

Partner Data Requirements and Protection

Coinflow Labs Limited (“Client”) has entered a partnership with [nSure.ai](#) (“Supplier”), the payment fraud prevention vendor of choice: including but not exclusive to Fintech, Crypto, Digital Assets, iGaming, Gaming, Prepaid & Gift Cards, in order to guarantee that each one of the Clients partners benefits from the most accurate technology to optimize a safe payment experience for their users.

[nSure.ai](#) offers a managed service based on adaptive AI that deploys, for each Client, a dedicated model trained on their data. Focusing on behavior patterns - the most accurate and uniquely effective way to mitigate modern scalable fraud - our solution takes a fundamentally different approach to detecting fraud and preventing it from happening. Our customers benefit from the highest-efficacy decisions delivered in under 500 milliseconds, with up to 98% approval rates and a chargeback guarantee, generating zero-risk net incremental profit.

[nSure.ai](#) prevents payment fraud using fully automated AI technology, which analyses hundreds of thousands of data point compounds in order to instantly decide to Approve or Decline each transaction.

In addition, nSure.ai takes chargeback liability and reimburses the merchant if a transaction it has decided to approve turns out to be fraudulent.

With their superior accuracy and financial guarantee business model, nSure.ai delivers Net Incremental Profit to all Coinflow partners using Coinflow payment solutions:

- Higher approval rates specifically for new buyers (higher CLTV)
- No cost of chargebacks
- Faster verification, more satisfactory UX

What information is collected from the end user for each reviewed transaction?

A Data Processing Addendum (“DPA”) made by and between Client and Supplier, as required by the EU General Data Protection Regulation 2016/679 (“GDPR”), the California Consumer Privacy Act of 2018, as amended (“CCPA”), and other applicable data protection and privacy laws (together “Applicable Laws”). This Agreement governs matters of data protection with respect to Personal Data between the Parties and shall be in force for as long as Parties Process Personal Data in connection with their partnership agreement.

Supplier would ingest the following personal data into Client's dedicated AI model: consumer name (first and last), address, email, device information, transaction-related data, usage of Client online platform, and any other information either provided directly by Client or otherwise processed through Supplier Services.

What policies or processes are in place around how end user data is used and stored?

Supplier uses the most advanced protection technology, processes, and compliance standards, guaranteeing end user data is safe, at rest and in transit, and will not be used or resold:

1. AWS US cloud services data security in multiple data centers
2. Secure APIs with encryption for all data both in transit and at rest
3. SOC 2 Type 2 certification with highest security controls for client data protection
4. Compliance with GDPR and California CCPA
5. Data not shared with any third parties, including other Supplier Clients

What policies or procedures are in place around retention of end user data?

Supplier would encrypt stored data for up to 5 years before it is anonymized in the system. Supplier recommends retention period to be as long as possible: shortening the retention period, the greater the risk minimization. If Client elects, Supplier would be prompted to delete and procure the deletion of Personal Data were so instructed by Client unless and to the extent that retention is required by applicable laws.

So, why share your data?

Because AI technology's efficacy is directly correlated to the amount of data fed to the machine learning model. In addition, it is a natural anticipation of new partners to see high results in the first weeks of engaging with Coinflow Labs. Therefore, the more data the nSure.ai models will receive from each new partner, including historical data, the better results will be delivered from day one, because the model will have had the ability to learn from more data.

MyEDPO



Data Protection Services

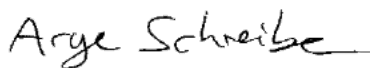
The purpose of this review is to assuage potential clients and end-users that the data processing performed by nSure.ai on behalf of its clients (in their roles as a controller of such data) is subject to strict data protection and data security measures in order to ensure the data's integrity.

In our role as nSure.ai's DPO, MyEDPO assists nSure.ai in maintaining its compliance with applicable data protection laws, including the European Union's General Data Protection Regulation 2016/679 ("GDPR") and the California Consumer Protection Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA"), including through the implementation of a comprehensive data protection compliance program. nSure.ai adheres to relevant data protection standards, in part by leveraging Amazon Web Services, Inc. ("AWS") for its US cloud services, benefiting from their established data security practices.

Additionally, from a data security perspective, nSure.ai maintains SOC 2 Type II certification, which ensures the ongoing implementation by nSure.ai of security controls for the protection of its clients' data. Therefore, such data is transferred between nSure.ai's clients and its servers solely through secure APIs with encryption both in transit and at rest.

nSure.ai processes data solely on behalf of its clients and under their instructions to analyze, detect, and prevent fraudulent digital transactions. Clients receive real-time risk assessments based on data provided by their end-users during transactions, securely transferred to nSure.ai for analysis. Currently, only transaction-specific data is processed, though adding historical data, if provided, would enhance assessment accuracy. Any such data would be processed under the same rigorous data protection and security standards as all other client data handled by nSure.ai and would not be shared with third parties, including other nSure.ai clients.

For any further questions or elaborations, please contact nSure.ai's Data Protection team at privacy@nSure.ai.



Arye Schreiber, CEO