protection and retention. Individuals have the right to access and correct their personal data. Furthermore, organisations must ensure personal data is accurate and complete. In addition to this, organisations must retain personal data only as long as necessary. This act covers the healthcare and the financial institutions. Personal Data Protection commission is responsible for enforcing the personal data protection Act. In case of non-compliance fines

Day: M T W T F S
Date: / /20

upto SGD 1 million can be imposed.

The Asia Pacific Economic Corridor has established a frame work for cross-border security rules. The purpose of these security rules is to secure transfer of personal data across borders. The key features of these rules are certification validity and accounting and trust. On case of certificates which is valid for one year and in case of reappear the validity is for three years. Furthermore, it also demonstrate accountability and trust to consumers and national enforcement bodies. In addition to these key features, businesses can insure compliances with cross border security rules and maintain a trust of consumers in the Asia-pacific Region.

California consumer privacy Act (CCPA) is a state level privacy law in California. This law grants significant rights

Day: M T W T F S
Date: __/__/20

regarding their personal data. The key provisions of this act are data transparency and data access and deletion. Organizations must disclose what personal data is collected and how it is used. In addition to this, consumers can request access to their data and ask for it to be deleted. In addition to this opt-out rights are important provisions in which consumers have the right to opt-out the sale of their personal data. In case of non-compliance companies can be fined for violations and individuals can sue in the event of a data breach. Therefore, the CCPA provides regulations for shaping the future of online privacy.

Data privacy laws are confronting challenges as these rules have failed to keep pace with evolving technologies. Technology is evolving continuously. This evolving need in ~~evolution~~ technology needs changing laws. Some of these laws have failed.

Day: M T W T F S
Date: / /20

compliance with the law. Like the 21st century is the age of AI many countries including United Nations are fearful about its consequences. Because the existing rules are not capable enough to cope with the challenges. In this regard, United States and European countries are try their best to harness AI Therefore, laws are not in compliance with evolving time in technology.

Different cultural attitudes are also obstacles in shaping the future of online privacy. Different cultural attitudes lead to varying regulatory measures creating a challenge for the international business. In addition to this, cultural norms can influence enforcement and compliance with some countries prioritizing economic growth over data protection. Furthermore, raising awareness about data privacy concerns can be difficult in cultures where privacy is not highly valued. Moreover, impla

Day: M T W T F S
Date: __/__/20

data protection measures, requires significant technological and infrastructure investments.

Fastest growing data needs fastest regulations. As with the increase in the data, there is also a need in growing hands to cater the challenge. In this century every fraction of even the personal duties are being performed by machines which are doing run on data. Therefore the need of the data increases and so it requires rules and regulations to be in compliance. Furthermore, data is being used in wars. This is evident in Palestine - Israel conflict as Israel have signed a project worth 12 bn with Google to share the data. In this way, to regulate the data is a biggest challenge.

Cross-border data flows needs comprehensive regulations. In this world of global village everyone is in contact with

Day: M T W T F S
Date: __/__/20__

everyone. They share their views, experiences and have different regulatory habits in time of use. Therefore, rules of one country may be objectionable in other country. The recent example is the anti-Muslims protests in Germany sparked fury and led to violent skirmishes by using propaganda on social media. Therefore, there is a need to make a comprehensive strategy to cope with this challenge.

Implement holistic regulatory compliance programs to overcome the challenges posed in implementing data privacy laws. Identify and prioritize high risk areas and develop targeted compliance strategies. In addition to this develop comprehensive policies and procedures that address multiple regulations. Furthermore, educate employees on data privacy laws and regulations. Moreover, leverage the technology to support compliance efforts and ensure the governance and oversight.

Day: M T W T F S
Date: 1 /20

Therefore, the above discussed are the components of healthcare regulatory programs.

Implement technology driven compliance solutions as a way forward to overcome the challenges. There are different components of compliance solutions like compliance management platform and regulatory intelligence are most important. Integrated platforms that manage compliance tasks, policies and procedures. Also implement the regulatory changes and updates with the help of AI. The above discussed compliances are helpful in ensuring transparency and accountability.

To conclude, global regulations like General Data Protection Regulation and Asia Pacific economic cooperation cross border security rules are playing the future of online privacy often confronting challenges in implementing data privacy laws. Among these diff

Day: M T W T F S
Date: __/__/20__

ering cultural attitudes and cross-border data flows are more important. To cope these challenges certain steps like implementing holistic compliance programs and technology driven compliance solutions are most beneficial. Therefore, by implementing these measures, we can shape the future of online privacy in positive manners.