Data Privacy and Freedom of Expression

1. Happiest Minds has conducted detailed assessment of our internal processes to comply with Privacy regulation like GDPR. Data flow maps are developed and evaluated for each function/business process to identify the overall lifecycle of the collected data, privacy risk is assessed and mitigation measure and controls are deployed accordingly. Some of the key policies/practices implemented include:

1a. **Awareness (Article 39):** Annual information security awareness sessions

1b. **Review and Update Privacy Notices (Article 19):** The current privacy policy is updated as per the GDPR requirement. The same has been published in the Happiest Minds website.

1c. **Appoint or Hire a Data Protection Officer (Article 37):** In-house Full-time DPO has been appointed.

1d. **Evaluate Data Retention Procedures (Article 12):** Data retention policy is in place and timeline of data retention is mentioned by different process owners.

1e. **Conduct a Privacy Impact Assessment (PIA) or DPIA (Article 35):** DPIA was conducted when the GDPR was implemented identifying various PII data and its respective controls and owners. Annual audit is conducted to verify the DPIA.

1f. **Establish Contracts with Third-Party Processors (Article 28, 46):** Happiest Minds has modified the contracts to ensure that all third parties have adequate data protection measures and procedures in place. Annual privacy risk reviews are conducted for the identified critical vendors.

1g. **Implement Procedures for Prompt Mandatory Notification (Article 33, 34):** We have procedure in place to ensure that breaches are reported to regulators within 72 hours of the Company becoming aware of the breach. If notification occurs later than 72 hours after we become aware of a breach, eventual notice is accompanied by an explanation for the delay. DPO manages and oversees the activities.

Data Security and Privacy Policies

Information Security and Privacy Policies and Procedures: We have well-defined and implemented information security and data protection policies and procedures (as per ISO 27001 and ISO 27701 framework). Policies and practice related to Data Security includes:

1
Vendor Risk Management Policy

2
Information Security Policy

3
Access Control Policy

4
Clear Desk and Clear Screen Policy

5
Information Classification Policy

6
Policy on use of Encryption

7
Removal of Information Assets

8
Policy on Back-up and Restoration

Accounting Metrics for the Fiscal - 1

1	Total amount of monetary losses as a result of legal proceedings associated with user privacy	None
2	Number of law enforcement requests for user information, number of users whose information was requested, Percentage resulting in disclosure	None
3	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	None
4	The entity shall disclose the number of unique users whose information is used for secondary purposes	None

2. As part of our Information Security Management System, ongoing risk assessment is conducted (both internal and third parties) to assess the risk and mitigation/controls. We undergo annual ISO 27001 certification and SOC 2 Type 2 attestation by third parties. The following Data security controls are in place:

2a. Encryption - Both at end points and at Network level

2b. Strong Access Control - Including Multi-factor and Risk-based Authentication and access control

2c. Malware protection - At end point and network layers (to protect web and email traffic)

2d. Device control - Restriction on usage of USBs, Mobile devices

Accounting Metrics for the Fiscal - 2

1	Number of data breaches	None
2	Percentage involving personally identifiable information (PII)	0%
3	Number of users affected	None