### **Data Sharing and Protection Agreement**

**Between**: **Apex Financial Services Ltd.** ("Data Provider")  
**And**: **Cogniflow Analytics Pvt. Ltd.** ("Data Recipient")  
**Effective Date**: February 1, 2024  
**Duration**: 3 Years

### **1. Objective and Purpose**

This Data Sharing and Protection Agreement ("Agreement") outlines the terms and conditions under which Apex Financial Services Ltd. ("Provider") shall share select financial, behavioural, and transactional datasets with Cogniflow Analytics Pvt. Ltd. ("Recipient") for the purpose of building AI/ML-driven credit risk models, subject to applicable data privacy laws, ethical AI practices, and internal security controls.

### **2. Scope of Data Sharing**

2.1. The Provider will share de-identified and pseudonymized datasets related to:

* Credit card transaction summaries
* Loan repayment behaviour
* Geo-demographic risk clusters
* Customer complaint patterns

2.2. No Personally Identifiable Information (PII) such as names, phone numbers, addresses, Aadhaar, or PAN shall be included in the dataset.

2.3. Datasets will be made available via secure SFTP access on a monthly schedule, with the first transfer initiated on or before February 15, 2024.

### **3. Data Use Limitations**

3.1. The data shall be used **only** for the purposes specified in this Agreement.  
 3.2. Use of data for marketing, behavioural profiling unrelated to creditworthiness, or any form of consumer targeting is **strictly prohibited**.  
 3.3. The Recipient shall not attempt to re-identify data subjects using any external sources.

### **4. Consent and Recordkeeping**

4.1. The Provider affirms that all original data collection from end-users included an explicit opt-in consent clause for research and analytics.  
 4.2. The Provider shall maintain audit logs of consent records for a period of **5 years** from the date of data collection.

### **5. Data Protection and Security**

5.1. The Recipient shall adopt the following technical and organizational measures:

* AES-256 encryption for data at rest and in transit
* Role-based access control (RBAC)
* Access logging and periodic audits
* MFA for administrative access

5.2. Cloud storage must comply with ISO 27001 and SOC 2 Type II standards.  
 5.3. No data may be transferred or stored outside of India unless prior written approval is granted by the Provider.

### **6. Breach Notification and Incident Response**

6.1. In case of an actual or suspected data breach, the Recipient shall notify the Provider within **12 hours** of discovery.  
 6.2. A detailed Root Cause Analysis (RCA) report and mitigation plan must be submitted within **72 hours**.  
 6.3. The Provider reserves the right to suspend data transfers until the breach is fully resolved and verified.

### **7. Audits and Inspections**

7.1. The Provider may conduct security and data usage audits of the Recipient no more than **twice per year** with 10 days' advance notice.  
 7.2. The Recipient shall grant access to logs, cloud configuration settings, and data access records during such audits.  
 7.3. Failure to comply with audit requests may result in contract suspension.

### **8. Liability and Penalties**

8.1. The Recipient shall be liable for any damages or regulatory fines arising out of misuse, breach, or unauthorized processing of data.  
 8.2. A penalty of ₹15,00,000 shall be levied for each confirmed incident of non-compliant data use.  
 8.3. The Recipient’s total liability under this agreement shall not exceed ₹1 Cr, except in cases of willful misconduct.

### **9. Term and Termination**

9.1. This Agreement shall remain in effect for 3 years from the Effective Date unless terminated earlier.  
 9.2. Either party may terminate with 45 days' written notice.  
 9.3. In the event of termination:

* All data must be deleted within 15 days
* A deletion certificate must be provided
* Any ongoing model training using the data must be discontinued

### **10. Governing Law and Jurisdiction**

10.1. This Agreement shall be governed by the laws of the Republic of India.  
 10.2. Any disputes shall be resolved through binding arbitration in Mumbai under the Indian Arbitration and Conciliation Act, 1996.

### **Annexure A – Monthly Data Fields**

* Credit Card Usage Summary (Total Spend, Category Breakdown, Number of Transactions)
* Geo Risk Index (District-level clustering)
* Complaints Received (Issue Type, Channel, Time to Resolution)
* Loan Repayment Score (30d, 60d, 90d buckets)

### **Annexure B – Data Flow Architecture**

* Source → ETL Masking → Secure API Gateway → Encrypted Cloud Blob → Recipient Download
* Monitoring dashboard to track download timestamps and access origin

### **Annexure C – Risk Summary**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Type** | **Likelihood** | **Impact** | **Mitigation** |
| Misuse of data | Medium | High | Legal penalty + audit trail logging |
| Breach during transfer | Low | Medium | Encrypted SFTP + endpoint whitelisting |
| Cloud misconfiguration | Medium | High | SOC 2 audits, RBAC |
| Consent data mismatch | Low | High | Consent log retention for 5 years |