# Data Privacy and Protection policy

## Objective

Dependence on Data/Information is high in the present digitized and networked environment. At Ojas Innovative Technologies Pvt Ltd (Herein after it will be referred as "Ojas") this increases the risk of information being copied or stolen or modified hidden, encrypted misused or destroyed. Although defined controls provide an essential element of protection, these only deliver a percentage of the required protection the most of effective defense being achieved through awareness and good working practices.

This Policy document forms Ojas Data Privacy and Protection Policy in support of the information security policy. Compliance with this Policy will minimize the risk to information that being compiled, used, transported, proceed or held within/outside Ojas premises and aligns with the Indian IT Act, 2000, the EU DATA Privacy Protection Directive, 1995, the UK's Data Protection 1998, the USA's Safe Harbor Principles and other related privacy principles and the best practices.

The purpose of this Policy is to define requirements to safeguard personal data, which includes, personal information (PI) and sensitive personal information (SPI), as defined below, related to Ojas or its clients that are accessed OR contained on any system, portable devise and portable electronic storage media On or off Ojas Premises and the procedures to be followed. This policy also explains how the most important PI and SPI which identifies Ojas Staff (also referred to as Associates in this Policy) will be used and proceed by and on behalf of the Ojas group.

IN addition, the aim is to ensure that associates handling the PI or SPI are fully aware of the Data Privacy and Protection requirements and handle it in accordance with the Data protection procedures.

This Policy must be read in conjunction with all other relevant information security policies, data security policies and HR policies as necessary. For the evidence of doubt, nothing in this policy shall supersede the provisions regarding data protection and privacy contained in the Data provided by the respective client or any related documents signed for such protection of data but not limited to:

- In any data protection policy provided by the Client to Ojas
- Any data breach policy provided by the Client to Ojas
- In the agreement between the Client and Ojas

## 2. SCOPE

This Policy covers PI or SPI held in (Electronic and Paper form) including that held in Associated IT Infrastructure such Software's, Networks, Desktops, Tapes (eg: Audio, and CC TV) and Servers that all Ojas facilities.

## 3. Applicability

This Policy applies to all business units and associates of Ojas who create, store or access PI and/or SPI. This policy defines the minimum requirements for Data Privacy and Protection which need to be compiled by Ojas and its associates. Clients may adopt more stringent requirements depending on them in-country specify regulations and compliance on data privacy and protection. Whilst it is recognized that compliances with all aspects of the Policy can't be policed. Those to whom it applies will be held accountable and responsible for any aspects of non-compliances involving them that subsequently come to light under the enforcement clause of this policy.

**4. Definitions:**

**A.** Business Requirements: Requirements that can be traced back to the planning and execution of Ojas vision, mission, business goals and objectives, and its compliance to all relevant laws regulations, procedures and policies.

**B.** Personal Data or Personal Information (PI) (Also known as personally identifiable information): Any information that when used alone or combined with other data, may be used to identify living individual this includes, but not limited to

- First Name
- Middle Name
- Last Name / Surname
- Email address
- Address
- Telephone Number
- Title
- Birth date
- Gender
- Age
- Occupation
- Biometric Info
- Health Info
- Credit Card or Bank Information
- Biographical information (where it is combined with information that identifies someone)
- Individual Tax Info

**C.** Sensitive Personal Information (SPI) – means any personal information like

- Password (not even if applicable law may not categorize passwords as sensitive Ojas does and you should treat them accordingly)
- National Insurance Number
- Social Security Numbers / Any country unique SSN
- Race
- Ethnic Origin
- Sexual Orientation
- Political Opinions
- Religious or Philosophical beliefs
- Trade Union Memberships that contain individual's health related records (example: Patient records, medical photographs, diet information, hospital information records, biological traits and genetic materials)
- Criminal Records
- Legal investigations and Proceedings etc.

**D.** Processing – is obtaining, using holding amending, disclosing, destroying, deleting, transferring and any other activity with personal data. This includes some paper personal data as well as that kept on computers.

**E.** Data Subject – is an individual who is the subject of personal data.

**F.** Data Controller – the legal entities alone with or others, control the purpose and way the personal data are used, for example, Ojas in its role as Provider of employment and other related services/benefits to the employees.

**G.** Data Processor – is someone who provides services to its clients and processes personal data on behalf of data controller. (For Example: Ojas in its role as a Service Provider to its clients)

**H.** Portable Devises – Electronic computing and communication devices designed for mobility, including laptop, desktop, tablets, smartphones, in vehicle personal computers, personal data/digital assistants (PDAs), Cellular Phones, and other devises that have the ability to store data electronically.

**I.** Portable Electronic Storage Media (Portable Storage) – includes Floppy Disks, CDs, DVDs, Optical Platters, Flash Memory Drives, Back UP Tapes, USB HDDs, and other Electronic Storage media that provide portability or mobility of data.

**J.** Secured Storage Environment – Data Storage devises and support systems, such as direct attacked server storage and storage area network (SAN) Devises, managed by our OIM Team or IT Team are provided explicitly under contract, and/or secured by physical and logical means consistent with data storage best practices and Ojas information security policy recommendations ensuring – Confidentiality, Integrity and Availability (CIA).

## 5. High Level Policy

Personal/Sensitive personal data (PI or SPI) that is held or processed in any form including paper/electronic form within/outside Ojas premises, related to Ojas or its clients must be protected appropriately and always in line with Ojas and its clients Policies and procedures.

Such data must be collected and used fairly. Store safely and not disclose to any other person unlawfully in each cases in line with the provisions of Ojas policies and Client Senior Manager Directions. Physical access to and transmission and storage of PI or SPI shall be restricted to only those who require such access part of their day to day job function.

Ojas is committed to protect the PI or SPI of its associates as well as its customers. No matter where it is collected, transported, processed or retained within the scope of the applicable contractual as well regulatory requirements.

## 6. Detailed Policy

If you require more related policies, procedure information on how Ojas assure and ensure Data Privacy and Protection please write an email to: corporate@ojas-it.com

**Compliance:**

- Associates shall note and comply with the applicable data protection and privacy laws and take note of the relevant guidelines and industry quotes of practices and standards.
- Compliances shall be indicated by individual and organizational adherence to the requirements and procedures of the policy and data privacy and protection and directives of the Client.
- In addition, associates need to undergo regular training on Data Security and Privacy and be aware of the Security Procedures and Controls requirements as mentioned in the agreement and or regulatory requirements provided by the Client.
- The internal information security team to regularly audit and access the compliance to the security and privacy requirements and report it through online audit management tools.
- All the information security and privacy related incidents to be reported immediately through online Incident Management Portal. Such incidents will be further escalated depending on the type of the incidents and contacts for the relevant location as defined Ojas Incident Management Policy and procedure.

- With regard to breach of security and privacy policy the organization and individual may be liable for costs incurred as a result of loss, theft or unauthorized use of PI or SPI and remedy measures as relevant. The action will be taken based on HR Policy and Legal team's opinion regarding the issue.

- For business reasons, and in order carry out legal obligations in our role as an employer use of our IT and Telephone systems include devises which we allow our staff to access or use or monitor. Further Ojas reserves the right to retrieve the contents of the messages sent and searches made by and to inspect contents stored on company owned devises. Monitoring only carried out if any to the extent permitted or as required by law and as necessary and justifiable for business purpose. If evidence of misuse of Ojas and its groups IT system is founded, Ojas may undertake a more detailed investigation in accordance with its disciplinary policy. If necessary, the matter may be reported to Police Authority for criminal investigation. Investigation and disclosure of information to the relevant authorities shall be carried out in terms of the applicable laws.

- IN order to fulfill the data privacy laws and regulations, Ojas reserves the right to disclose and individual PI and SPI to law enforcement agencies, regulatory bodies, government bodies as required law or for statutory compliance.

| | |
|---|---|
| **Title of the document** | Ojas Data Privacy and Protection Policy |
| **Policy Owner** | Manager - IT |
| **Reviewed & Approved BY** | Mr. Arun Kumar Alampally - MD |