Finstein

Unleashing Cybersecurity Brilliance

The Einstein Way!

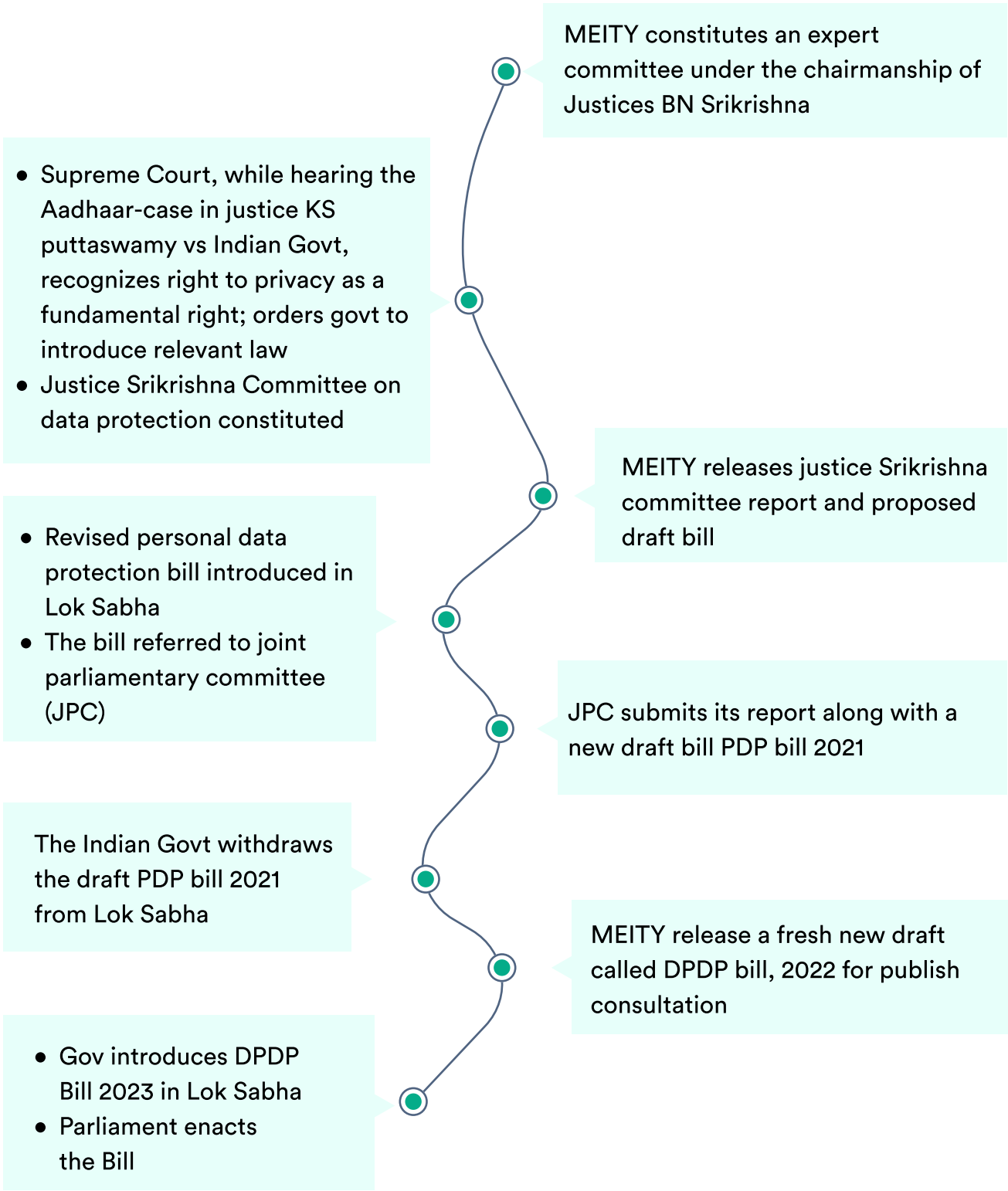
Sep 2023

Finstein

TABLE OF CONTENTS

Finstein

Journey to the Digital Data Protection Act 2023



Finstein

The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Bill of 2023 was presented in the Lok Sabha on August 3, 2023, by the Minister of Electronics & Information Technology. It was approved by the Lok Sabha on August 7, 2023, and received unanimous support in the Rajya Sabha on August 9, 2023. The President gave his assent to the bill on August 11, 2023.

Applicability of the Act

The Act has extra territoriality as it is applicable for Data processed within or outside India.

In India:
If the personal data is collected in digital form or in non-digital form and digitized later on.

Outside India:
If the digital personal data is processed outside India for offering the goods and services to persons (Data Principal) in India. (Person for brevity shall mean the Data Principal).

Consent is crucial.

Consent stands as a pivotal right under the Act, serving as both a duty for the Data Fiduciary and a privilege for the individual (Data Principal). For consent to be valid, it must be given freely, with clarity, informed awareness, without conditions, and through a clear affirmative action. From now on, ambiguous terms, assumed approvals, generalized permissions, or pre-selected checkboxes, as seen on some websites and in privacy policies, will not be considered valid 'consent' as per this Act

Finstein

Specified Purpose

The Data Fiduciary ought to state the purpose for which the data is to be collected and the Person has the right to receive notice of such purpose and further has the right to revoke the consent.
The Act specifies that the consent taken should always be connected with the specified purpose for which the personal data is collected. Once, the purpose is accomplished or it can be reasonably assumed that the purpose is no longer served, the personal data has to be deleted.

Rights:

- Right to access: An individual can request a summary of their processed personal data from the Data Fiduciary and learn about all entities (Data Fiduciaries and Data Processors) the data has been shared with.
- Right to correct: An individual can amend, complete, or update their personal data.
- Right to erase: An individual can request the removal of their personal data.
- Right to grievance redressal: An individual can access mechanisms to address their grievances.
- Right to nominate: In case of death or incapacity, an individual can designate another person on their behalf

Duties:

- Duty to comply with the provisions of all applicable laws
- Duty not to impersonate another person
- Duty to ensure not to suppress any material information
- Duty to ensure not to register a false or frivolous grievance or complaint
- Duty to furnish only verifiably authentic information

Finstein

Obligations of the Data Fiduciary

- Engage with a Data Processor to process personal data on its behalf through a valid contract only
- Provide a clear, concise and comprehensible notice to Data Principals
- Obtain verifiable parental consent before processing children's personal data
- Abstain from processing personal data that may cause harm to children or undertake behavioral monitoring of children or targeted advertising directed at children
- Implement technical and organizational measures to ensure effective adherence with the Act
- Delete and cause its Data Processor to erase data as soon as the purpose is accomplished
- Report Personal Data Beaches to Data Protection Board and Data Principals

Significant Data Fiduciary

Significant Data Fiduciary will be determined based on an assessment which includes

- The volume and sensitivity of personal data processed
- Risk to electoral democracy
- Risk to the rights of data principal
- Potential impact on the sovereignty and integrity of India
- Security of the state
- Public order

Obligations of the Significant Data Fiduciary

- Appoint a Data Protection Officer (DPO) based in India
- Appoint an Independent Data Auditor for evaluating compliance
- Conduct Data Protection Impact Assessment (DPIA) & periodic audits

Personal Data Breach

- A Data Fiduciary is required to protect personal data, including any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent Personal Data Breach.
- In the event of a Personal Data Breach, the Data Fiduciary needs to notify the Board and each affected Data Principal of such breach.
- No specific timeline for reporting the breach
- Data Fiduciaries to inform about the breach in prescribed form

Finstein

Penalty Details

Below is a summary of the penalties as outlined by the Act:

Type of Violation	Penalty
Failure to uphold the duty of the Data Fiduciary to ensure reasonable security measures against personal data breaches	Upto 250 Crores
Neglecting the responsibility to inform the Board or the affected Data Principal about a personal data breach	Upto 200 Crores
Not adhering to obligations concerning children	Upto 200 Crores
Non-compliance with specified duties	Rs.10,000

Next Steps....Journey to Compliance

- Assess state of readiness
- Create a Data Privacy Framework and launch a Privacy Program
- Perform Data Privacy Impact Assessments (DPIAs)
- Explore data through a Data Discovery Exercise
- Develop Privacy policies and procedures
- Enhance technology for consent management
- Apply Technical and Organizational safeguards
- Provide training and raise awareness
- Conduct regular audits and assessments
- Implement Privacy by Design principles
- Review and evaluate Third-Party Risks

Finstein

Harnessing Generative AI for Enhanced Cybersecurity

In today's digital age, the constant evolution of technology brings both opportunities and challenges. While advancements in cybersecurity have made it possible to protect sensitive information from cyber threats, the sophistication of these threats is also increasing. To stay ahead in the cybersecurity game, many organizations are turning to generative AI, a powerful tool that has the potential to revolutionize the field.

Understanding Generative AI

Generative AI, a subset of artificial intelligence, focuses on creating data or content rather than just processing or analyzing it. It leverages deep learning techniques to generate human-like text, images, or even entire applications. This technology has found applications in various fields, including art, entertainment, and now, cybersecurity.

The Role of Generative AI in Cybersecurity

- **Threat Detection and Analysis:** One of the primary applications of generative AI in cybersecurity is threat detection and analysis. Traditional methods of identifying malware and suspicious activities rely heavily on predefined patterns and signatures. However, cybercriminals are constantly developing new techniques to bypass these defenses. Generative AI can adapt to evolving threats by learning from historical data and identifying anomalies that may not be apparent through conventional means

- **Password Security:** Generative AI can help organizations strengthen their password security by generating complex and unique passwords for each user, making it exponentially more challenging for attackers to crack them.
- **Phishing Detection:** Phishing attacks are a prevalent and deceptive form of cybercrime. Generative AI can analyze and detect phishing emails or messages by examining the content, language, and sender behavior. This proactive approach helps organizations identify and neutralize phishing threats before they can cause harm.
- **Security Patch Generation:** Keeping software and systems up-to-date with the latest security patches is crucial for preventing vulnerabilities from being exploited. Generative AI can assist in automatically generating and applying patches.
- **Predictive Threat Intelligence:** Generative AI can analyze large datasets to identify emerging threats and vulnerabilities. By providing predictive threat intelligence, organizations can proactively secure their systems against potential future attacks.

Challenges and Considerations

While generative AI holds great promise in enhancing cybersecurity, it also comes with challenges. Some considerations include:

- **Ethical Concerns:** The use of AI in cybersecurity raises ethical questions about privacy, surveillance, and data handling. Striking a balance between security and individual rights is essential.
- **False Positives:** Generative AI systems can sometimes generate false positives, leading to unnecessary alerts and operational disruptions. Fine-tuning and constant monitoring are necessary to mitigate this issue.
- **Adversarial Attacks:** Cybercriminals can also use generative AI to launch attacks. As AI becomes more integral to cybersecurity, defending against adversarial AI is a growing concern.

Conclusion

Generative AI is a valuable addition to the cybersecurity toolkit. Its ability to adapt to evolving threats, enhance password security, detect phishing attempts, and provide predictive threat intelligence can significantly bolster an organization's defenses. However, it's crucial to address ethical concerns, manage false positives, and guard against adversarial attacks. As the cybersecurity landscape continues to evolve, generative AI will play an increasingly pivotal role in protecting our digital world. Organizations that embrace this technology will be better equipped to face the ever-growing challenges of cyber threats.

Finstein

About Us

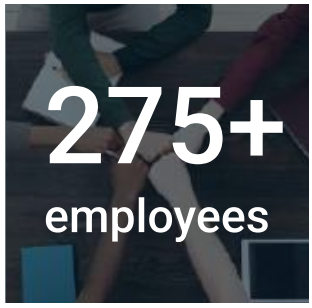
Unleashing Cybersecurity brilliance, the Einstein Way!

In a world where digital threats loom larger than ever, our mission is clear: Unleashing Cybersecurity brilliance, the Einstein Way! At Finstein, we don't just protect; we innovate, adapt, and anticipate. Our purpose is to redefine Cybersecurity, harnessing the genius of Einstein himself to craft solutions that outthink and outmaneuver the ever-evolving threats cape. Join us on a journey where brilliance meets security, and together, we'll safeguard the digital future.

We support the following illustrative frameworks

NIST SANS HITRUST

ISO 27001 Certified · AICPA SOC · CSA cloud security alliance · PCI DSS



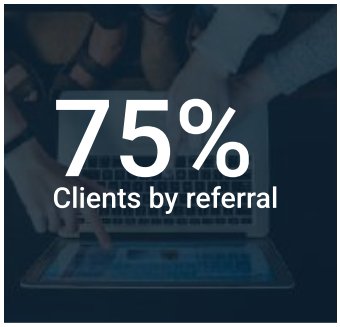
6 Practice Leaders

An experienced Leadership having expertise Security and Technology

Multi-Disciplinary

CEH CREST B.E MS

CA CISA CDPSE CFE



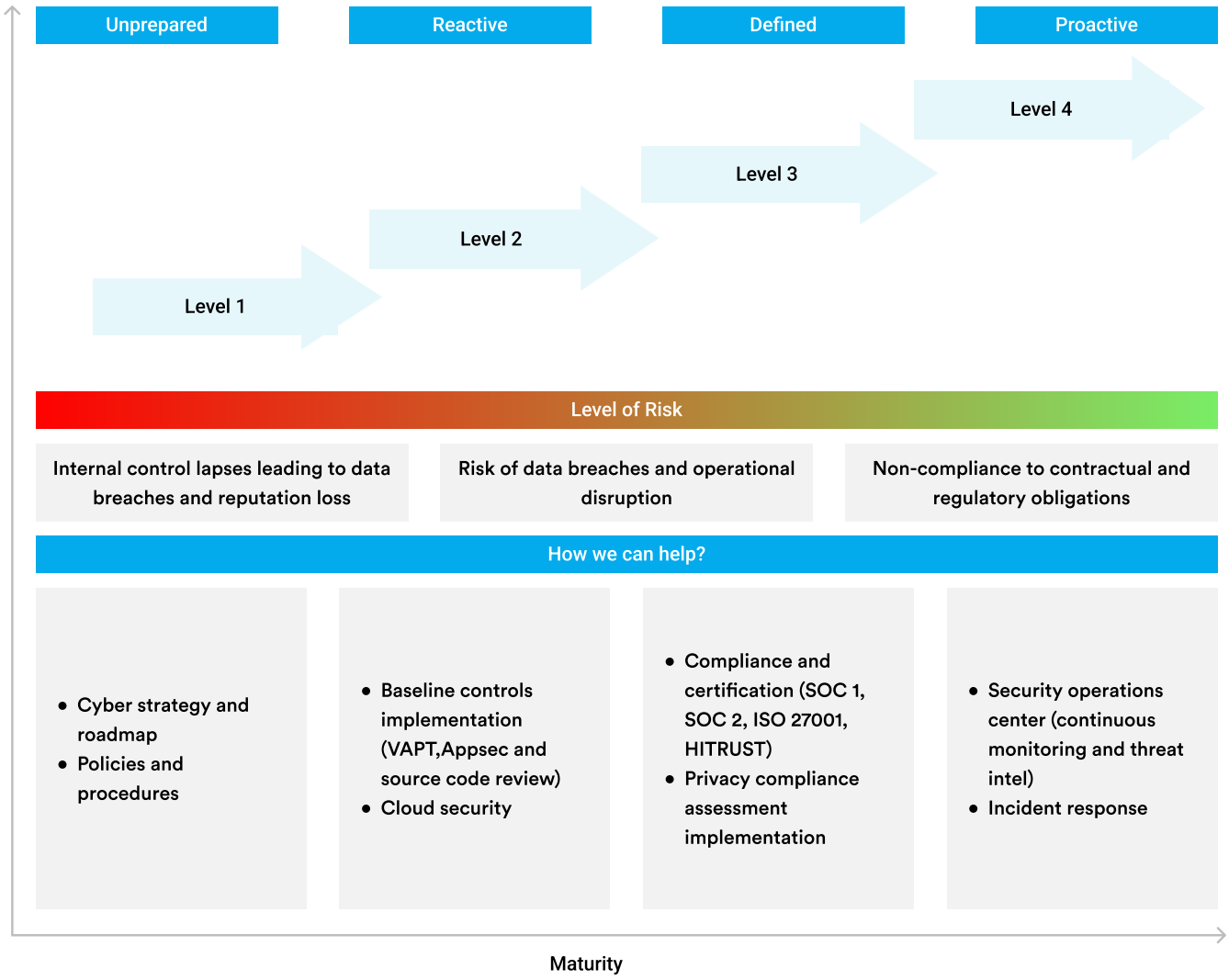
ISO 27001 Certified · AICPA SOC · CERTIFIED ISO 9001:2015 COMPANY

We are SOC 2 Type II, ISO 27001:2013 and ISO 9001:2015 Certified and .

Finstein

Cyber Security Maturity Model

At Finstein, we've crafted a unique and comprehensive cybersecurity model designed to support our clients at every level of their security journey. Whether you're just starting out, in reactive mode, well-defined, or aiming for proactive excellence, we have tailored solutions you need. From strategic guidance and policy development to baseline controls implementation, compliance and certification, and even the establishment of a Security Operations Center (SOC), our commitment is to elevate your cybersecurity posture and resilience. Join us on this transformative path to cybersecurity excellence.



Finstein

Our Solutions

Strategy

- Cyber Strategy and Roadmap
- Policies and Procedures
- Information Security CISO dashboard
- Third Party Risk Management

Threat and Vulnerability Management

- Vulnerability Assessment
- Penetration Testing
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- IOT VAPT
- 5G Security Testing

Build Cloud Security

- Cloud Security Review
- Cloud Security Maturity Assessment
- Google Apps and O365 Security Review

Compliance and Certification

- ISO Management Support and Certification
- SOC1, SOC2 and SOC3 Attestation
- HITRUST Assessment and Implementation
- PCI-DSS Management Support and Certification

Attack Surface Management

- Threat Hunting
- Deep and Dark Web Monitoring
- Threat Intelligence

Manage and Monitor

- Co-managed SIEM
- SOC as a Service
- PAM as a Service
- Incident Response

Finstein

Our Privacy Solutions

Current State Assessment

- Data privacy maturity assessments
- Data privacy gap assessments against applicable law
- Data privacy audits

Strategy and Roadmap

- Data privacy strategy and program definition
- Data privacy framework design
- Data privacy policies and procedures

Implementation

- Data privacy framework implementation
- Consent management
- Data breach management
- DPO-as-a-service

Why Us?

We have been there and done this....

Cyber security program

A well integrated, collaborative team that puts your needs in the front and centre

Finstein

Our Practice Leaders

An experienced Leadership having extensive expertise in Cybersecurity and Technology

Praveen Kumar
praveen@finstein.ai

Dinesh Kumar
dinesh@finstein.ai

Santosh Kumar
santosh@finstein.ai

Unleashing Cybersecurity Brilliance

India
floor no. 6, block b84, greams rd, chennai, india 600006

Singapore
no. 3, shenton way, #14-30, shenton house, sg 068805

New York
no. 110 wall street, new york, us 10005

Finstein

Unleashing Cybersecurity Brilliance

The Einstein Way!

Sep 2023