Ingenico GO

- Description: Ingenico GO consists of a fully-featured solution for Processing and Financial Services to accept online payments. Through its easy integration the Merchant can start selling online in a fast and secure manner. The Financial Services and intuitive back office allow the Merchant to save costs and time to manage its payments.

- Contains:

  - Hosted Payment Page:
    Contains a link to a Payment Page hosted by Ingenico FS (via redirection from the Merchant's servers to a Payment Page hosted by Ingenico FS): a secure page to capture the Account Data. The Hosted Payment Page facilitates the processing of E-Commerce Transactions, because the Merchant does not need to comply with the highest PCI DSS standards.
  - Advanced customization of the Hosted Payment Page (dynamic template):
    Gives the Merchant the possibility to create its own template of the Hosted Payment Page. The fields (name, language, amount, Payment Methods) cannot be changed but the Merchant fully controls the page layout (colors, logo display, background,...).
  - API (DirectLink):
    DirectLink allows the Merchant to set up a server-to-server integration with the Ingenico Platform to submit Transactions, e.g. when initiated from a Payment Page hosted by the Merchant.
  - Batch file Processing:
    Allows the Merchant to upload a file with Transactions for bulk offline Processing on Ingenico Platform.
  - Merchant Area:
    Access to the Ingenico Account to perform operations and maintenance of Transactions. It also provides advanced search criteria, such as Account Holder name, Card number and payment encoder to retrieve specific Transactions more efficiently, and to generate payment reports.
  - User manager:
    Allows the administrator of the Merchant to define up to 5 Merchant Users including the settings for each Merchant User accessing the Ingenico Account.
  - Reconciliation:
    Allows the Merchant to match its Transactions processed by Ingenico FS with the Merchant's bank account statements
  - Reporting tools (push reports):
    Allows the Merchant to create and receive up to 5 reports per day containing information on Transactions and /or payment status.
  - 3D-Secure Cardholder authentication:
    An additional layer of protection with secure Cardholder authentication (Verified-by-Visa, MasterCard SecureCode, American Express SafeKey, Diners ProtectBuy and J/Secure).
  - Basic fraud prevention tool:
    The basic fraud prevention allows to reduce the Merchant's exposure to risk by:
    - Blocking fraudulent Transactions in real-time using IP-address, credit-card and BIN black lists
    - Restricting Payment Methods to certain geographic regions and used currencies

- Allowing only 3-D secure payments to minimize Chargebacks
- Set minimum and maximum amounts per Transaction for each Payment Method

The Merchant is required to activate the fraud tool, and to configure the applicable rules in the Merchant Area.

Whenever the Merchant activates this option, the Merchant has the quality of data controller and Ingenico FS acts in the quality of data processor. Therefore, the data processing clauses (Annex 2) shall apply.

- Tokenization (Alias Manager):

An alias or token is a reference to the stored Cardholder data of an Account Holder. It may consist out of Primary Account Number (PAN), Cardholder name, service code, expiration date. By using an alias or token, the Account Holder can complete a Transaction without having to re-enter his Cardholder data on the Ingenico Platform. Tokenization implies the use of Account Holder's Cardholder data which can only be stored and linked to an alias if the Merchant has obtained the written permission from the relevant Account Holder in this respect. In addition the Merchant also needs to obtain the written permission of the relevant Account Holder for any other use relating to its Cardholder data and alias (such as the sharing of the Cardholder data and the alias of the Account Holder with other legal entities (notably entities whose Ingenico Accounts are grouped under the same Ingenico Group Account).

Whenever the Merchant activates this option, the Merchant has the quality of data controller and Ingenico FS acts in the quality of data processor. Therefore, the data processing clauses (Annex 2) shall apply.

- MO/TO (subject to acceptance by Acquirer):

Possibility to perform Mail order Telephone order (MO/TO) Transactions and use Ingenico FS's virtual terminal to submit new Transactions manually trough the Merchant Area.

- Advanced fraud prevention solution (payable option)

The advanced fraud prevention solution consists of two levels of fraud risk prevention:

➢ **Level one fraud risk prevention:** the Scoring module or the Checklist module

Description

Representing the first level of fraud risk prevention, the Scoring or Checklist module allows you to accept, review and/or block Transactions based on your own fraud prevention parameters. The Checklist and Scoring modules cannot be used simultaneously. You must choose either one or the other.

Processing of Personal Data

Please note that with regard to the fraud module Scoring and the fraud module Checklist, as well as with regard to the final risk score, the Merchant acts in the quality of data controller and Ingenico FS acts in the quality of data processor. Therefore, the data processing clauses (Annex 2) shall apply.

➢ **Level two fraud risk prevention:** the Fraud Expert solution

Description

Representing the second level of fraud risk prevention, the Fraud Expert solution is used in combination with the Scoring or Checklist modules.

Processing of Personal Data

An affiliate of Ingenico FS is the data controller regarding the second level of fraud risk prevention. Such affiliate shall respect the applicable Data Protection Law.

Manual review and device finger print feature: Optional in the level two fraud risk prevention:

☐ Outsourcing of manual reviews of medium-risk Transactions to an expert*

*This service can be activated later by selecting it in the Ingenico Account (select the appropriate checkboxes). As soon as the Merchant activates this service, it will be invoiced according to the prices mentioned in article 3.5 below and the Merchant will be contacted to agree on the modalities.

☐ Device fingerprint feature *

*This service can be activated later by selecting in the Ingenico Account (select the appropriate checkboxes). This option implies cookies and other tracking technologies. Therefore, you undertake, prior to this activation, to obtain consent from your own customers in compliance with the applicable provisions on cookies and other tracking technologies. In the absence of this consent, you undertake to refrain from activating or refrain from requesting the activation of this feature.