# ABSTRACT

Data Protection and Privacy is the most important concern of any organization or for an individual. Pertaining to the needs, standard rules and regulations are the prime factors for maintaining privacy of an individual & safeguard the interests of the organization's personal data. Implementation of various IT Companies are working in different ways for its execution through varied principles and methods.

Personally Identifiable Information (PII) and to protect it under Personal Data Protection policies. Personal Data Protection requires companies to protect the privacy of their customers. That means keeping personally identifiable information (PII) safe.

Implementation of Data portability with existing policies and at the same time considering it with the security point of view also helps in maintaining the integrity and consistency at large scale.

# ACKNOWLEDGEMENT

I would like to put my sincere gratitude for being mentored under the **DIGITAL INDIA INTERNSHIP SCHEME, NIC(HQ)** by **Deepak Goel**, STD & HOD, Legal Services Division. He has helped me towards gaining skills, knowledge and important standard methodology of defining the structure of any project.

The project undertaken under him '**IMPLEMENTATION OF PERSONAL DATA PROTECTION POLICIES IN IT APPLICATIONS**' has a well-defined procedure for all the Data Protection implementation on IT applications mostly including some Case Studies, also.

I own my regards to NIC from where I have learnt the management and techniques to inculcate the project that enabled me in the entire duration of this work.

# CONTENTS

# Implementation of Personal Data Protection Policies in IT Applications

**(DIGITAL INDIA INTERNSHIP)**


**Project Trainee**

Nikunj Pansari

(Cyber Security Research Intern)

**Project Head/Mentor**

Deepak Goel

Legal Services Division

STD & HOD

## Introduction

Data Protection and Privacy is the most important concern of any organization or for an individual. Pertaining to the needs, standard rules and regulations are the prime factors for maintaining privacy of an individual & safeguard the interests of the organization's personal data. Implementation of various IT Companies are working in different ways for its execution through varied principles and methods. *[Annexure (1.1)]*

## Data Protection Laws in India

- The Indian Supreme Court affirms the fundamental right to privacy.
- Current data protection laws in India are seen as too narrow, and pressure has been applied to enact new legislation more consistent with global trends, including the right to be forgotten.
- New legislation could expand the extra-territorial jurisdiction and applicability of Indian data protection laws.

## Domains /Industry concerning the Personal Data Protection –

- Processing office employees' personal data
- Processing PII (Personal Identifiable Information) of an individual.
- Processing PII associated with business domains of the organization.

## Aims of the Personal Data Protection-

- Uniform instead of defragmented rules for personal data.
- One stop shop for securing the PII of an organization
- Strengthen existing rights & introduce new laws to tackle the existing technological challenges for maintaining data privacy.
- Transparency, accountability and self-regulation for strengthening the DPA's cooperation regarding sensitive data.
- Risk-based: obligations proportional to risks can lead to data loss.

## Personal Data Protection and the Tech Industry

The Personal Data Protection will definitely transform the way businesses functions in the tech industry work. There are currently over 2.5 quintillion bytes of data produced every day, and much of that data is personal in nature and used for various activities by tech companies. Because of the huge amount of data being processed and controlled, the Personal Data Protection is reported to be one of the most expensive pieces of regulation. It is imperative that companies ensure their policies and procedures are clearly defined and meet Personal Data Protection law.

## Challenges for the Tech Industry

Many in the tech industry have cited four of the Personal Data Protection's requirements to be the most difficult to meet:

1. **Documentation of all the "personal data" the company has processed or stored and being able to delete it or provide it to the individual upon request.**

   As far as the documentation is concerned, most of the companies try hard to maintain the privacy and security of the personal data, but when it comes to providing the same to the individual or the organization, they face a lot of difficulty.

   They can either keep the useful data with themselves and store it on their storage medium or just delete it, to free up their storage space.

   **IT Implementation-**From the IT implementation point of view, this documentation of the personal data of an individual or an organization is quite useful. They can make a replica of the original file, and then work on the further documentation. They can use different masking and Encryption algorithms for securing the personal data.

2. **Hiring Data Protection Officers, a great expense for many companies.**

   Data Protection Officers are also an important part to maintain, monitor and report the security loopholes in the data(PII).

**IT Implementation-**DPOs can also improve the efficiency of the Data protection but manually only. Hiring of them can lead to a great expense for most of the companies. It can affect their budget structure and can ultimately also alter the functioning of an enterprise.

3. **Identifying and reporting data breaches as early as possible.**

Data Security and Identification of all the risks associated with the personal data.

**IT Implementation-**Timely reporting and monitoring of the data breaches of the organization(PII).

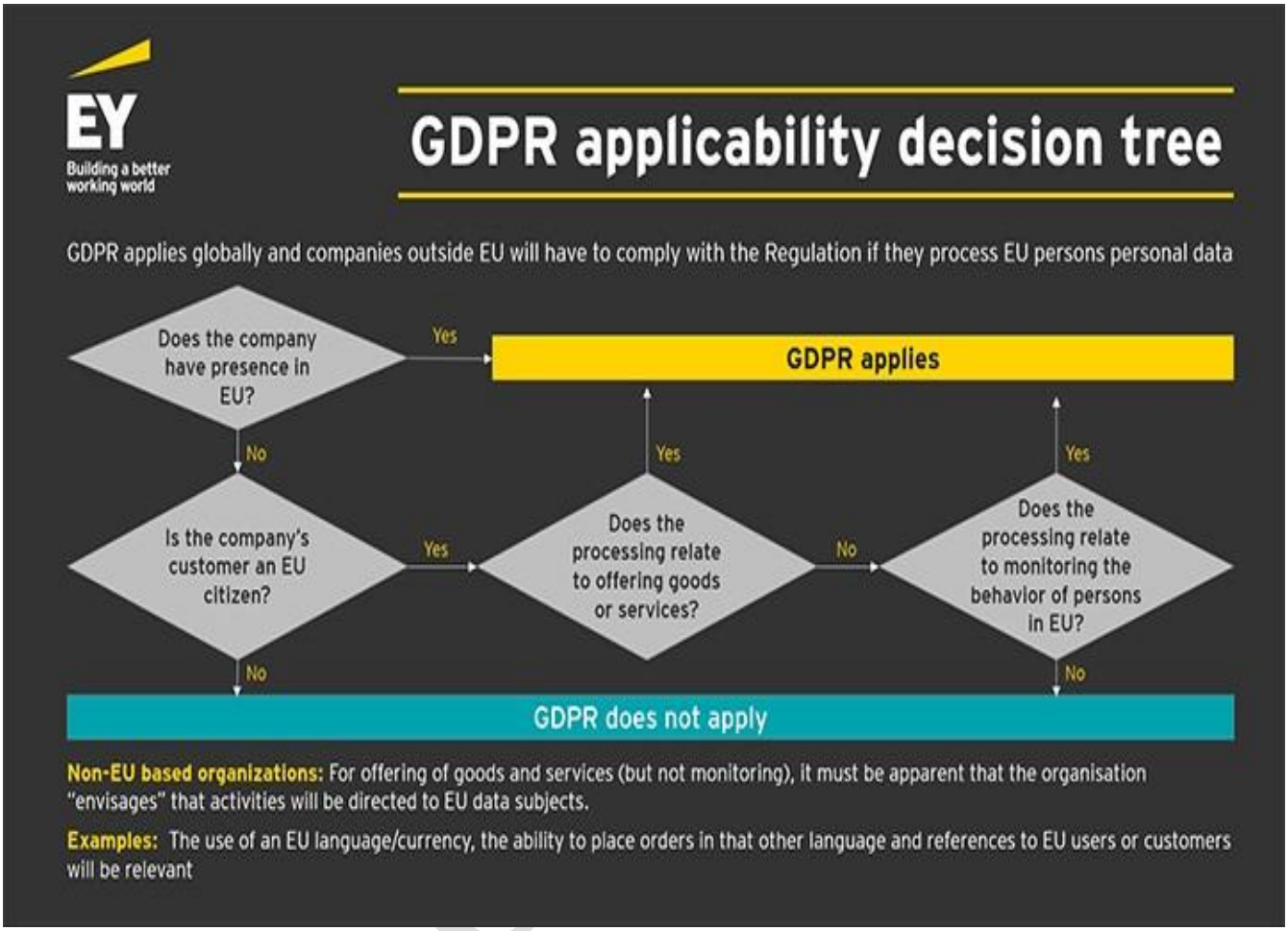
4. **Customers will be allowed to download and take away their data, potentially giving it to a competitor.**

Consumers have easy accessibility to their personal data so that they can protect it and at the same time, maintain the integrity of the same.

**IT Implementation-**User friendly services to the consumers for maintaining their personal data (protection and privacy) so that it can help in data loss.

## Importance/Focus-

The main focus of the implementation phase in IT application is on **(Chapter 2, 3, 4 and 8)(1.1)**. All these chapters containing various Articles are defined specifically for the Data Protection and Privacy for the IT Applications.



**Analysis for ensuring Personal Data Protection compliance** (in reference to Tata Consultancy Services) *(Annexure-1.2)*

## (A)IT Implementation point of View

- **Processing and Storing Personal Data** -
  Business logic depending on requirement-The personal data should be made into use only for the required or stipulated period of time. It should be ethically worked with and processing should be lawful and fair, without any kind of biasness.

  No indefinite use of the personal data should be inculcated, so, as to violate/deny the Right to Privacy.

  **IT Implementation**-Appropriate masking, encryption and anonymization of all the PII according to the exact working procedure and functioning.
  PII should be secured at any cost, with barring the replication of the personal data and knowing wherever copied with the version controls.

- **User Consent**-
  All the collected data should be processed and made into use only after the legal (lawful) consent from the user.
  **IT Implementation**-The user consent is important in maintaining the integrity as well as the authentication of the data of the user.
  All the processes linked to the Value Added Services and other monetization strategies should be perfectly in accordance with the user's needs.

- **Rights of the Data Subject**-
  Major emphasis is on the Right to access, modification, right to be forgotten and data portability.
  **IT Implementation**-Ease in the data modification and portability facilitation, so that, management framework including the data minimization and access control could be ensured. Data security and maintenance of it, is the sole responsibility of the data owner, himself.

- **Data Protection by Design**-
  Carrying out the data protection impact assessments regularly, both by design and by default.

**IT Implementation**-Data Encryption, masking and Pseudonymization solutions can be leveraged easily.

Remote accessing and the Data management strategies for onsite and off-site employees, can go together considering the internal threats. It help in improving the efficiency of the employees.

A VAPT (Vulnerability Assessment and Penetration Testing) report can be maintained for all the applications and BCP (Business Continuity Plan) can also be devised.

## (B)Post-Analysis IT Implementation or processing of PII

- **Records of Processing** -
  All the processing activities should be properly, strategically and systematically monitored as per the defined norms. Maintain a Personal Data Protection based Compliance and assessment report as per the nature of records.

- **Data Breach**-
  Data Breach should be identified as early as possible and should be reported within at max 72 hours of the incident. Appropriate policies should be devised so as to curb/reduce the breaching of the Data.

- **Impact Assessments**-
  Risk Analysis and Impact Assessment should be performed on the records or data set, in order to identify and mitigate the risk. A suitable compliance report program should be made to audit program for risk management.

- **Data Protection Officers(DPO)**-
  A DPO should be assigned a proper task for monitoring the Data Security Breach and the Personal Data Protection compliance. Fixing the accountability for proper Data governance.

# Personal Data Protection-An Industry and Geography agnostic regulation(Infosys)

## Industrial ramifications

For certain industries, personal customer data is a precious commodity. This data predominantly falls under categories 2 and 3 in the above table. For example, the financial services industry deals with highly sensitive and high-risk data containing financial records of individuals that can directly identify data subjects. The healthcare industry also keeps records of sensitive health-related personal data that can identify a data subject.

Owing to the sensitive nature of such data, a privacy breach has serious repercussions in terms of negative brand image, legal ramifications, and heavy penalties. Thus, the onus for data protection rests squarely on the DPO due to the high-risk nature of data and proliferation of data between various systems and processes.

## Technical ramifications

Most of the existing enterprise cloud applications and enterprise documents that are stored and shared across organizations are not GDPR-compliant. As GDPR takes effect, organizations can expect significant changes to budget allocations, and technological and infrastructural changes, as well as expenditure for security and storage software.

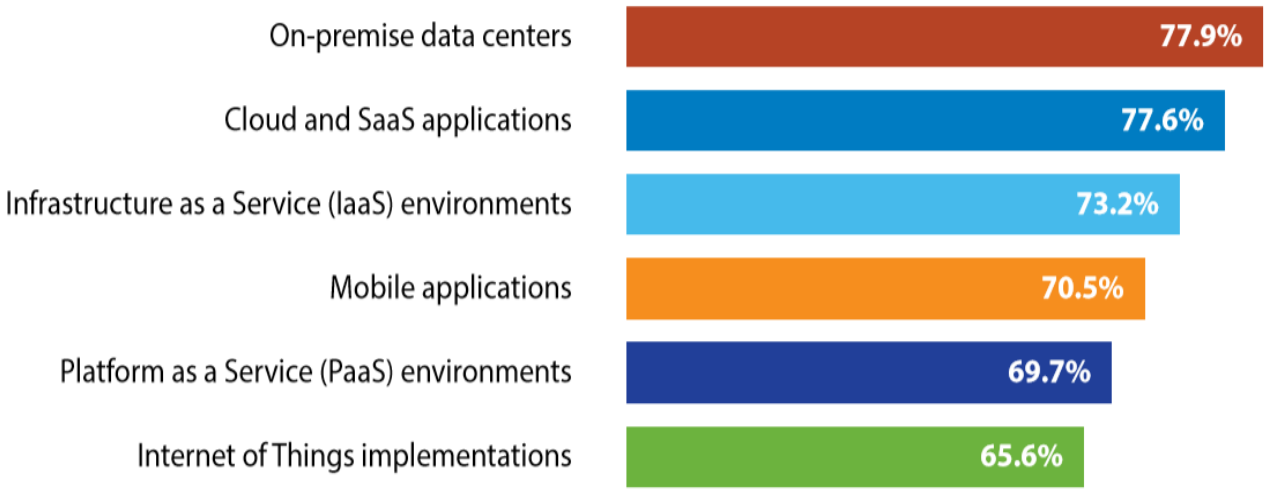



*Fig 3: Technology environments that will be regulated for sensitive data within the next 3 years*

## How can my organization prepare for GDPR?

Organizations can expect significant changes with the rollout of GDPR. Thus, it is paramount that they study the features of this new regulation and learn how to implement it while unlearning existing data regulations. This requires a dedicated as-is analysis to uncover the lacuna between the future-state and existing data models.

The Infosys Framework for GDPR (ADAM - Assess, Define and Design, Administer and Implement, Manage and Secure) is an end-to-end solution that helps organizations achieve GDPR-readiness in four phases:

- **A: Assess –** Here, Infosys identifies the gaps between GDPR requirements and the organization's current state and generates a road map. An organization-wide assessment is conducted that can be further drilled down to an application-level assessment, if required.
- **D: Define and Design –** In this phase, policies for GDPR requirements are defined at the organizational / unit level and the future data architecture to support these policies is designed.
- **A: Administer and Implement –** Here, the processes and technology changes identified in the previous phase are implemented, tested, and integrated with the existing system.
- **M: Manage and Secure–** This phase focuses on providing support and enabling audits while the refined system is deployed across the organization.

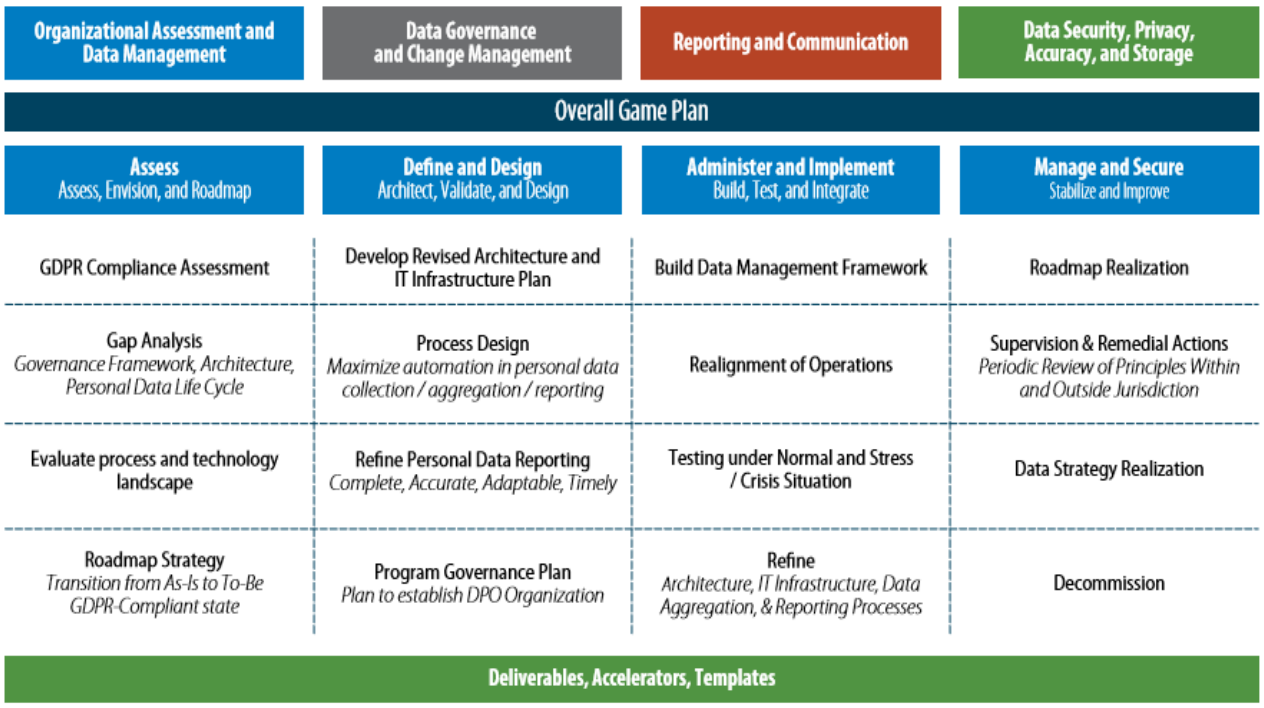



*Fig 4: Infosys Framework for GDPR*

## How can Indian Organizations prepare for the Personal Data Protection regime??

### Organizations need to look at the following aspects as part of their compliance efforts:

- Develop a vision and strategy for compliance with the Personal Data Protection.
- Assess gaps between your current compliance programme and the requirements of the Personal Data Protection, and analyze risks.
- Create an accountability framework for data protection compliance.
- Develop the operational structures needed to facilitate compliance.
- Document processing activities and data flows.
- Review lawful processing bases and third-party contracts.
- Create processes for privacy by design and privacy impact and risk assessments.
- Identify and prioritize key remediation activity to reduce your risk profile.

### Areas which need focus under the Personal Data Protection are:

- **Data processing**
  Personal Data Protection rules can be easily used for the data processing and data protection activities. They help in maintaining the integrity of the PII.
- **Notice and consent**
  Appropriate user content is also benefited due to this data protection rights and principles.
- **Data subject rights**
  Rights to access, modification, right to be forgotten and Data portability. These rights provide an ease in IT Implementation for the security of the PII.
- **Accountability**
- **Third-party and vendor management**
- **Transparency of information and communication**
- **Data security, storage, breach, breach notification**
- **Training and awareness**

## How should Indian companies prepare for the Personal Data Protection?

### Indian companies need to carefully look at the requirements for Personal Data Protection compliance. They need to:

- Review policies, procedures and existing privacy programmes.
- Conduct data discovery exercises and maintain documentation in order to demonstrate visibility of the personal data processed;
- Impart data privacy training to employees or subcontractors;
- Implement processes to perform data protection impact assessments (DPIAs), manage data subject requests, privacy by Design, etc.
- Review/update contracts signed with third-party vendors.

### In addition to the above, organizations should focus on changing the technologies they use and should consider:

- Pseudonymisation and encryption required while processing personal data;
- Reviewing and updating configurations of data loss prevention (DLP), Security Information and Event Management (SIEM) and other technical solutions;
- Equipping the security ecosystems with effective identity and access management (IdAM) solutions;
- Reviewing data retention schedules, cross-border data transfers, privacy notices, consent, etc.;
- Logging monitoring and incident management solutions;
- Investing in systems to carry out data discovery exercises to determine what/how/where PII (specifically unstructured data i.e. PII stored on local workstations, emails, file servers, etc.) is handled within the organization will help Indian companies to enter the Personal Data Protection regime smoothly. ***(Annexure-1.3)***

# DATA PROTECTION AS A SERVICE

Data protection as a service (DPaaS) is a cloud-based or web-delivered service for protecting data assets. Companies can utilize this type of service to enhance network security and to build better security for data in transit and data at rest.

Companies that offer DPaaS provide tools and services that can deliver the functionality of modules, such as network analysis software programs, through a service model. In addition to keeping data safer, DPaaS providers claim that their tools can help clients in bringing their own services to market.

In general, DPaaS tools support the use of technologies like VPN to aid in remote work security. In addition to having these secure "tunnels," clients may need data backup solutions and more. DPaaS vendors step in and inject their services into the data models used by a business for remote computing. DPaaS services may include the use of hypervisors and network virtualization tools, or firewalls and other resources. Where previously security used to be built into a physical network at a corporate site, much of it can now be outsourced to DPaaS vendors.

There are three basic components for the business continuity: There's offsite backup, disaster recovery, and data protection as a service (DPaaS). Data protection has an important role, besides the disaster recovery and offsite backup. Below are a few examples of practical applications of data protection as a service in:

**Example A**: Company A is a data clearinghouse for the healthcare insurance industry, and requires a more efficient way to tackle their long-term data clearance and data archiving. They use DPaaS for cloud-based archive storage that's easily retrievable for compliance reasons. There's no software or vendor lock-in with the cloud, so the old-data can be easily retrieved without much considering about the software compatibility.

**Example B**: A healthcare company was looking to overhaul their traditional tape-based backup system, and turned to DPaaS. DPaaS restores large files faster and more frequently than traditional backup, with no proprietary deduplication of data. In addition, the company can choose their own backup windows, and data is retrievable within hours rather than days, all while remaining in compliance with federal HIPAA regulations. This has saved the company hundreds of hours that would normally have been spent waiting for their data to be restored.

**Example C**: A SaaS company seeking more agile web development can use DPaaS to quickly restore large databases (think 10 TB) and create zero-byte copies of production databases for dev, testing and QA. When they need to access a database for development or testing purposes, all sensitive information is automatically scrubbed to maintain data integrity.

## Nonprofit Enterprise at Work – A Virtualized Desktop Case Study

### THE CHALLENGE

After working with their nonprofits, NEW discovered that many of their small and medium-sized clients did not have the funding or resources for IT equipment or staff to operate effectively in a technology-driven business landscape. In fact, many nonprofits did not even have access to the Internet nor did they have basic office functions like email, shared files, secure data backup or remote access.

As a way to provide nonprofits essential technology support and infrastructure, NEW developed the program, npServ. npServ helps nonprofits cut IT costs, operate more efficiently and stay focused on their missions. "The idea behind npServ is to go into an organization, install relatively unique IT systems and manage them remotely from our locations," says Neel Hajra, NEW President and CEO.

The npServ program is essentially a virtualized desktop platform using a combination of open source office technologies hosted at Online Tech's SAS-70 certified data centers.

The open source desktop virtualization uses older, cost effective desktops to connect through a portal to the hosted servers. Nonprofits can avoid purchasing expensive workstations and having to replace hardware when it becomes obsolete by moving to npServ's thin client devices. With npServ, a single server hosted at Online Tech runs all of the different working environments for all of their clients' workstations. Plus, the thin client model reduces NEW's maintenance costs and makes it easier to support their customers remotely. NEW is able to serve more nonprofits and support them at a price point lower than they expect to pay for other IT services.

While developing npServ, NEW realized that they would need an enterprise-level server infrastructure to support the program. npServ would require a centralized server in a secure data center for all of their nonprofit's data to be backed up and stored. With these technical requirements, NEW realized that they had to go beyond the usual nonprofit "mom and pop" solution. They would require a managed server with 24x7 support.

## THE SOLUTION

"We knew that we needed a world class data center with world class service and support and Online Tech is the leading managed data center operator in Michigan," says Hajra. Through a generous grant, Online Tech agreed to provide managed dedicated servers and back-up services to NEW and their nonprofits.

NEW recently aided a Detroit-area nonprofit who had been without email for a week and no access to their server. It had become nearly impossible for this organization to continue to serve their community without access to documents and email.

"As we started troubleshooting and eventually added them to our Linux thin client program, we learned that data security was a sensitive issue for the organization. Not only was there data that needed to be HIPAA compliant, but like many nonprofits, there was staff turnover creating an increasingly difficult challenge in maintaining institutional memory," says Linh Song, Director of npServ. Installing a fileserver with different permissions was a first step for the organization. But more importantly, this organization needed to make sure their critical data was saved and secure offsite. NEW

was able to get this organization back up and running and set them up in Online Tech's secure HIPAA compliant data center.

"It is nice to work with experts in the field who are the best in the business," says Hajra. "From Yan Ness (Online Tech's CEO) down to the support staff our team works with, we get treated like every one of other Online Tech's clients even though we are a relatively small nonprofit. We have been really happy with the support and it has given us the confidence to expand and grow knowing we have a strong data center partnership backing us up." In fact, Hajra has found that when NEW talks with potential nonprofit partners they are always reassured that npServ is supported by a world class managed data center operator like Online Tech.

# What is personally identifiable information (PII)? How to protect it under Personal Data Protection?

Personal Data Protection requires companies to protect the privacy of their customers. That means keeping personally identifiable information (PII) safe.
Personally identifiable information (PII) is any data that can be used to identify a specific individual. Social Security numbers, mailing or email address, and phone numbers have most commonly been considered PII, but technology has expanded the scope of PII considerably. It can include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioral data can also be classified as PII.

It creates security and privacy challenges, especially when specific and stringent safeguards for it are spelled out.

The new rules grant people more rights regarding how companies handle their personally identifiable information (PII), and it imposes heavy fines for non-compliance and data breaches--up to 4 percent of a company's yearly revenue. The Personal Data Protection also requires that companies report data breaches as soon as possible.

## Top 10 priorities to make Indian Companies Personal Data Protection-compliant

It is high time for Indian organizations to look at ways that help them comply with the regulation in the shortest possible time. Many Indian Information Technology & ITeS, pharmaceutical and financial services firms have presence in the market. They need to take the speedy lane to comply with the Personal Data Protection to avoid fines which regulators will be entitled to as per the unprecedented powers provided to them.

Here are the top 10 priorities that organizations need to focus on for speedy compliance:

- **Spread awareness within the organization:** Ensure key stakeholders and decision makers in the organization are aware of the Personal Data Protection and its impact so that resources to be allocated are identified in the right time frame. Organizations are required to train staff on key Personal Data Protection requirements and at the same need to issue instructions to them on handling personal data appropriately.

- **Maintain records of personal data processing activities**: Organizations should conduct data discovery exercises to identify where and how personal data and special categories of personal data, as defined under the Personal Data Protection, are processed within the organization.

- **Determine the legal basis for processing personal and special categories of data:** Organizations should identify the legal basis for processing personal data for each processing activity and assess its validity.

-- The data subject has given explicit consent
-- Due to an obligation on, or a specific right of, the controller
-- The personal data has been clearly made public by the data subject

- **Create/review privacy notices and consent**: Privacy notices have to be drafted or updated as per the Personal Data Protection requirements to include the range of information that controllers must communicate to data subjects. Since under the Personal Data Protection, consent must be freely given, specific, informed and unambiguous, the organization shall review how it seeks, records and manages consent to process data and implement mechanisms to obtain and record consent (where applicable) both retrospectively and for new personal data processing activities.

- **Uphold data subject rights:**
  -- Respond to subject access requests
  -- Support rectification of personal data
  -- Handle objections to processing of personal data
  -- Enable personal data portability
  -- Erase personal data as requested by data subjects
  -- Investigate objections to automated decision making

- **Manage privacy incidents:** It is important for organization to update the existing security incident management processes to cover the identification and initial handling of suspected personal data breaches. They also need to use automated security tools to detect suspected data breaches that may involve personal data, for example:

-- Intrusion detection systems (IDS)
-- DLP
-- Security information and event management (SIEM)

- **Manage data protection impact assessment (DPIA):** Organizations need to define the circumstances under which a DPIA is required as per the Personal Data Protection. They need to perform DPIA for any personal data processing likely to pose a high risk to the rights and freedoms of natural persons and managing the potential impact on data subjects from processing such personal data.

- **Appoint a data protection officer (DPO)**: This will be essential when an organization is a public body, is processing operations requiring regular and systematic monitoring, or has large-scale processing activities, or when a member state law specifies the appointment of a DPO.

- **Meet data transfer requirements:** Organizations have to establish a process for managing personal data transfers and adequately protect the rights and freedoms of data subjects when transferring personal data to internal or external parties.

- **Establish data processor accountability:** The Personal Data Protection requires organizations to perform due diligence before establishing a relationship with a third party and ensure contracts with them to process all the PII.

## Data masking: anonymization or pseudonymization?

The two techniques differ and in face of the Personal Data Protection the choice will depend on the degree of risk and how the data will be processed.

## What is pseudonymization?

Pseudonymization enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Specifically, the Personal Data Protection defines pseudonymization in Article 3*(Annexure-1.1*), as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymize a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

## Pseudonymization or Anonymization?

The legal distinction between anonymized and pseudonymized data is its categorization as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified.

Pseudonymization techniques differ from anonymization techniques. With anonymization, the data is scrubbed for any information that may serve as an identifier of a data subject. Pseudonymization does not remove all identifying information from the data but merely reduces the link ability of a dataset with the original identity of an individual (e.g., via an encryption scheme).

Both pseudonymization and anonymization are encouraged in the Personal Data Protection and enable its constraints to be met. These techniques should therefore be generalized and recurring. Those in possession of personal data should implement one or other of these techniques to minimize risk, and automation can reduce the cost of compliance.

## Which data should be anonymized?

By definition, data anonymization techniques seek to conceal identity and thus identifiers of any nature. Identifiers can apply to any natural or legal person, living or dead, including their dependents, ascendants and descendants. Included are other related persons, direct or through interaction.

**For example:**

- Family names, patronyms, first names, maiden names, aliases.
- Postal addresses
- Telephones
- Postal codes + Cities
- IDs: social security number (e.g. Fiscal Code in Italy, National Insurance number in UK), bank account details (e.g. IBAN), credit card numbers, valid keys, partial anonymization.

# Personal Data Protection, Data Masking & Encryption usage

| Characteristics | Persistent Data Masking | Dynamic Data Masking | Tokenization | Encryption |
|---|---|---|---|---|
| Protects sensitive data at rest (in storage) | ✔ | | ✔ | ✔ |
| Protects sensitive data when accessed | No one can see original data | Authorized users can view data | Authorized users can view data | Authorized users can view data |
| Protects data in transmission | | | | ✔ |
| Obfuscation based on user privileges / roles | | ✔ | ✔ | ✔ |
| Suited for protecting sensitive data in production | | ✔ | ✔ | ✔ |
| Suited for protecting sensitive data in non-prod | ✔ | | | |
| Impact on application performance | None | 2-3% | More significant | 2-3% |
| Does not require change in application to implement | ✔ | ✔ | | Change in database |
| Support indexing, optimized search | | ✔ | ✔ | Some limitations |
| Format preserving | ✔ | ✔ | Limited | Limited |
| Repeatable – resulting obfuscated data is deterministic | ✔ | ✔ | ✔ | ✔ |
| Reversible – original data is retrievable | | ✔ | ✔ | ✔ |
| Original data is not stored anywhere | ✔ | | w/ stateless tokenization | ✔ |
| Original data is still stored either in original location or central location | | ✔ | | |

**Masking:** 3 use cases: Test data, live data in transit, production data at rest (or used by an Application).

Personal Data Protection uses terms like pseudonymisation (masking). Article 4 defines pseudonymisation (masking) as:

**"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person**".

**This could include:**

- an encryption key or mapping table,
- making sure that the data cannot be used to identify an individual
- removing direct identifiers, ideally prevent indirect identifiers from being combined and used (e.g. name from one part of the system, address from another, and bank card # from another).

**Masking vs Encryption-** Masking and Encryption can be used together in most architectures for data in transit and data at rest. Note that Masking can replace encryption for data at rest.

**Benefits of Masking over Encryption could include:**

1.1) better at maintaining relationships within databases than encryption.

1.2) can be applied dynamically, causing fewer application side effects.

Encryption is deployed as part of the infrastructure (SSL, TSL, in transit, embedded in SAN) or as part of the data masking process — particularly to satisfy regulations like Personal Data Protection that prescribe encryption.

## Pseudonymised data vs. anonymous data

Despite pseudonymised data removing any direct identifiers, because that information still exists – albeit in a separate, secure form – if it were to fall into the wrong hands it could be used to revert the data to an identifiable form and then acted upon in an inappropriate way.

Therefore, pseudonymised data is still classified as personal data, and cannot be considered anonymous. It's important to make this distinction, because anonymous data is not subject to the Personal Data Protection controls and restrictions, whereas pseudonymised data is.

If the data can be re-identified with reasonable effort, it cannot be regarded as anonymous, despite data masking being used. However, if you were to mask data and then delete the original data set and its identifying information, it would be almost impossible to identify an individual and would thus be classed as anonymous.

## The benefits to businesses

Although pseudonymised data is still subject to data protection regulation, it is afforded a new distinct status under the Personal Data Protection, which could be beneficial to many businesses.

The data protection does not recognize any distinction between regular personal data and pseudonymised data. Any kind of data masking is treated the same as raw personal data, and subject to the same, full weight of the law. As such, there is no incentive or regulatory benefit to putting in the extra effort and cost to protect data by masking, hashing or encryption.

The Personal Data Protection changes that. It specifically promotes the value and importance of pseudonymisation throughout its articles, encouraging companies to adopt such security measures as soon as possible.

### The reduction of data breach notification requirements

There are strict new protocols on reporting data breaches of the Personal Data Protection. If such a breach occurs, companies are responsible for reporting it to both the supervisory authority (as soon as possible) and to all of the individuals who could be affected (without undue delay).

This could be a big burden for businesses, on top of the damage done by a breach in the first place. Along with the financial costs to re-secure data, the requirement to notify individuals could bring about additional reputational damage and associated legal costs.

### An easing of data disclosure obligations

As the Personal Data Protection places more emphasis on the rights of the individual, much of the law is focused on the ability of a person to request information about what data a company holds on them. This is known as the 'right of access', and has the potential to be another large burden for businesses.

However, early interpretations of the Personal Data Protection suggest that data disclosure rules are greatly relaxed for pseudonymised data because it is too difficult for a business to identify a single individual.

## Further use of data beyond its original purpose

Another core feature of the Personal Data Protection is the requirement that data is collected only for specific purposes that are clearly explained. The law states that data must not be used in any other way than that which it was originally collected for.

However, if the data has been pseudonymised, there is more leeway for it to be processed in other, additional ways. If a business wanted to process personal data for scientific, historical and statistical purposes, the Personal Data Protection also requires appropriate safeguards be in place – i.e. pseudonymisation.

## Additional data profiling options

One final benefit to businesses who implement data masking or other such pseudonymisation is that data profiling should still be possible, without running afoul of the law.

The Personal Data Protection makes broad statements about the use of profiling, and goes on to explain that businesses should not make 'decisions' about an individual that has a 'legal effect' – based on such automated processes – unless a number of legal criteria is met, including the explicit consent of the individual.

This has the potential to have ramifications for analytics and digital advertising. Although the law is somewhat ambiguous, pseudonymised data is likely to reduce any kind of 'legal effect' on an individual, and so profiling for analytical purposes should still be permitted.

# Data masking and Personal Data Protection compliance

On the one hand, those businesses who put such *'appropriate safeguards'* in place will be looked upon favorably. They will have certain requirements relaxed, have more flexibility with their processing, and could be protected from heavy fines if they have the necessary technical and organizational structures in operation. That's the carrot.
On the other hand, the Personal Data Protection provides both regulatory bodies and individuals with additional powers to make data requests and legal claims against those companies which process their data. They have much more clout under the law to act against non-complaint businesses, thus further incentivizing companies to protect personal data with procedures such as masking – for both production and non-production.

But the real stick is the heavy fines that can be imposed upon companies who break the law, are subject to data breaches, and do not have any kind of pseudonymisation in place. Those who do not have adequate protection and security could be subject to fines as high as 4% of global

turnover. Compliance is, therefore, an absolute must and something which all departments need to understand.

## Top 3 Reasons to Include Data Masking in Your Data Security Strategy

Also known as data anonymization or pseudonymization, data masking is used to reduce the unnecessary spread and exposure of sensitive data within an organization—protecting it while simultaneously maintaining its usability. Data masking replaces real data with functional fictitious data so that it can be used safely in situations where actual data is not needed. **Data masking can protect many forms of sensitive data, including (but not limited to):**

- Personally identifiable information (PII)
- Protected health information (PHI)
- Payment card information (subject to PCI-DSS regulation)
- Intellectual property (subject to ITAR and EAR regulations)

With data masking, data values are changed while data formats remain unchanged. For example, credit card numbers have a 16-digit format that looks like this: 1234-5678-9123-4567. Masking data changes the numbers, but maintains the same 16-digit format. Using the example above, the masked credit card number could become: 9876-5432-1987-6543. Data masking uses several methods to alter sensitive data, including character or number substitution, character shuffling, or the use of algorithms to generate random data that has the same properties as the original data.

Given the high priority need for organizations to protect their sensitive data, here are three top reasons IT security practitioners should include data masking in their broader data security strategy.

### 1) Protect Non-Production Data

For many organizations it's often necessary to make copies of production data for non-production use. Examples include:

- Application development and testing
- Personnel training
- Business analytics modeling

Having one or more copies of sensitive data floating around increases your risk of it falling into the wrong hands.

While enabling the safe sharing/copying/use of sensitive data, masking lets you protect those data sets, and meet compliance requirements without hampering your business operations. So

long as your data remains usable for non-production purposes, masking can control the spread of real data that could be vulnerable to a breach or outright theft. It also reduces your organization's potential attack surface.

**2) Protect Against Insider Threats**

Trusted employees who are already inside perimeter defenses—developers, trainers, business analysts—may have a legitimate need to access data, but may not need access to real production data.

By masking sensitive production data, organizations liberate the data employees need to get their jobs done while reducing the risk of a data breach from a malicious, careless or compromised insiders.

**3) Comply with Personal Data Protection**

Intended to strengthen and unify personal data protection, in part it's a reaction to data breaches affecting the other citizens. *(Annexure-1.4)*

**Personal Data Protection introduces two key concepts:** data minimization and pseudonymization as ways to protect citizens' privacy rights while letting data controllers use collected data for other purposes.

Personal Data Protection requires that organizations practice **data minimization**, which is that they collect and use data limited to what is necessary for a specific purpose, retain it no longer than necessary and not make it available to an indefinite number of people.

E.g. if an insurance company collects personal information for the purposes of issuing a policy, and they now want to analyze this data collected from their clients to improve pricing of policies, they would not be able to do it because the personal data collected for one purpose (e.g., issuing a policy) cannot be used for a new purpose (e.g., creating a database for pricing analysis).

However, if the data is pseudonymized or anonymized via data masking, then they could use the masked database for pricing analysis.

**Pseudonymization** can also be used to meet Personal Data Protection's data security requirements. Data masking is a means to pseudonymize data, especially in non-production data environments such as application development and testing, training and analytics. By replacing sensitive data with realistic, fictitious data, data masking solutions help organizations comply with key Personal Data Protection requirements.

## Encryption-How Does Personal Data Protection get affected by it and How does it view it?

Encryption is a broadly used process whereby data gets turned into an encoded and unintelligible version, using encryption algorithms and an encryption key, and whereby a decryption key *(which in some forms of encryption is the same as the encryption key)* or code enables others to decode it again.

Encryption is a form of cryptography and comes in many shapes and types, with various solutions and applications, including plenty of Internet and data transmissions and operations we often don't "see" or know about. Encryption and cryptography are also key in the transaction update data model of block chain.

There is obviously far more to say about it but in the scope of this article where we look at encryption under the Personal Data Protection, for now let's say that data encryption is an increasingly used data protection method.

### What if you don't implement encryption?

In a hypothetical future where the company has lost the personal data information, the question "Was the data encrypted?" comes up. Initially it may be law enforcement, the press, the customers, but eventually the regulator will ask as well with a mind to pursuing regulatory action. The anticipation that personal data subjects and, consequently, the regulators, will take a dim view of companies that have not implemented encryption and an even dimmer view of those that have not even considered using encryption (or cannot prove that they have considered it carefully).

So, Personal Data Protection do require encryption, mandatorily? As a security design professional, the assuming that our network will be breached at some point and given the relative maturity of the encryption market, there's no reason why it should not be a part of every modern information system.

However, that does not mean that it is, on its own, sufficient to meet the demands of the regulator, neither is it mandated. What is mandated is that companies should examine every opportunity to implement encryption and must demonstrate that, where it has not been implemented, it is for a good reason of cost-efficiency or proportionality.

### Encrypting Data

The enterprise's legal, risk and compliance teams must essentially become the custodians of the business and apply corporate governance. Where once IT security controlled the IT and data

security, the scales have tipped in favour of compliance and it is becoming a massive driver for any business decision involving sensitive data. IT departments now need to become the implementers of solutions that meet these data compliance requirements.

Encrypting or tokenising data means that it is scrambled by an algorithm to such an extent that it is rendered unusable to any unauthorised party attempting to access it. The only way to decrypt the data is to use a key, which ideally should be under the control of the organisation who owns the data.

Currently, this is where many companies fall down in relation to Personal Data Protection, as 54% admitted that they rely on their cloud or Software as a Service (SaaS) provider to encrypt data and just over half (51%) think that it is acceptable for the solution provider to control all or part of the encryption keys.

Where 54 % rely on the SaaS vendor for encryption, this is usually for 'data at rest', which under Personal Data Protection is only a subset of the 'comprehensive security' guidelines and recommendations which specifies the protection of PII and sensitive PII 'data in motion', 'at rest' and 'in use'.

The key here, and something that is very well laid out in Personal Data Protection principles, is data control. Specifically, if sensitive encrypted data was intercepted or compromised – can it be reversed? If the answer is yes, then it is still regarded as data and therefore it is treated as data and is subject to Personal Data Protection principles.

## How File Encryption Helps Fulfill Personal Data Protection Requirements?

### The frequent causes of data breaches

- Data theft, either due to a targeted attack on the organization's datacenter or from the cloud.
- Mobile employees with portable devices that they lose in taxis, at airports or forget in their jacket pockets.
- E-mails with unencrypted file attachments that are dispatched to a large mailing list.

### Why encryption is such a vital part of the Personal Data Protection

It is a) logical and b) actually irrelevant that a Personal Data Protection will be unable to prevent all conceivable data mishaps at the drop of a hat. Equally, it is true that there will never be one solution to satisfy all the requirements of the Personal Data Protection.

**"Encryption is too complicated, eats up too many resources and kills the performance of databases and applications".**

It is without a doubt true that reasons such as these ones are often presented to postpone the implementation of an encryption solution or to shelve any plans entirely.

## When is hard disk encryption sensible?

What happens if a device is lost or stolen? The widespread use of mobile devices in corporate settings is making hard disk encryption increasingly important. The operating systems on most devices have a proprietary encryption solution.

E.g. Microsoft BitLocker for Windows or Apple FileVault 2 for macOS.

So, it is imperative to find an integral solution that provides central management of encryption and recovery functions for various platforms. It is equally clear that however important hard disk encryption may be it will not fix all the problems on its own.

Lost and stolen devices are protected and hard disk encryption does not protect devices that are currently in use from targeted attacks, hacking, malware or human error. This urgently requires file encryption.

## File encryption: Which data needs to be encrypted?

People tend to make things more complicated than they need to be. It goes without saying that an "encryption strategy" let loose may quickly reach an overwhelming degree of intricacy:

Which employee in which department is entitled to access which data, and how often? Which data need to be included in mandatory encryption? When might encryption be necessary in particular circumstances only? How do we define these requirements? Moreover, are there data that cannot yet be defined – as things stand – in terms of their encryption relevancy? What happens when all the rules that are used to classify data in terms of their encryption requirements fail, and precisely these data are breached? … There are many important questions.

Alternatively, organizations can take the easy approach and say: We will encrypt everything as a matter of course! After all, each of our data possesses the same importance and requires equal protection!

## What the Personal Data Protection Means for Email Security?

**Email Security**- Email Security systems should:

- Implement appropriate technical measures to comply with "privacy by design," organizations should include email encryption and compliance capabilities to their email security infrastructure.
- Ensure they will be able to comply with requests to access "the right to be forgotten" (the system may need to erase users' personal data and cease further dissemination of the data).
- Be equipped to quickly understand when there has been a breach of personal data and notify authorities as soon as possible of identifying a breach.
- Be prepared to inform organizations as to whether or not personal data concerning them is being processed, where and for what purpose.

### The Customer Privacy is of prime Concern and importance for the organisations:

- **Message Integrity**: Never store clean messages, our multi-layered approach providing a separation of messages and roles within shared platforms.
- **Message Security**: Strong inbound and outbound protection, with real time protection on spam, malware and phishing as well as with anti-fraud, anti-spoofing, authentication and encryption verification.
- **Message Transparency:** Offer extensive message details, permitting our customers to understand exactly the message path, the filtering process and the actions taken.
- **System Robustness:** Provide Secure access at an administration level (e.g. 2 factor authentication, detecting different login tentative), multiple roles, including Helpdesk users with non-privileged access, and multiple delivery authentication, including AD synchronization.

## How to improve security against email attacks and for Personal Data Protection compliance?

### Develop an Email Security policy

Developing a security policy for email can be relatively simple, and a natural first step for bringing organisations into alignment with Personal Data Protection's requirements. However, a company's email security protocols are only as strong as the employees who use them.

The first, cheapest and easiest stage in maintaining any security system is to ensure that all operating systems and applications are correctly patched with the latest updates. Some organisations may be tempted to delay patching, due to possible downtime or the need to

check compatibility with connected systems. But these delays can be costly, as hackers seek to identify known vulnerabilities and are quick to exploit them.

Anti-virus filtering should be used on all email traffic. Although this will not be a complete solution in itself, it will remove much of the "background noise" – the easy-to-spot threats – allowing security teams to focus on the more sophisticated attacks. Organisations should also consider using a secure anti-malware proxy or next-generation firewalls.

Some organisations may want to consider whitelisting or blacklisting filters for managing their email security. With whitelisting, only known, trusted email sources are allowed through; with blacklisting, all but the known, malicious email sources are blocked. Whitelisting offers more protection, but it will inevitably block some important emails, which can cause frustration for employees.

## Dmarc deployment

**Domain-based message authentication, reporting and conformance (Dmarc)** can be used for email authentication to block emails with spoofed addresses, which is one of the **main attack techniques**. Email risk-scoring tools can also be used to identify suspect emails and quarantine them for later analysis.

Dmarc is normally deployed by large organisations and public-sector organisations, but small to medium-sized enterprises (SMEs) can enquire if it can be deployed by their internet or email provider.

Smaller organisations should consider passing all emails through an outsource supplier of email scanning services before they are delivered to the organisation's email server.

Organisations should also consider network segmentation to isolate their email server from the rest of the network, thereby limiting access to sensitive areas of their network. Network segmentation should be deployed alongside regulated access controls and intrusion detection to further restrict access. The best solutions for intrusion detection rely on detecting the techniques used to exploit vulnerabilities.

Email filtering can be adopted through a network appliance before the email reaches the server. This technique allows any suspicious programs to be activated in a virtual sandbox

environment, for the purpose of detecting any host or network activity, in order to detect malware.

## Sending receipts

Although email settings allow requested read receipts to be ignored by the recipients, there are secure email applications that enforce the sending of these receipts. When an email is sent, the sender will receive an email saying when it has been delivered to the email server. A subsequent email will then notify the sender when their email has been opened. If the email has not been opened within three days, a third email is delivered to the sender, informing them it has not been opened.

The drawback of this application is that it increases email traffic. However, it does provide organisations with a clear auditable trail of emails being sent, received and read by the intended recipients. This email auditing is required to comply with Personal Data Protection, because it proves that not only has an email been sent, but that it has been received and read.

But although encryption protects the contents of emails being leaked, it does not block malicious content or attachments.

A multi-layered series of email security protocols will go a long way to ensuring compliance with Personal Data Protection, but only a properly educated and positively encouraged workforce will reliably protect an organisation from attacks via email.

# Test Data Privacy

## Secure Test Data Against Breaches, Reach Compliance

Two core areas that increasingly require mainframe teams to implement a test data privacy solution for more secure test data are -

1) data breach prevention and

2) compliance with data privacy laws.

## Data Breach Prevention

During the application testing process, the customer information may be exposed to development teams, IT vendors and even third-party developers. Any accidental or malicious misuse of test data would be costly and reputation damaging. To counteract this, Test Data Privacy supports static data masking (SDM), enabling the masking or desensitization of personally identifiable information (PII) in data to mitigate the risk of breaches and misuse of production data in test, analytics or training environments.

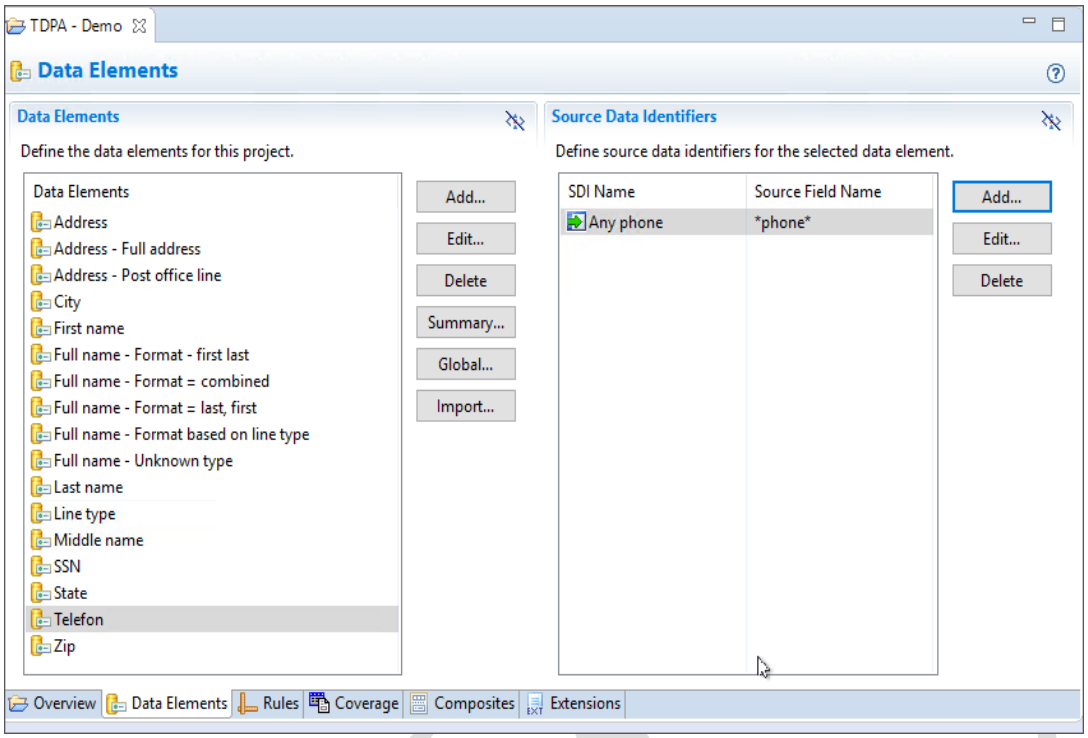
## Compliance with Data Privacy Laws

Using live data for testing creates risk because data used in test environments tends to be less secure. Data privacy regulations require that all data, whether used in production or test be secure. By using Test Data Privacy to apply consistent data disguise techniques across all environments, companies can address requirements to protect PII throughout the application testing process and comply with tightening data privacy laws and company policies.

To help mainframe teams improve these areas, Test Data Privacy provides a wide range of unique capabilities for ensuring test data is secure while remaining realistic.

## Code-free Masking Rules

Test Data Privacy reduces the complexity and tedium involved in masking test data by eliminating the coding of masking rules for every column/field. It groups columns/fields of the same category into one entity that is masked by a single rule.



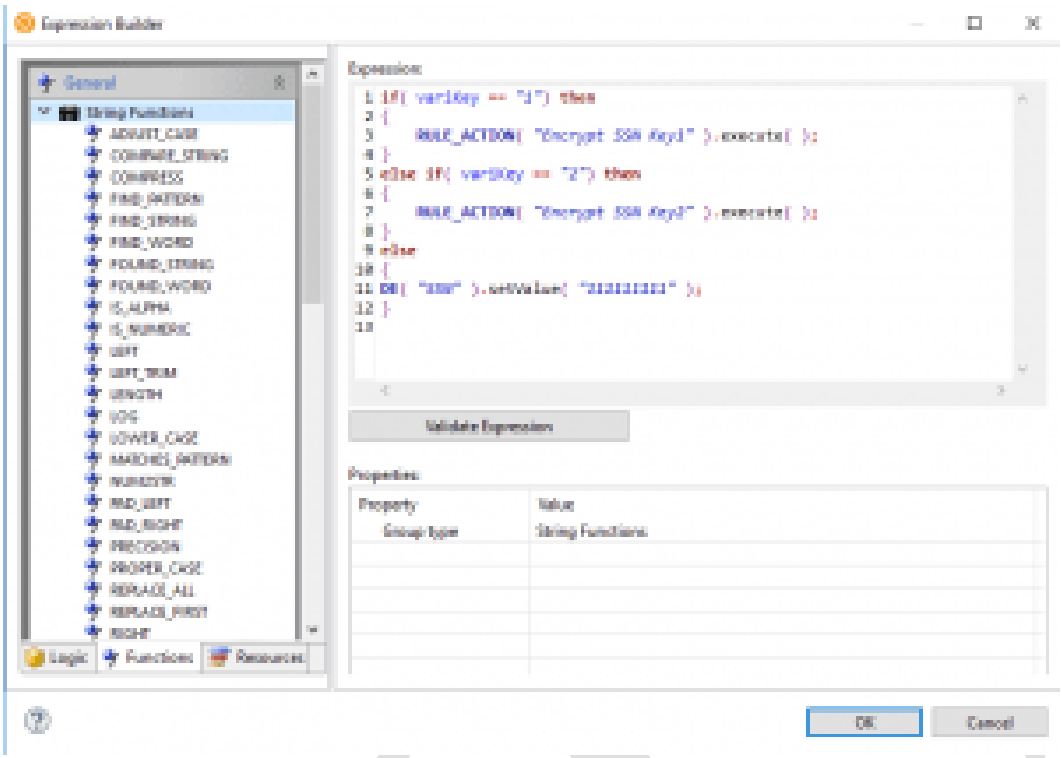

## Data Masking Techniques

Test Data Privacy also provides developers with data masking techniques. Format-preserving encryption keeps the original format of input data, thus making it more usable and realistic for data testing purposes. The translation technique uses existing values stored within files as replacements for sensitive test data values and fits well for fields that require resulting values to be fictionalized, yet still readable to a user and valid for an application test.

Many data manipulation functions are built into Test Data Privacy to handle commonly requested actions like aging dates, standardizing upper/lowercase and calculating check-digit values. In addition, user-defined custom functions can be added to handle unique disguise requirements.

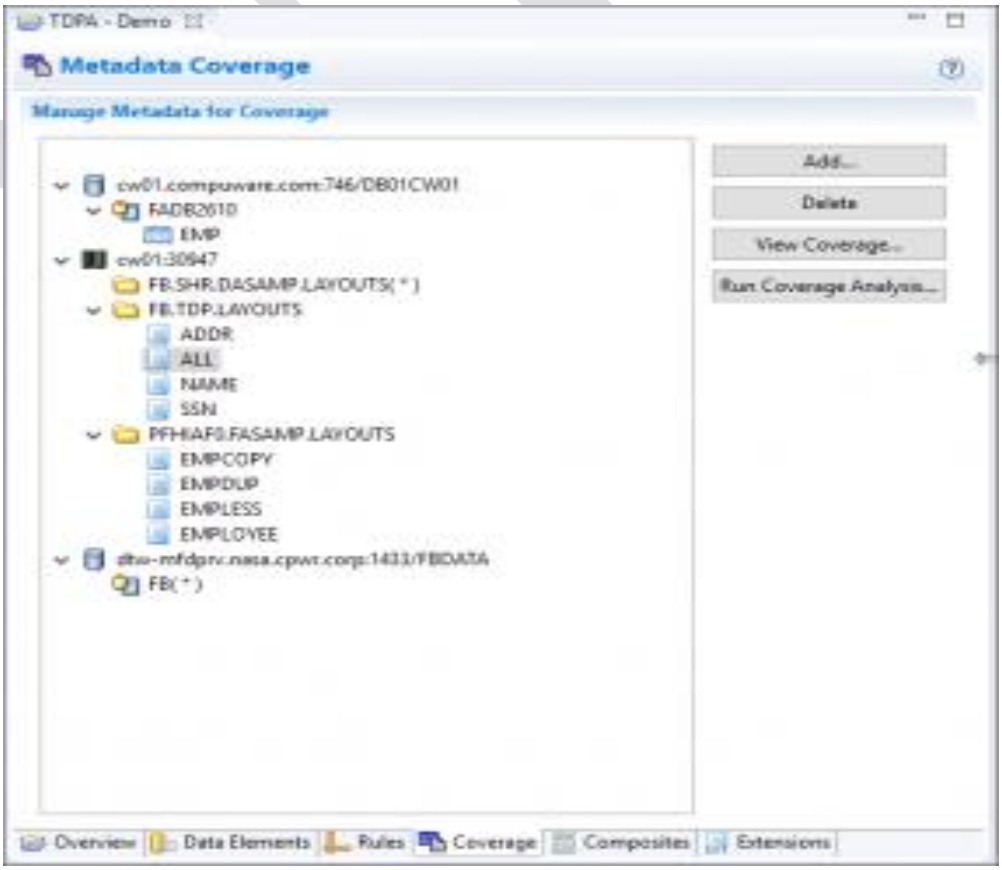
## Java-like Syntax for Building Rule Logic

The combination of robust disguise techniques, built-in and custom functions as well as rule logic will allow you to satisfy whatever disguise requirements your business mandates.



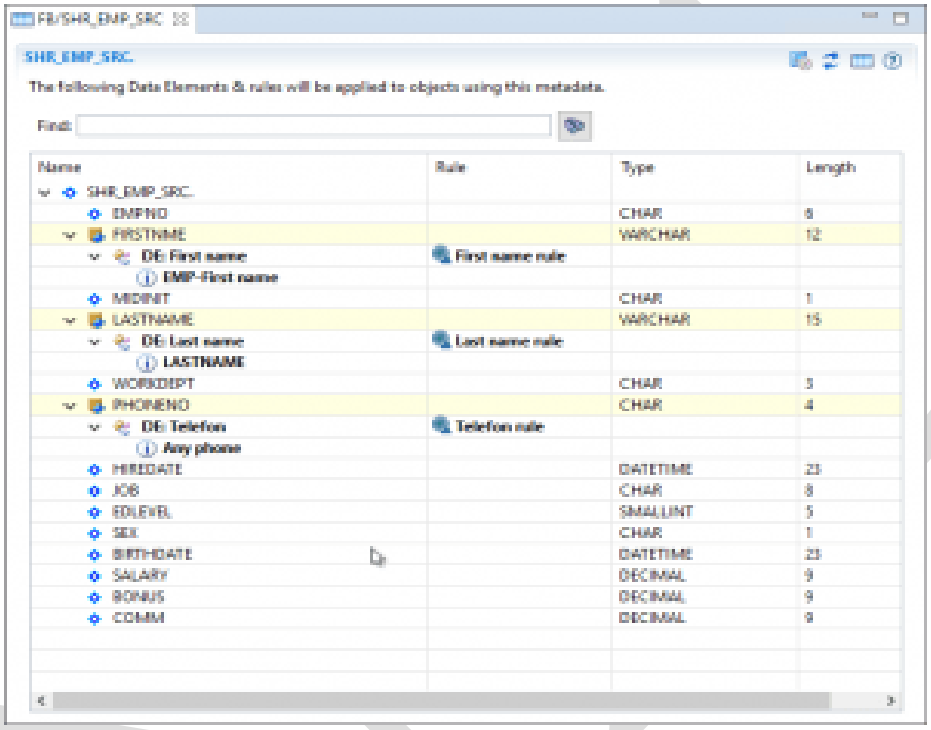

## Consistent Disguise Across Environments

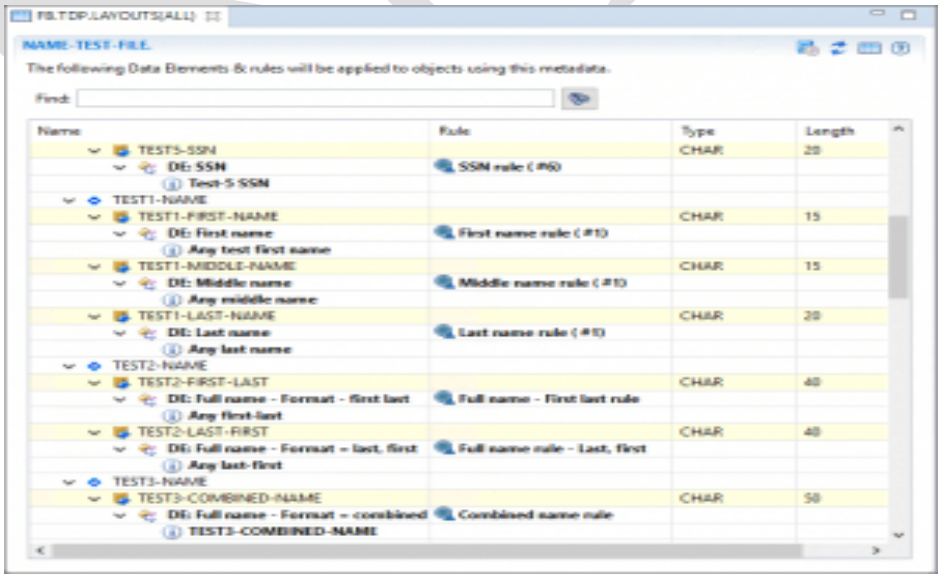
Test Data Privacy's test data masking technology performs data normalization into and out of the masking process, which ensures consistent masking across both mainframe and distributed files and databases, irrespective of the operational platforms or encodings.



## Dynamic Privacy Rules

Test Data Privacy uses unique technology to associate masking with sensitive test data elements such as card numbers, account numbers and names independent of objects (file/table) or platforms. A privacy rule is defined **once** for each data element. At disguise execution time, the appropriate disguise rules are dynamically applied to the file or database being disguised. The very same disguise rule is applied to each instance of the data element. That test data could be in a VSAM file, a Db2 table, an IMS segment or a distributed DBMS (Oracle, SQL/Server, Db2 LUW, Sybase).

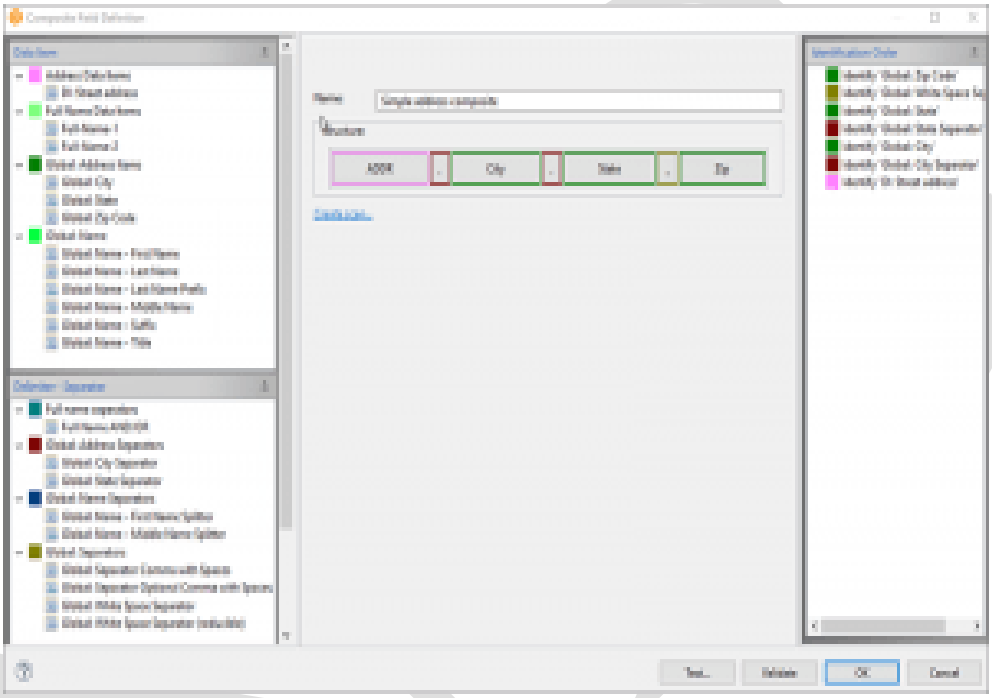


## Composite Processing

One of the unique features of Test Data Privacy is its ability to enable you to locate and disguise pieces of data within a larger field. This functionality is often used to disguise names and addresses, since there are many different formats in which that data is stored. Sometimes each part of the name is stored in a separate field, and sometimes the name is stored as a full name.

Composite processing allows you to locate the parts within the full name field so both formats can be disguised in the same way.



## Maintain Integrity with Data Selection and Sub-setting

Properties for Enterprise Data's data selection and sub-setting capabilities allow focused and relevant test data to be extracted while maintaining integrity, ensuring high-quality test data. Test Data Privacy includes capabilities for desensitizing copies of primary data containing PII, which can then be used for testing, QA or transmission to other business partners.

# Dynamic Data Protection key is the most effective way to protect data from cyber-attacks [Claims Forcepoint]

The new Dynamic Data Protection (DDP) solution harnesses the power of human centric behaviour analytics and is the most effective data protection method against advanced cyber threats, global cybersecurity firm Forcepoint. Forcepoint announced DDP, the industry's first risk-adaptive protection solution, in response to the challenges enterprise and government chief information security officers (CISO) face today in balancing users and data security with business productivity.

DDP surpasses legacy data loss prevention (DLP) offerings to uniquely deliver next-generation data protection that enforces security policies across enterprise endpoints or devices, without requiring administrator intervention.

"Legacy data protection based on point solutions is dead. A converged approach is the only path forward," the Forcepoint CEO said.
According to the company, cyber security solutions today rely on traditional threat blocking and static assessments that not only introduce security friction into business transactions but also overwhelm security analysts with millions of alerts from threats.
Forcepoint's risk-adaptive protection solution has capability to enable through the power of human-centric behaviour analytics that understand interactions with data across users, machines and accounts.

With human-centric behaviour analytics at its core, the Forcepoint DDP applies an anonymous and continuously updated behavioural risk score to establish a baseline of "normal" behaviour of each end-user on corporate or unmanaged networks.

# Informatica Delivers Industry's First Dynamic Data Masking Solution

## Provides Non-Invasive, Real-Time Protection Against Data Security Breaches

The author, Joseph Feiman, research vice president and Gartner Fellow said, "DDM is an emerging market. Among its first adopters are financial organizations concerned with their client services personnel's access to sensitive data in production databases. Adoption is driven by these enterprises' realization that other technologies — such as IAM (Identity Access Management), SDM (Static Data Masking) and data encryption — cannot solve the problem."

Informatica Dynamic Data Masking uses real-time data protection rules to provide finer grained control over the data that authorized users are allowed to see. These end-users, contract personnel, support teams, database administrators or developers can be given full access to production data, while ensuring access to Personally Identifiable Information (PII) and other sensitive data can be completely, or partially de-identified. This decreases the risk of data breach and ensures compliance with increasingly stringent data privacy regulations (PCI DSS, HIPAA, the HITECH Act, GLBA), without impacting user productivity, the underlying data, database structure, or query performance.

Informatica Dynamic Data Masking's sophisticated, yet flexible protection rules greatly enhance the standard access controls provided through standard database security. By enabling different masking algorithms to be applied dynamically to different sensitive data elements based on user privilege levels, customers have much more control over how information gets exposed to end users. Used in conjunction with data encryption to secure data at rest and with database activity monitoring to log and analyse utilization, dynamic data masking provides the perfect complement to ensure end-to-end security for production databases and applications.

**Informatica Dynamic Data Masking** empowers organizations to cost-effectively address current and future data privacy regulations through its comprehensive mix of real-time data anonymizing, blocking, auditing and alerting in a single environment. Customers benefit from the solution in the following ways:

- **Comprehensive, real-time data protection techniques** – Informatica Dynamic Data Masking employs a rich range of data masking techniques, including masking,

scrambling, hashing, randomizing, blocking and hiding, which preserve original data characteristics and maintain data integrity.

- **Rule-based access control (RBAC)** – Enforces user access privileges based on Active Directory grouping, LDAP, IAM, user roles and responsibilities when accessing personal and sensitive information across applications, reporting and development tools.
- **Non-intrusive to applications/databases** – Informatica Dynamic Data Masking requires no changes to application code or source databases.
- **Superior scalability and performance** – Informatica Dynamic Data Masking is proven to scale to support hundreds of databases and thousands of concurrent users in a single enterprise-wide environment.
- **Simple deployment** – Packaged CRM, ERP, billing and custom business critical applications can be protected in a manner of days, with real-time data protection rules extended to any sensitive data in any format. Numerous pre-built masking rules are provided with the solution, and new rules are quickly created and applied via a simple graphical interface.
- **Seamless integration with existing authentication software** – Informatica Dynamic Data Masking integrates seamlessly with Microsoft Active Directory, LDAP and IAM software to speed implementation and enhance data security by leveraging existing authorization and privilege models.

"Preventing data leakage and the need to comply with an ever increasing list of privacy regulations are of paramount importance to us in the telecommunications industry," said Alon Ofek, CISO, Pelephone Communications. "We needed a solution that could quickly and transparently mask sensitive fields within our application screens and across our development tools with no changes to applications, databases, or tools themselves. Informatica Dynamic Data Masking enables us to proactively protect our data in real-time."

Informatica Dynamic Data Masking is based on technology developed by ActiveBase, a pioneer in Dynamic Data Masking. ActiveBase was acquired by Informatica in July 2011. Gartner recognized ActiveBase as a "Cool Vendor" in 2010 for Application Security.

# Infosys Enterprise Data Privacy Suite (iEDPS)

## Securing and Sharing Business Data – Compromise no more!

Today, extended enterprises operate across multiple geographies where companies share high volumes of data within and beyond organizational boundaries. Such data sharing is needed for business application development, testing, training, statistical analysis, business process outsourcing, and market research. However, it also exposes organizations to several dangers. These include theft of sensitive client data resulting in penalties, lawsuits, loss of customer confidence, negative brand image, and erosion in share price. Ultimately, these risks mean higher costs and revenue loss.


Global regulatory norms such as HIPAA, PIPEDA, PCI DSS, GLBA, ITAR, SOX, and JSOX make it imperative for enterprises to protect confidential, sensitive, private, and personally identifiable information. Constrained by these regulations and concerned about data security risks, many companies are struggling to find secure ways for profitable outsourcing/off-shoring.

## Infosys Enterprise Data Privacy Suite secures your data and your business

Enterprises require a strategy where they can protect confidential client data while sharing it with internal/external entities for business purposes. Such a strategy involves using holistic data masking tools that 'de-identify' sensitive data and replace it with realistic but false data. In doing so, data stays secure and is still usable by application development, business intelligence and BPO teams.

Infosys Enterprise Data Privacy Suite (iEDPS) is an easy-to-use, high performance, scalable, and cost-effective data privacy and protection solution that automates the data masking

process of an enterprise in a centralized manner. iEDPS protects confidential, sensitive, private, and personally identifiable information within enterprise repositories. Loaded with deterministic, selective, dynamic, and static masking tools, iEDPS can be deployed on any platform, and supports all major databases and file systems.

**The key features of iEDPS are:**

- Sensitive data discovery
- Discovery dashboards
- Static and dynamic data masking
- Synthetic data generation
- Big data masking
- Data sub-setting

## Benefits of iEDPS

Besides data security, iEDPS provides additional benefits such as:

- Lower cost of implementation, operations and off-shoring
- Masking of any data store from VSAM to NoSQL
- Improved time-to-market
- Ability to scale effectively to mask millions of records with excellent performance
- Improved test data quality and data governance
- Assured data privacy and data compliance as per regional laws

## Case studies

## Use cases for iEDPS

**Data protection and off-shoring:** Businesses are responsible for the security and control of any personal data within their possession. However, most businesses overlook the importance of data protection from a legal and risk management standpoint when devising their outsourcing strategy. This raises serious data breach concerns during offshoring. By anonymizing data, iEDPS eliminates data sensitivity, thereby mitigating the risk of data leaks.

**Compliance with data privacy regulations:** Today, industries and corporations are obliged to comply with various data privacy regulations that could be sectoral or regional in nature. iEDPS can be configured to comply with multiple regulations simultaneously.

**Evaluate readiness for Personal Data Protection:** Faced with the deadline of October 2018 to implement Personal Data Protection, businesses within the EU that capture and process customer data need to place the necessary controls on sensitive data within their data stores. iEDPS can help these organizations identify where sensitive data resides in the organization while providing an assessment of their readiness for Personal Data Protection.

# National Scholarship Portal 2.0

# Data Protection Compliance Report

## (A) Registration Details *(Refer Annexure-2)*

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | State of Domicile | Processing and Storing personal data | Use personal data only for the specified purpose and in a lawful, fair and unbiased manner | Mask, Encrypt and anonymise all the PII |
| 2. | Name of Student | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 3. | DOB | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 4. | Mobile no. | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 5. | Gender | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 6. | Identification Detail | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 7. | Scholarship Type | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk |

| | | | | |
|---|---|---|---|---|
| | | | | factor associated with all the PII |
| 8. | Bank IFSC Code | User Content | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 9. | Scheme Type | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 10. | Bank Name | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 11. | Bank A/C No. | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 12. | Bank Passbook Copy(pdf) | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 13. | Aadhar Enrolment ID | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 14. | Date and Time | Useful in Data Protection | Helpful in data protection activities | Helpful in impact assessment |

| | | | | |
|---|---|---|---|---|
| 15. | EID Scan Copy | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 16. | Single Girl Child | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 17. | Religion | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 18. | Aadhar Number | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 19. | Community/Category | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 20. | Father Name | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 21. | Mother Name | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 22. | Annual Family Income | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 23. | Day Scholar/Hosteller | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 24. | Email ID (mandatory for post-matric) | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |

## AFTER SUCCESFULL FRESH APPLICATION LOGIN

- Upon successful registration, applicant is forced to change password if login is done for the first time. As the applicant logins an OTP is sent to his/her registered mobile number. After verifying the OTP, applicant is redirected to change Password page.
- Once the student changes the password, they will be directed to the Applicant's Dashboard page.

## (B) Academic Details

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | Select the Institute | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 2. | Present Class/Course | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 3. | Present year | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 4. | Mode of Study | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 5. | Present Class Start Date | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 6. | Previous University Board Name | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 7. | Previous Course | - | | |
| 8. | Previous Passing year | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |

| | | | | |
|---|---|---|---|---|
| 9. | Previous Class(%) | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 10. | University I,II Rank Holder | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 11. | $10^{th}$ Class Roll No. | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 12. | Board Name(10th) | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 13. | Year of Passing(10th) | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 14. | **$12^{th}$ Class Roll No.** | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 15. | **Board Name(12th)** | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 16. | **Year of Passing(12th)** | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 17. | **Competitive Exams Qualified** | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 18. | **Exam Conducted by** | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 19. | **Competitive Exam Roll No.** | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |

| | | | | |
|---|---|---|---|---|
| 20. | **Competitive Exam Year** | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 21. | Admission Fee | Maintain Records(Highly Encrypted) | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 22. | Tuition Fee | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 23. | Misc. Fee | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |

# (C) Basic Details

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | Is Orphan | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 2. | Guardian Name | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 3. | Is Disabled | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 4. | Type of Disability | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 5. | % of Disability | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 6. | Marital Status | User Consent | Collection and processing of all the personal data only after | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user- |

| | | | | |
|---|---|---|---|---|
| | | | appropriate user consent from the user | end and server-side while storage. |
| 7. | Parents Profession | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 8. | IFSC Code | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 9. | Bank Account Number | Maintain Records(Highly Encrypted) | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |

## (D) Contact Details

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | State | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 2. | District | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 3. | **Block/Taluk** | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 4. | House No./Street No. etc | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 5. | Pin code | User Consent | Collection and processing of all the | Appropriate Data Minimisation strategies |

| | | | | |
|---|---|---|---|---|
| | | | personal data only after appropriate user consent from the user | with proper PII owner's consent, both on user-end and server-side while storage. |

## (E) Scheme Details

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | Select the Scheme to Apply | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |

## (F) Upload Documents

| S.No. | PII(Personal Identifiable Information) | Requirement | Solution | Remarks |
|---|---|---|---|---|
| 1. | Scanned Copy of passbook | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 2. | Domicile Certificate | User Consent | Collection and processing of all the personal data only after appropriate user consent from the user | Appropriate Data Minimisation strategies with proper PII owner's consent, both on user-end and server-side while storage. |
| 3. | Scanned Copy of Mark sheet of last exam passed | Records of Processing | All the processing records are useful for further analysis | Easily able to analyse the impact assessment report |
| 4. | Income Certificate | Maintain Records(Highly Encrypted | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |
| 5. | Student Photograph | Maintain Records(Highly Encrypted | Ensure data protection by design (highly encrypted algorithm) to prevent from data breach | VAPT(Vulnerability Assessment and Penetration Testing) on client-side as well as server-side helps in determining the risk factor associated with all the PII |

# Masking, Encryption and Anonymization Analysis

| S.NO. | Details(PII) | Masking | Encryption | Anonymization |
|---|---|---|---|---|
| 1. | Registration Details | Persistent | AES(Advanced Encryption Standard) / 3DES(Triple Data Encryption Standard) | Proper and Specific Data minimisation and Storage |
| 2. | Academic Details | Dynamic | Not compromise with RSA,better with 3DES | Editable at run time with minimum data loss |
| 3. | Basic Details | Dynamic | AES(Advanced Encryption Standard) / 3DES(Triple Data Encryption Standard) | Useful in maintaining the records of all encrypted modules in a secured, portable and dynamic fashion to analyse impact factor |

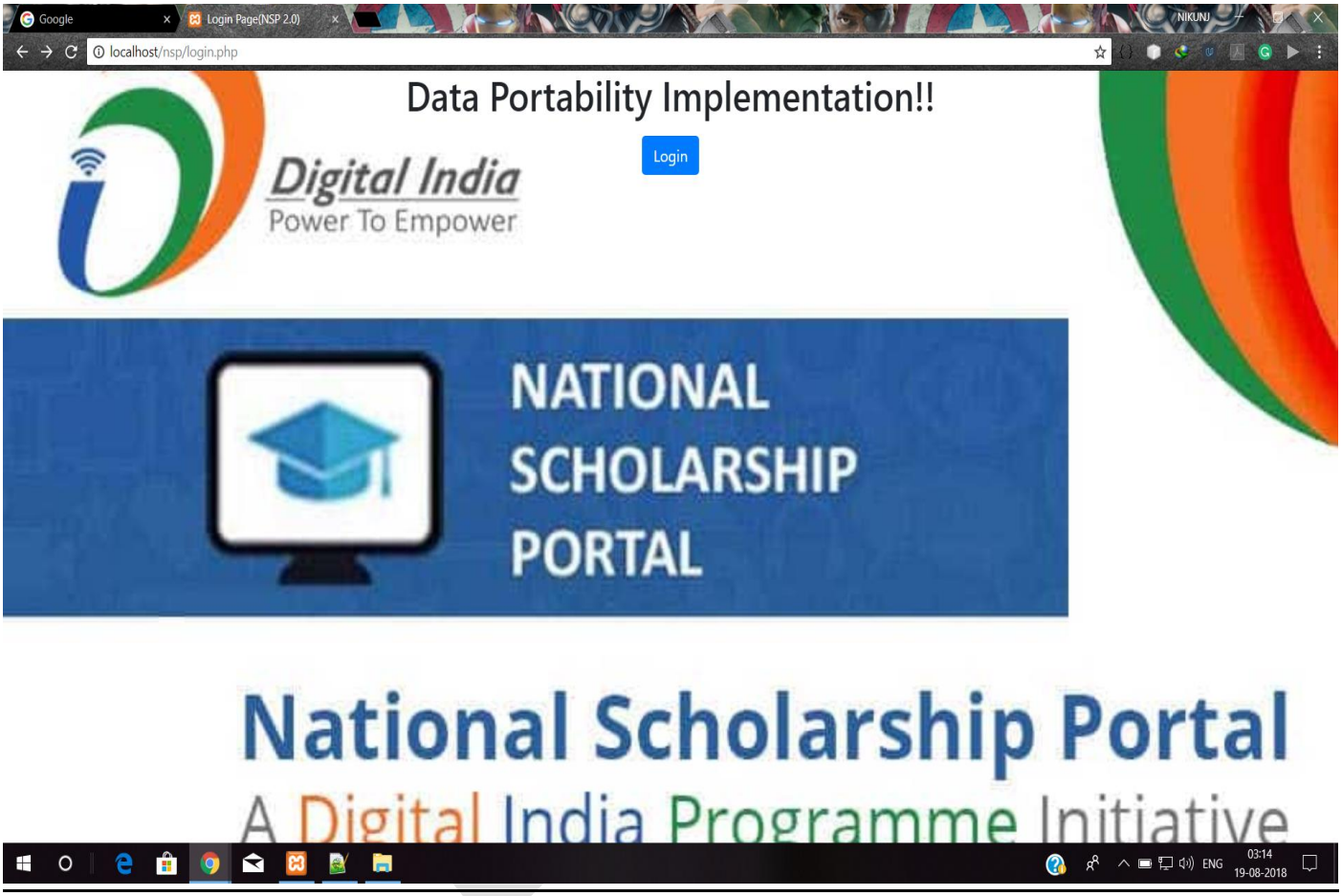
## High Important Points for NSP 2.0 -

- Maintaining the PFMS secure payment gateway.
- Monitoring the regular progress with the Institute (Tracking the work).
- Checking the account Details and other documents uploaded, carefully and systematically.
- Use of strongest encryption algorithm for securing the PII of the applicant.
- Proper/Un-biased merit list, to be monitored by the NSP.
- Report the Data Breach as soon as possible.
- Maintain all the processing and storing records of applicant securely.
- User Consent always required at each step of functioning.

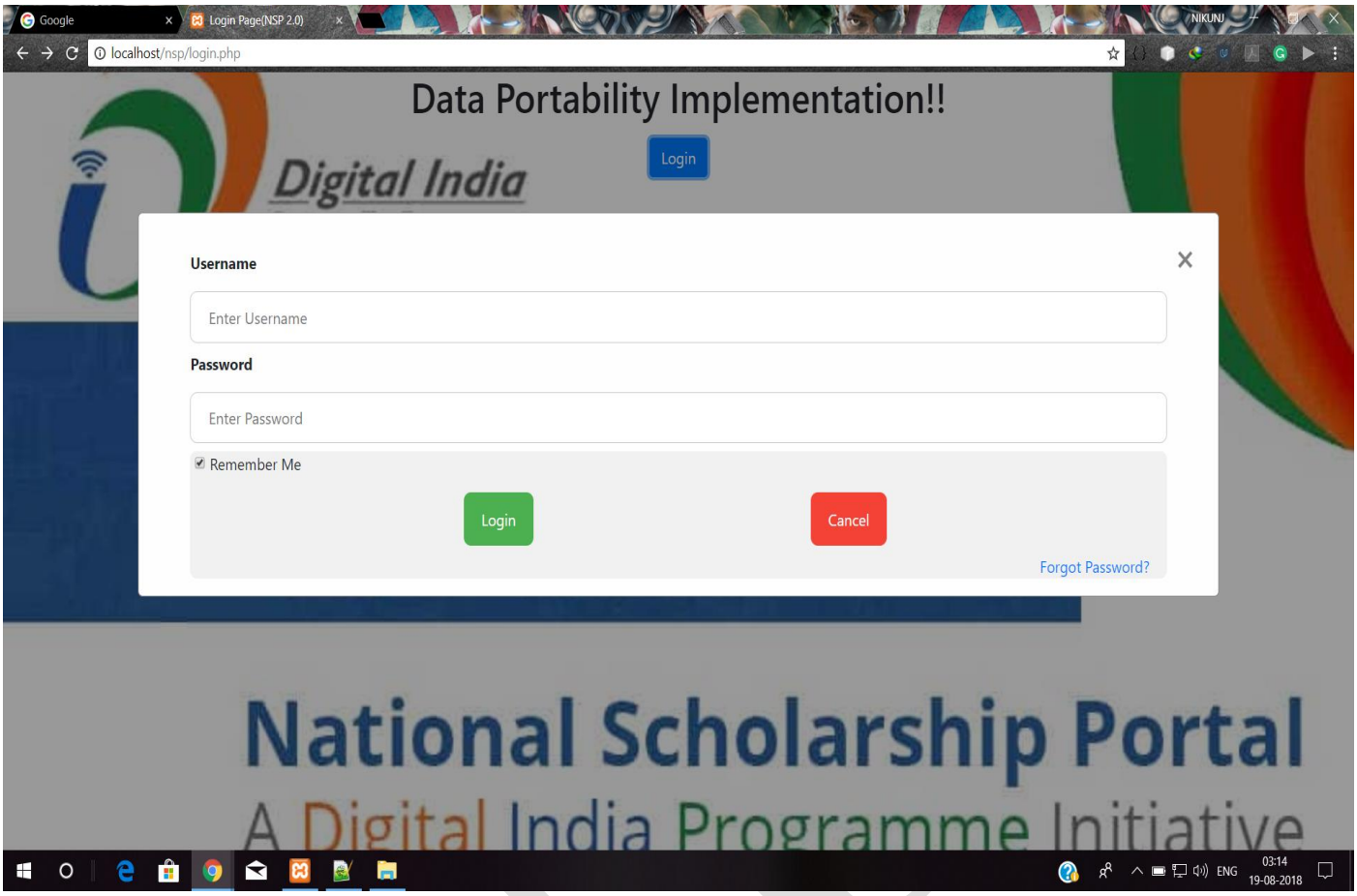
# National Scholarship Portal 2.0

# Implementation of Data Portability

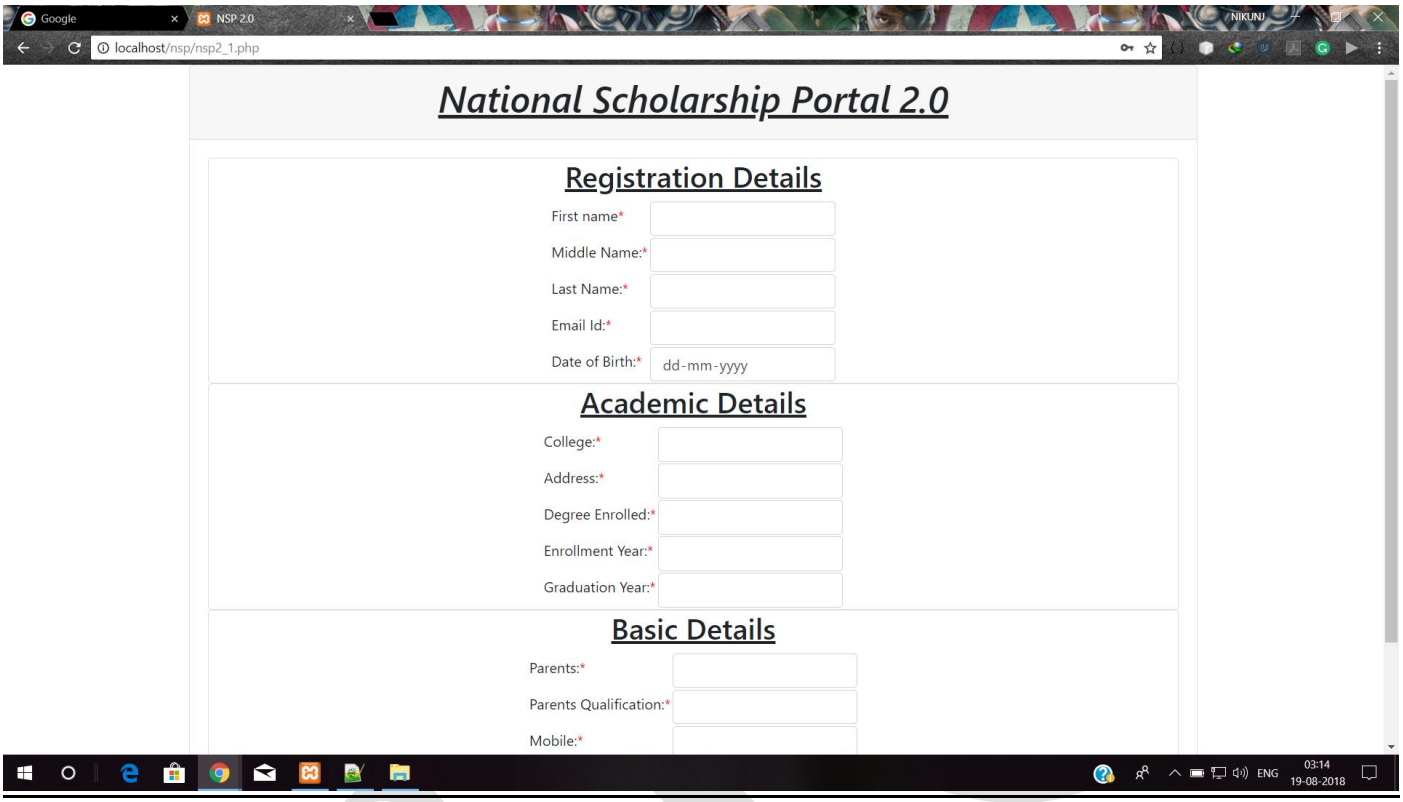
Login.php

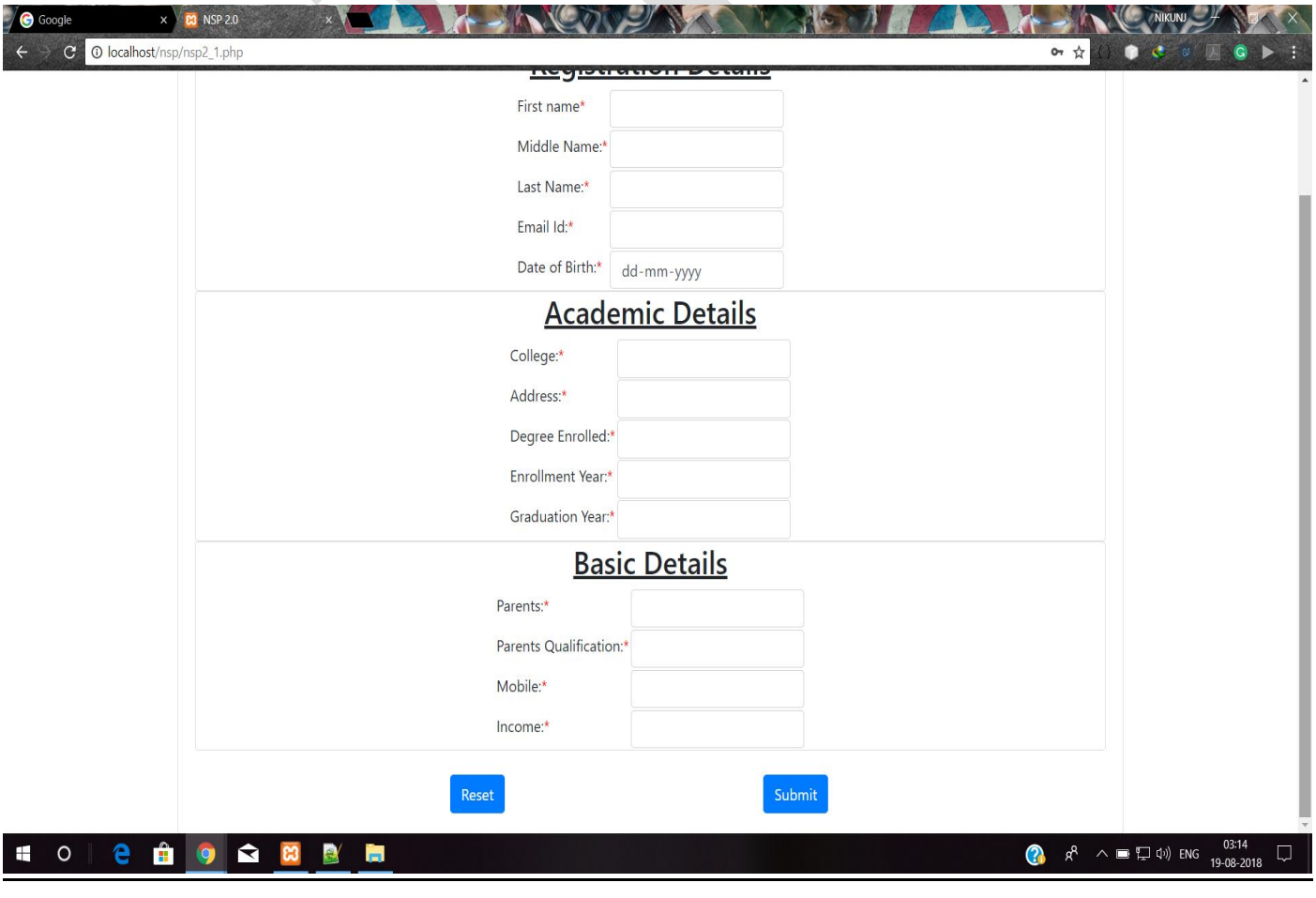


# Login UI for Registration



# Details of NSP 2.0 (to be filled)



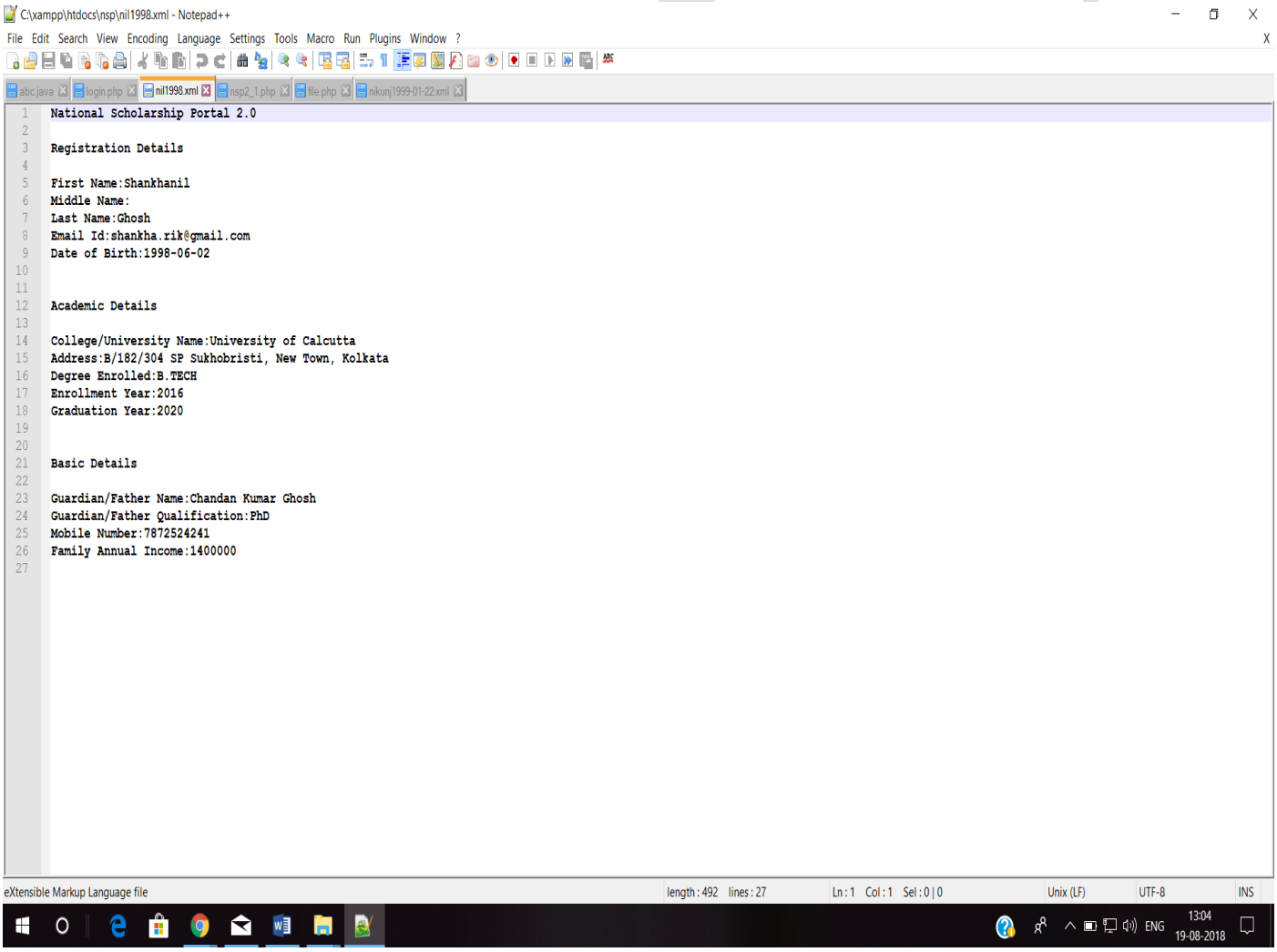



# NOTE-

1)When the form is submitted, it generates an.xml file in the root folder of all the files.

2)This will help in maintaining the data portability issue to a long cause, thus pertaining to the needs and expectations of most of the organisations.

3)The .xml file will be saved with student_name_dob.xml format in root folder.



# Annexure

## (1.1) GDPR-

One most effective way for its implementation is the concept of **General Data Protection Regulation** (**GDPR**) (EU) 2016/679.**GDPR** is a regulation in EU law on data privacy and protection for all the individuals within the European Union (EU) and the European Economic Area (EEA). It also takes into account the export of personal data outside the EEA and EU areas. The GDPR motive is to give control to citizens and residents over their personal data and to simplify the regulatory environment.

GDPR basically deals with following Chapters and Articles as defined below-

**Chapter 1 (Article 1-4)**

--General provisions

**Chapter 2 (Article 5-11)**

--principles

**Chapter 3 (Article 12-23)**

--Rights of the Data Subject

**Chapter 4 (Article 24-43)**

--Controller and processor

**Chapter 5 (Article 44-50)**

-- Transfers of personal data to third countries or international organizations

**Chapter 6 (Article 51-59)**

--Independent Supervisory authorities

**Chapter 7 (Article 60-76)**

--Cooperation and Consistency

**Chapter 8 (Article 77-84)**

--Remedies, liabilities and penalties

**Chapter 9 (Article 85-91)**

--Provisions relating to specific processing situations

**Chapter 10 (Article 92-93)**

--Delegated acts and implemented acts

**Chapter 11 (Article 94-99)**

--Final Provisions

## Liabilities and Fines-

- Liability to controllers, processors & their representatives
- Shared liability to joint controllers
- For violations of obligations of controllers & processors and certifications :
  **€10 million or 2% of last year global turnover**
- For violations of principles, rights, transfers &for noncompliance with other sanctions:
  **€20 million or 4% of last year global turnover**

## (1.2) A Systematic Approach to Ensuring Personal Data Protection Compliance: Key Action Items for Telecom Operators (in reference to Tata Consultancy Services)

| Reference to the GDPR Act | Requirement | Solution | |
|---|---|---|---|
| ***Article 5*** | **Processing and Storing Personal Data** | Use personal data only for the purpose and time specified by the user, and process it lawfully, fairly, and in a transparent manner | Mask, encrypt, and anonymize all PII, depending on their exact usage and storage state |
| ***Articles 6, 7 and 8*** | **User consent** | Collect and process all personal data only after obtaining explicit consent from the user | Redesign processes linked to VAS and other data monetization strategies, in line with the user consent mandate |
| ***Article 12 to 22*** | **Rights of the data subject** | Honor the rights of the data subject with respect to right to access, rectification, right to be forgotten (data erasure), restriction of processing, notification obligation, data portability, and right to object including automated decision making (user profiling) | Implement a robust data lifecycle management framework involving data minimization and data access management, with built-in functionalities for easy data modification, portability and erasure |
| ***Articles 25 and 32*** | **Data protection by design** | Ensure data protection by design, and by default; carry out data protection impact assessments regularly | Leverage solutions such as data encryption, masking, and pseudonymization<br>To shield subscriber data from internal threats, implement effective mobile device management (MDM) mechanisms for streamlining access for remote, off-site employees<br>Promote role-based access to IT and data assets through enforcement of advanced identity and access management (IAM) protocols |

| Reference to the GDPR Act | Requirement | Solution | |
|---|---|---|---|
| ***Articles 25 and 32*** | **Data protection by design** | Ensure data protection by design, and by default; carry out data protection impact assessments regularly | Conduct a vulnerability assessment and penetration testing (VAPT) for all applications, and chalk out a business continuity plan (BCP) for each one |
| ***Articles 30*** | **Records of processing** | Maintain a record of all processing activities, covering specifically mentioned information on the processing | Prepare records of processing as a part of the GDPR assessment report |
| ***Articles 33 and 34*** | **Data breach** | Report data breaches within 72 hours | Build effective breach detection and notification mechanisms across internal systems |
| ***Article 35*** | **Impact assessments** | Conduct data protection impact assessments to identify risks to users, and also detail how such risks will be mitigated | Roll out an extensive compliance audit program for robust risk management |
| ***Articles 37, 38 and 39*** | **Data protection officers (DPO)** | Appoint a DPO to oversee the data security strategy and GDPR compliance | Appoint a DPO, and fix accountability or effective data governance |

## (1.3) Data Protection for maintaining Personal Data Protection Compliance

| ARTICLE | WHAT IT MEANS | REQUIREMENTS FOR DATA SECURITY | IMPERVA SOLUTION |
|---|---|---|---|
| **25:** Data protection by design and by default | Implement technical and organizational measures to show consideration and implementation of Data Protection Principles and appropriate safeguards | • Data minimization<br>• User access limits<br>• Limit period of storage and accessibility | Camouflage<br>SecureSphere |
| **32:** Security of processing | Implement appropriate technical and organizational security controls to protect personal data against accidental or unlawful loss, destruction, alteration, access or disclosure | • Pseudonymization and encryption<br>• Ongoing protection<br>• Regular testing and verification | Camouflage<br>SecureSphere<br>CounterBreach |
| **33 and 34:** Data breach notification | 72 hour notification to Data Protection Authority following discovery of data breach, and notification to affected individuals | Breach report that includes:<br>• what happened<br>• numbers of affected individual<br>• what data was breached | SecureSphere<br>CounterBreach |
| **35:** Data protection impact assessment | Assessment of the purpose, scope and risk associated with processing personal data | Inventory of personal data across organization, access rights to data, and risk associated with that access | SecureSphere |
| **44:** Data transfers to third country or international organization | Permit transfers only to entities in compliance with GDPR regulation | Monitor and block access to entities or regions that do not meet requirements | SecureSphere |

## (1.4) Comply with GDPR

And the penalties for non-compliance have some bite. According to the International Association of Privacy Professionals (IAPP), imposed Personal Data Protection sanctions can include:

- A written warning in cases of first and nonintentional noncompliance
- Regular periodic data protection audits
- A fine up to **10,000,000 EUR or up to 2% of the annual worldwide turnover** of the preceding financial year for enterprises, whichever is greater
- A fine up to **20,000,000 EUR or up to 4% of the annual worldwide turnover** of the preceding financial year for enterprises, whichever is greater

## (1.5) 3 ways technology can help businesses become Personal Data Protection compliant

# Annexure-2

# Personal Data Protection, Data Masking & Encryption usage

| Characteristics | Persistent Data Masking | Dynamic Data Masking | Encryption | Anonymization | Pseudonimisation |
|---|---|---|---|---|---|
| Protect Sensitive data at rest (in storage) **(A,D)** | | | | | |
| Protect Sensitive data when accessed **(B,C)** | | | | | |
| Protect data in transmission **(B,C,D)** | | | | | |
| Obfuscation based on user privileges/roles **(A,F,C,D)** | | | | | |
| Suited for protecting sensitive data in production **(A,D)** | | | | | |
| Suited for protecting sensitive data in non-prod **(B,C)** | | | | | |
| Impact on application performance **(B,C,E)** | | | | | |
| Does not require change in application to implement **(A,B,D)** | | | | | |
| Support indexing and optimised search **(A,B,F)** | | | | | |
| Format preserving **(F)** | | | | | |
| Repeatable-resulting obfuscated data is deterministic **(C,F)** | | | | | |
| Reversible-original data is retrievable **(B,C,F)** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Original data is not stored anywhere **(A,C)** | | | | | |
| Original data is still stored either in original location or central location (A,B,D) | | | | | |

# National Scholarship Portal 2.0

# Implementation of Data Portability!!

# Annexure-3

## Login.php

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">

    <title>Login Page(NSP 2.0)</title>
  </head>

  <style>
  body,html {
        /* The image used */
    background-image: url("https://www.sarkariresult.biz/wp-content/uploads/2017/08/nsp-3.jpg");

    /* Full height */


    /* Center and scale the image nicely */
    background-position: center;
```

```
    background-repeat: no-repeat;
    background-size: cover;
    position: absolute;

        top:0px;
        left:0px;
        width: 100%;
        height: 100%;

        }


 .text{
        text-align: center;
        }

  .button{
        text-align: center;
        }


input[type=text], input[type=password] {
    width: 100%;
    padding: 12px 20px;
    margin: 8px 0;
    display: inline-block;
    border: 1px solid #ccc;
        border-radius: 8px;
    box-sizing: border-box;
}
```

```
/* Set a style for all buttons */
 button {
    background-color: #4CAF50;
    color: white;
    padding: 14px 20px;
    margin: 8px 0;
    border: none;
    cursor: pointer;
    width: auto;
          border-radius: 8px;
}

button:hover {
    opacity: 0.8;
}

.cancelbtn {
    margin-left: 10px;
    background-color: #f44336;
}

.imgcontainer {
    text-align: center;
    margin: 24px 0 12px 0;
    position: relative;
}


span.psw {
    float: right;
    padding-top: 16px;
}
```

```
.modal {
    display: none; /* Hidden by default */
    position: fixed; /* Stay in place */
    z-index: 1; /* Sit on top */
    left: 0;
    top: 0;
    width: 100%; /* Full width */
    height: 100%; /* Full height */
    overflow: auto; /* Enable scroll if needed */
    background-color: rgb(0,0,0); /* Fallback color */
    background-color: rgba(0,0,0,0.4); /* Black w/ opacity */
    padding-top: 60px;
}

.modal-content {
    background-color: #fefefe;
    margin: 5% auto 15% auto; /* 5% from the top, 15% from the bottom and centered */
    border: 1px solid #888;
    width: 80%; /* Could be more or less, depending on screen size */
}

.close {
    position: absolute;
    right: 25px;
    top: 0;
    color: #000;
    font-size: 35px;
    font-weight: bold;
}

.close:hover,
```

```
.close:focus {
   color: red;
   cursor: pointer;
}

.animate {
   -webkit-animation: animatezoom 0.6s;
   animation: animatezoom 0.6s
}

@-webkit-keyframes animatezoom {
   from {-webkit-transform: scale(0)}
   to {-webkit-transform: scale(1)}
}

@keyframes animatezoom {
   from {transform: scale(0)}
   to {transform: scale(1)}
}

@media screen and (max-width: 300px) {
   span.psw {
      display: block;
      float: none;
   }
   .cancelbtn {
      width: 100%;
   }
}

.containers{
        background-color:#f1f1f1;
```

```
        margin-bottom: 5px;
        border-radius: 8px;
}

.containers button {
        margin-left: 28%;
}

  </style>
  <body>
    <div class="container">
<div>
<h1 class="text">Data Portability Implementation!!</h1>
</div>
<div class="button" >
<button class="btn btn-primary" onclick="document.getElementById('id01').style.display='block'"
>Login</button>
</div>
<div id="id01" class="modal">

  <form class="modal-content animate" action="nsp2_1.php" method="POST">
    <div class="imgcontainer">
      <span onclick="document.getElementById('id01').style.display='none'" class="close" title="Close
Modal">&times;</span>
    </div>

    <div class="container">
      <label for="uname"><b>Username</b></label>
      <input type="text" placeholder="Enter Username" name="uname" required>

      <label for="psw"><b>Password</b></label>
      <input type="password" placeholder="Enter Password" name="psw" required>
```

```
   <div class="containers">
          <div style="margin-left: 5px">
         <label>
       <input type="checkbox" checked="unchecked" name="remember"> Remember Me
     </label>
           </div>
         <div><button href="nsp2_1.php" type="submit" >Login</button>
    <button type="button" onclick="document.getElementById('id01').style.display='none'" class="cancelbtn">Cancel</button>
          </div>
          <div>
              <p class="psw" style="margin-left:87%"> <a href="#">Forgot Password?</a></p>

          </div>

   </div>
          </div>

  </form>
</div>

</div>

   <!-- Optional JavaScript -->
   <!-- jQuery first, then Popper.js, then Bootstrap JS -->
   <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>
   <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
```

```
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js" integrity="sha384-JZR6Spejh4U02d8jOt6vLEHfe/JQGiRRSQQxSfFWpi1MquVdAyjUar5+76PVCmYl" crossorigin="anonymous"></script>


<script>
// Get the modal
var modal = document.getElementById('id01');

// When the user clicks anywhere outside of the modal, close it
window.onclick = function(event) {
    if (event.target == modal) {
        modal.style.display = "none";
    }
}
</script>

  </body>
</html>
```

## nsp2_1.php

```
<!DOCTYPE html>
<html>
<head>

  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css">
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.3/umd/popper.min.js"></script>
  <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js"></script>

<title>NSP 2.0</title>
<style>
```

```
.btn {
	margin-left: 28%;
}


.error {color: #FF0000;}
</style>
</head>
<body bgcolor="#00FFFF">


<div class="container">

<div class="card">
<div class="card-header">
<H1><center><U><I>National Scholarship Portal 2.0</I></U></center></H1>
</div>
<div class="card-body">


<form name="form" action="file.php" method="POST">
<div class="card">
<H2><center><U>Registration Details</U></center></H2>

<table align="center">
<tr>
	<td><label for="exampleInputEmail1">First name</label><span class="error">*</span>
	<td><input type="text" name="fname" class="form-control" ></td>
</tr>
<tr>
	<td><label for="exampleInputEmail1">Middle Name:</label><span class="error">*</span>
```

```
        <td><input type="text" name="mname" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Last Name:</label><span class="error">*</span>
        <td><input type="text" name="lname" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Email Id:</label><span class="error">*</span>
        <td><input type="email" name="email" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Date of Birth:</label><span class="error">*</span>
        <td><input type="Date" name="dob" class="form-control" ></td>
</tr>

</table>
</div>
<div class="card">
<H2><center><U>Academic Details</U></center></H2>
<table align="center">



<tr>
        <td><label for="exampleInputEmail1">College:</label><span class="error">*</span>
        <td><input type="text" name="clg" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Address:</label><span class="error">*</span>
        <td><input type="optional" name="clgadd" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Degree Enrolled:</label><span class="error">*</span>
```

```
        <td><input type="text" name="degree" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Enrollment Year:</label><span class="error">*</span>
        <td><input type="Year" name="enr" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Graduation Year:</label><span class="error">*</span>
        <td><input type="Year" name="grad" class="form-control" ></td>
</tr>

</table align="center">
</div>
<div class="card">
<H2><center><U>Basic Details</U></center></H2>
<table align="center">



<tr>
        <td><label for="exampleInputEmail1">Parents:</label><span class="error">*</span>
        <td><input type="text" name="g_f_name" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Parents Qualification:</label><span class="error">*</span>
        <td><input type="optional" name="g_f_qual" class="form-control" ></td>
</tr>
<tr>
        <td><label for="exampleInputEmail1">Mobile:</label><span class="error">*</span>
        <td><input type="Number(10)" name="mobile" class="form-control" ></td>
</tr>
<tr>
```

```
        <td><label for="exampleInputEmail1">Income:</label><span class="error">*</span>
        <td><input type="text" name="inc" class="form-control" ></td>
</tr>
</table>
</div>
<br>
<div>
<button class="btn btn-primary" type="reset" name="Reset">Reset</button>
<button class="btn btn-primary"  name="submit" type="submit" value="Submit" bg-color:
"#008CBA";>Submit</button>
</form>
</div>



</div>

 </div>
 </div>




</body>
</html>
```

## file.php

```
<?php
error_reporting(0);
$myfile = fopen($_POST["fname"].$_POST["dob"].".xml", "w") or die("Unable to open file!");
fwrite($myfile, "National Scholarship Portal 2.0\n\n");
fwrite($myfile, "Registration Details\n\n");
fwrite($myfile, "First Name:".$_POST["fname"]."\n");
fwrite($myfile, "Middle Name:".$_POST["mname"]."\n");
fwrite($myfile, "Last Name:".$_POST["lname"]."\n");
```

```
fwrite($myfile, "Email Id:".$_POST["email"]."\n");
fwrite($myfile, "Date of Birth:".$_POST["dob"]."\n\n\n");
fwrite($myfile, "Academic Details\n\n");
fwrite($myfile, "College/University Name:".$_POST["clg"]."\n");
fwrite($myfile, "Address:".$_POST["clgadd"]."\n");
fwrite($myfile, "Degree Enrolled:".$_POST["degree"]."\n");
fwrite($myfile, "Enrollment Year:".$_POST["enr"]."\n");
fwrite($myfile, "Graduation Year:".$_POST["grad"]."\n\n\n");
fwrite($myfile, "Basic Details\n\n");
fwrite($myfile, "Guardian/Father Name:".$_POST["g_f_name"]."\n");
fwrite($myfile, "Guardian/Father Qualification:".$_POST["g_f_qual"]."\n");
fwrite($myfile, "Mobile Number:".$_POST["mobile"]."\n");
fwrite($myfile, "Family Annual Income:".$_POST["inc"]."\n");

fclose($myfile);
echo $_POST["fname"].$_POST["dob"].".xml file created successfully in the root folder";
?>
```