Blockchain Platform

Apla General Terms and Conditions

*This Apla General Terms and Conditions **("Apla T&C")** describe mutual rights and obligations of Apla Users in the course of accessing and using Apla blockchain platform.*

It is to be acknowledged and confirmed either electronically or in paper form by each Apla User prior to onboarding to Apla Platform. A record of the consent shall be kept by the responsible Eligible Person.

Document Ref.	APL/TC
Version:	1
Dated:	01 February 2018
Document Owner:	EGAAS S.A.
Document Author:	V. Bondar (Avocats associés ChristmannSchmitt)

Revision History

Version	Date	Approved by	Summary of Changes

Table of Content

1. Glossary of Terms

1.1. Unless the context requires otherwise, the following terms of this Article 1 shall be used in this Apla T&C and Apla Policies:

Affiliate or **Affiliated Person** means in relation to any Person, a Person that directly or indirectly through one or more intermediaries controls such Person, is controlled by or is under the common control with such Person. For the purposes of this Agreement, **to control** (including the terms **controlled by** and be **under the common control** with the respective meanings) means with respect to any Person the direct or indirect power to manage or give instructions in respect of managing the actions of senior officers or policies of such Person or the right to veto important strategic decisions of such Person based on the ownership and on holding voting securities, by contract or on any other grounds

APL Wallet means a software application for storing, holding and transferring APL Tokens

APL Wallet Owner means any natural person or legal entity, including international, national or intergovernmental body or institution that have got a private key to access a specific APL Wallet

APL Tokens means Tokens generated by the source code of one of the Apla Ecosystems that are used by Apla Users to pay a license fee for the execution of Smart contracts, creation of tables, and adding new columns and rows to them in all Apla Ecosystems

Apla Association means Apla Consensus ASBL, a non-profit organisation established under Laws of Luxembourg at the following address: L-2143 Luxembourg, 45 rue Laurent Ménager

Apla Contractual Documentation means the T&C and Apla Policies, as amended from time to time

Apla Ecosystem means is an autonomous software environment within Apla Platform that consists of a certain number of applications (interfaces, contracts, and database tables) and Apla Users, who create these applications and work with them

Apla Ecosystem User mean any natural person or legal entity, including international, national or intergovernmental body or institution that has been admitted by Eligible Person as a member of Apla Ecosystem

Apla platform means a permissioned Blockchain, the source code of which is stored at GitHub.com/AplaProject

Apla Policies means any and all of the following policies and documents adopted by Apla Association that are published on the website www.GitHub.com/AplaProject, including but not limited to the following: Apla Admission Policy, Apla Compliance Policy, Apla Data Protection Policy, Apla Information Security Incidents Procedure, Apla Consensus Protocol, Apla Technical Paper as amended or added from time to time

Apla Software means both GenesisKernel Software and EGAAS Software the source code of which is published at GitHub.com/AplaProject

Apla User means any of the following categories of persons: Supervised Financial Institutions, including other Validating Nodes, APL Wallet Owners or Apla Ecosystem Users

Apla Software License means the license to use Apla Software granted by EGAAS to Supervised Financial Institutions and sub-licensed by them onwards to the other Apla Users on terms and conditions set forth in Article 7 hereof

Applicable Laws means Laws applicable to the relationship between the parties arising from or in connection with Apla Contractual Documentation, as defined in accordance with Article 17 hereof

Blockchain means a software program for executing Smart laws and Smart contracts based on the distributed ledger technology. The program operates on the basis of peer to peer (P2P) architecture that is a system of peer client-side programs installed on users' computers and participating in data exchange via peer to peer (P2P) computer network

Content means data files, written texts, music, graphics, images, sounds, videos, messages and the like

EGAAS means a legal entity established under the Laws of Luxembourg, registered with RCS Luxembourg under the number B216352 at the following address: L-1273 Luxembourg,

20 rue de Bitbourg

EGAAS Software means modifications of and/or additions to the source code of GenesisKernel Software, programming elements of Smart contracts and Smart laws developed by EGAAS corporation and published at GitHub.com/AplaProject

Eligible Persons means Apla Users that are eligible to open APL Wallets and other Wallets to third parties under Apla Admission Policy (i.e., Supervised Financial Institutions and APL Wallet Owners)

Fiat currency means an official currency of the members of the United Nation recognized as a legal tender in those countries

GenesisKernel Software means free software product published for the first time at https://github.com/GenesisKernel/go-genesis and distributed under the MIT license (https://github.com/GenesisKernel/go-genesis/blob/master/LICENSE)

Laws means the civil law in general, any constitution, legislation, decree, order, instruction, rule, regulation, ordinance, code, directive, by-law, judgment, international treaty or any other legislative or quasi-legislative measure related, in each case, to the respective jurisdiction that may be applicable to any transaction closed or to the circumstances existing as of the respective date and, in each case (if any liability is stipulated by or may arise in accordance with them) including any former provision (that may be statutorily amended or re-enacted from time to time) that was directly or indirectly replaced by such provision

Luxembourg means the Grand Duchy of Luxembourg

Person means any individual or legal entity, corporation, company, partnership, joint venture, association, limited liability company, joint-stock company, organisation, trust, association, trustee, administrative receiver or liquidator or any Public Authority, including personal legal representatives and assigns of such Person (or executors or heirs of a deceased person)

Private key means is a set of specific parameters, based on the algorithmic encryption formula, that act to access to APL Wallet or Wallet and to sign Transactions in Apla Ecosystem

Private Contractual Arrangement means a contractual

arrangement between Eligible Person and other Apla User or between different Apla Users as regards opening Wallets, Smart contracts, Smart laws and other participation in Apla Platform

Public Authority means any supranational, national, municipal, local or foreign public authority or organisation, or any department, commission, administration, bureau, agency, court or instrumentality, subdivision or any other authority thereof, or any quasi-public or private authority having any regulatory, tax, financial regulation and any other public or quasi-public authority

Smart contracts or contract means a self-executable, self-enforceable and self-verifiable computer protocol that is distributed and run in each Apla Ecosystem

Smart laws mean a computer protocol governing the formation and execution of Smart contracts in each Apla Ecosystem

Supervised Financial Institution means a member of Apla Association that is either (i) an entity that is licensed or otherwise authorised by the financial market regulator in the country of its establishment to be engaged in payment services or (ii) an international, national or intergovernmental body or institution that engage in payment services, including central banks

T&C means this multiparty agreement, including all appendices and addenda hereto that may be further amended, modified or supplemented from time to time

Tokens means a digital representation of value generated by Apla Ecosystem that functions as either a medium of exchange, and/or a unit of Wallet, and/or a store of value but does not have legal tender status

Transaction means any of the following operations generated by Apla User and executed in the Apla Platform environment: Smart contract, Smart law, creation of tables, and adding new columns and rows

Validating Node means an entity engaged in the execution of Apla Consensus Protocol as defined in Article 4 of Apla Admission Policy

Virtual currency exchange means a software application and/or services enabling the holders of the Tokens and/or APL

Tokens to exchange them into other Tokens or Fiat currency

Wallet means a software application for storing, holding and transferring Tokens

1.2. In the context of this T&C and Apla Policies:

1.2.1. A reference to this T&C shall be interpreted as a reference to this document, including Apla Policies, with all amendments, supplements, appendices, novations or transfer of rights made from time to time;

1.2.2. A reference to the article, clause, sub-clause or appendix, unless such reference is followed by the name of a particular document, shall be deemed the reference to an article, clause, section or appendix to this T&C;

1.2.3. A reference to the terms defined in this T&C includes the singular and plural of those terms and denotes the masculine, feminine or neuter gender, as the context requires;

1.2.4. It is understood that the words "including" and "includes" are followed by the expression "without limitation", and such expressions shall be without prejudice to the generality of the foregoing;

1.2.5. Headings are for the convenience only and shall not affect the interpretation of this T&C; and

1.2.6. All terms that are written in capital letters and not defined in Article 1.1 shall have the meaning ascribed to those terms in the text of this T&C and Apla Policies or appendices hereto.

2. Introduction

Apla Platform is a Blockchain platform that is designed by the developers for building digital ecosystems and carrying out other e-commerce activities. Apla Platform is not meant to be used for non-business-related activities by any Person.

The distributed ledger technology, which is deployed in Apla Platform, assumes that the data recorded in the tables of each Apla Ecosystem will be spread among the computer devices of Apla Users that have legitimate access rights to this Apla Ecosystem. Considering the fact that Apla Users may theoretically be established (for legal entities) or residing (for natural persons) in any world jurisdiction, all Apla Users can potentially be subject to the application of public laws and policy rules of different states in relation to such matters as information security and data protection, any-money laundering and scope of restricted or illegal activities being prosecuted under criminal and/or administrative laws of such states.

The approach adopted in this T&C aims at all Apla Users applying the most stringent set of rules governing the particular area of public law. This set of rules is indicated in this T&C and the other parts of Apla Contractual Documentation. If Applicable Laws establish different rules, Apla User must ensure the compliance with those rules in addition to Apla Contractual Documentation.

The purpose of this T&C is to establish a legal framework for contractual relationship between different categories of Apla Users. It applies to all Transactions and other activities in Apla Ecosystems, including but not limited to the following:

- distribution and use of Apla Software;
- opening Wallets and AML/CFT compliance;
- information security and data protection;
- transaction validation services;
- compliance with Applicable Laws;
- liability and dispute resolution matters.

Apla Users may agree upon Private Contractual Arrangements with their direct counterparties that do not violate Apla Contractual Documentation and Applicable Laws.

3. Opening Wallets and AML/CFT Compliance

3.1. Any Person can open Wallet on Apla platform if it satisfies the eligibility criteria and follow the procedure set forth in Apla Admission Policy. Apla Software for opening an Wallet can be downloaded from GitHub.com/AplaProject. It will have a limited functionality until activated by Eligible Persons.

3.2. Supervised Financial Institutions and APL Wallet Owners shall apply the know-your-customer procedure during client onboarding process in cases indicated in Apla Admission Policy and implement internal procedures to ensure their compliance and compliance of their counterparties with Apla Compliance Policy in the course of using Apla Platform.

3.3. Apla Admission Policy and Apla Compliance Policy have been designed for Apla Users to comply with the following international Laws and recognised standards:

- UN Convention Against Transnational Organized Crime (New York, 2004);[1]
- UN Convention on the Suppression of the Financing of Terrorism (1999);[2]
- FATF Guidelines on Risk-Based Approach to Virtual Currencies.[3]

Both UN Conventions provide for the obligation of the participating countries to set domestic regulatory and supervisory regime for banks and non-bank financial institutions, which shall include requirements for customer identification, record-keeping and providing information on suspicious transactions, licensing activities of such organizations, etc.[4]

According to the FATF Guidelines on Risk-Based Approach to Virtual Currencies[5], any natural or legal person can be qualified as a financial services provider if it carries out as a business the

1. https://www.Unodc.Org/documents/middleeastandnorthafrica/organised-crime/united_nations_convention_against_transnational_organized_crime_and_the_protocols_thereto.Pdf

2. http://www.un.org/law/cod/finterr.htm

3. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

4. paragraph 1 (a) v. 7 of the UN Convention against Transnational Organized Crime and article. 18 of the UN Convention for the Suppression of the Financing of Terrorism.

5. Page 6 point 17 of the Guidance: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

following activities: decentralized cryptocurrency exchange, services to create virtual wallets, payment processing activities senders of funds and similar businesses.

3.4. Eligible Persons shall take appropriate measures to comply with Applicable Laws and Apla Contractual Documentation at their own cost, including mandatory reporting of non-compliance cases to Public Authorities concerned, if required by Applicable Laws and Apla Contractual Documentation.

3.5. The other roles and responsibilities of Apla Users in connections with AML/CFT compliance are set forth in Apla Admission Policy and Apla Compliance Policy.

4. Information Security and Data Protection

4.1. Apla Users acknowledge and agree that the source code of Apla Software, including Smart contracts and Smart laws, are still in an early development stage and are not certified by any Public Authority in any jurisdiction.

4.2. Apla Users further acknowledge and agree with the following risks in connection with their use of Apla Platform, including underlying Apla Software, Smart contracts and Smart laws:

- Apla platform may not be free from any vulnerabilities or technological bugs;

- any Content and Tokens, including APL Tokens, stored in any Apla Ecosystem may be damaged, lost or stolen as result of information security incidents and/or illegal hackers' attacks;

- content may be decrypted with the use of new evolving technologies, and, therefore, it may become publicly available to third parties.

4.3. Neither EGAAS nor Eligible Persons give no warranty to their counterparties that the events indicated in Article 4.2 hereof, will not occur. If this happens, the affected Apla Users and EGAAS shall use their best endeavors to mitigate the damage caused by the specific event and restore the functionality of the system by following the procedures set forth in the respective Apla Policies and Articles 4.4 to 4.6 below.

4.4. Apla Users shall adhere to the set of Apla Policies designed to ensure protection of personal data, data integrity, confidentiality and proper management of information security incidents. The roles and responsibilities of Apla Users in the area of information security and data protection depend on whether they act as data controllers, data processors, users or administrators of a specific Apla Ecosystem (as defined in the respective Apla Policies). Specifically, the following Apla Policies address the matters set forth in this Article:

- Apla Data Protection Policy;
- Apla Personal Data Breach Notification Procedure;
- Apla Information Security Incidents Response Procedure.

4.5. Apla Users acknowledge and agree that if the information security incident has affected the accuracy and integrity of the data stored in any Apla Ecosystem, the Apla Platform source code deploys the Smart laws mechanism whereby Validating Nodes may vote to restore the data to the pre-incident condition without the need of creating a fork of Apla Platform. In this case, the recovery Smart contract is generated by Apla Association. This Smart contract is to be validated by at least 75 (seventy-five) % of Validating Nodes.

5. Content

5.1. Apla Users shall refrain from submitting for storage in tables of any Apla Ecosystem of any Content that is not encrypted with cryptographic technologies. Any Content is the sole responsibility of Apla User from whom the submission is originated. Apla Users who merely excise the processing and transaction validation roles in relation to Content, do not control the submitted Content, and, therefore, do not guarantee its accuracy, integrity and quality.

5.2. Apla Users shall not use Apla platform and/or allow the usage of Apla platform for submitting Content, whether encrypted or not, that is:

- harassing, threatening, harmful, tortious, defamatory, libelous, abusive, violent, invasive of another's privacy, hateful, racially or ethnically offensive;

- engaged in any copyright infringement or other intellectual property infringement, or disclosing any trade secret or confidential information in violation of a confidentiality, employment, or nondisclosure commitment;

- containing computer code or files that are designed to harm, interfere or limit the normal operation of Apla Platform (or any part thereof);

- interfering with or disrupting Apla Platform, or any servers or networks connected to Apla Platform;

- in any other way violating Apla Contractual Documentation, Private Contractual Arrangements and Applicable Laws.

5.3. By submitting Content to any Apla Ecosystem, Apla Users agree to grant a worldwide, royalty-free, not-exclusive license to use, distribute, reproduce and publish such Content to those Apla Users who have access rights to Apla Ecosystem in which such Content is submitted for storage. Apla Users shall further agree that any Content submitted by them shall not infringe or violate the rights of any other party or violate any laws, contribute to or encourage infringing or otherwise unlawful conduct.

6. Transaction Validation Procedure

6.1. All Apla Users shall acknowledge and agree to the Transaction validation procedure described in Apla Consensus Protocol that will be executed by Validating Nodes.

6.2. Validating Nodes shall not be liable for any failure to validate Transaction if it's not in line with the algorithm described in Apla Consensus Protocol.

6.3. Any claims relating to Transaction validation services shall be addressed by Apla User to the person who opened Wallet to such Apla User on Apla Platform.

7. Apla Software License

7.1. Apla Software includes an integrated development environment with a multi-level system for the management of access rights to data, interfaces, and Smart contracts. The technical characteristics of the Apla Software are indicated in Apla Technical Paper.

7.2. Apla Users are granted a permission to deal in the Apla Software without restrictions, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of Apla Software, and to permit persons to whom Apla Software is furnished to do so, subject to the following conditions:

- the copyright notice of GenesisKernel and EGAAS S.A. and this permission notice shall be included in all copies or substantial portions of the software;

- a result of the dealing in Apla Software cannot be implemented outside of the Apla Platform environment.

7.3. THE APLA SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ERROR FREE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE APLA SOFTWARE.

8. Charges and fees

8.1. Supervised Financial Institutions shall pay a license fee to EGAAS (the software copyright holder) for the use of Apla Software by Supervised Financial Institutions and other Apla Users. Specifically, the license fee is paid for the following activities: execution of Smart contracts, creation of tables, and adding new columns and rows to them in any Apla Ecosystem.

The license fee rate is set in conventional units, called Fuel but it is to be paid in APL Tokens. The exchange rate of Fuel to APL Tokens can be configured in the parameters of the respective Apla Ecosystem and is set by voting of the Supervised Financial Institutions (simple majority voting).

The Platform Configuration Ecosystem has a parameter to set the maximum amount of Fuel that one transaction can cost (max_fuel_tx), and the maximum amount of Fuel that can be spent for the creation of one block (max_fuel_block). This parameter is set by voting of Supervised Financial Institutions (simple majority).

8.2. [Forty percent] of the license fees collected by EGAAS shall be equally shared by the latter between Validating Nodes as a payment for the maintenance of the IT infrastructure by Validating Nodes necessary for carrying out Transaction validation services.

8.3. Upon creation of a new Smart contract by Apla User, the license fee in APL Tokens is automatically charged to APL Wallet of Apla User who created this Smart contract.
For Apla Users who don't have APL Wallet and, therefore, cannot pay a license fee in APL Tokens, there is an option to bind Smart contract to an arbitrary Wallet (for example, the ecosystem founder's APL Wallet, which will make the execution of the license free for ecosystem members). The binding of the contract to APL Wallet can be changed at any time. To do so, a special application is used that notifies APL Wallet Owner to which the smart contract is being bound, and binds the contract after receiving confirmation.

8.4. Apla Users acknowledge and agree with the license fee calculation and payment methods set forth in Articles 8.1 to 8.3 hereof. The license fee does not include VAT, if applicable, that

must be added by responsible Eligible Person on the top of the license fee.

8.5. Supervised Financial Institutions and APL Wallet Owners may charge additional fees to their counterparties for Wallet opening and administration services. These charges shall be indicated in Private Contractual Arrangements.

9. APL Tokens Exchange

9. 1. A rate of exchange of APL Tokens into Fiat Currencies and other Tokens and cryptocurrencies shall be established by each Supervised Financial Institutions at their full discretion.

9.2. APL Tokens can be traded on organized exchanges administrated by Supervised Financial Institutions. No other Apla User is entitled to offer exchange services in relation to APL Tokens and/or any derivative instruments linked to APL Tokens as a business activity.

10. Liability

10.1. *Liability of EGAAS*

10.1.1. The scope and limitations of the EGAAS liability in connection with the distribution and dealings in Apla Software is set forth in Article 7.3 hereof.

10.1.2. Without prejudice to the EGAAS's liability exemption under Article 7.3, for any claim, damages or other liability, whether based on contract or tort, arising from, out or in connection with participation in Apla Platform and/or proper performance of the EGAAS's obligations (expressed or implied) under Apla Contractual Documentation and/or under any applicable Law of any state, EGAAS can be made liable for direct damages only and as a result of willful misconduct and/or gross negligence on the side of EGAAS subject to the following limitations:

I. for claims about damage to, or loss of, APL Tokens, and/or other Tokens, and/or Content in any Apla Ecosystem, EGAAS's total cumulative liability to all Apla Users (in aggregate) for all such claims duly notified in any one calendar year will not exceed [1 (one) million] Euro

II. for any other claims, EGAAS's total cumulative liability to all Apla Users (in aggregate) for all such claims duly notified to EGAAS in any one calendar year will not exceed [300,000 (three hundred thousand)] Euro

For the purpose of this Article, if a claim from an Apla User is followed by one or more claims that relate to the same event or series of connected events, these claims shall be treated as one claim, notified on the date the first claim was notified.

The notice to EGAAS shall be sent by registered mail with acknowledgment of receipt to the following address: L-1273 Luxembourg, 20 rue de Bitbourg.

10.1.3. EGAAS shall be liable to pay compensation only under the established claims that are either (i) the claims approved by EGAAS or (ii) the claims awarded by final and binding arbitral award or judgement of the court of any

jurisdiction enforceable against EGAAS in Luxembourg.

10.1.4. If the aggregate claims from all Apla Users exceed the amount set forth in Article 10.1.2 above, the liability of EGAAS to each Apla User in connection with established claim of such Apla User shall be reduced and be determined as a percentage of the claim of such Apla User in the aggregate claims from the other Apla Users within the established liability limit.

10.1.5. For the purposes of this Article 10.1, the term "EGAAS" shall include collectively EGAAS S.A., its Affiliates, subsidiaries, directors and employees.

10.2. *Liability of Apla Association*

The liability of Apla Association in connection with its participation in Apla Platform and/or proper performance of its obligations under Apla Contractual Documentation, including applicable Laws of any jurisdiction, shall be subject to the same terms and conditions and liability limits as set forth for EGAAS in Article 10.1 hereof. Any reference to EGAAS in this Article shall be deemed to be the reference to Apla Association.

The address for sending a claim notice to Apla Association shall be as follows: 45, rue Laurent Menager, L-2143 Luxembourg.

10.3. *Liability of Supervised Financial Institutions and other Apla Users*

Unless otherwise is expressly stated in contractual arrangements between specific Apla Users, the liability of Apla User (including Supervised Financial Institution) in connection with its participation in Apla Platform and/or proper performance of its obligations under Apla Contractual Documentation, including applicable Laws of any state, shall be subject to the same terms and conditions and liability limits as set forth for EGAAS in Article 10.1 hereof.

Any reference to EGAAS in this Article 10.1 shall be deemed to be the reference to Apla User. The reference to Luxembourg in Article 10.1.3 shall be deemed the reference to the state where the Apla User has got a permanent establishment (in case of a legal entity) or permanent residence (in case of a natural person).

The address for sending a claim notice to Apla User shall be

specified in Private Contractual Arrangement between Apla User and Eligible Person.

10.4. *Indemnification*

Apla Users **("Indemnifying Persons")** agree to defend, indemnify and hold the other Apla Users, including EGAAS and Apla Association, their Affiliates, directors and employees **("Indemnified Persons")** harmless from any claim or demand, including reasonable attorneys' fees, made by any Person, relating to or arising from: (a) any Content they submit to processing and storage in Apla Platform; (b) any violation by Indemnifying Persons of Apla Contractual Documentation, Private Contractual Arrangements and Applicable Laws; (c) any action taken by data controllers and data processors (as defined in Apla Data Protection Policy) as part of their investigation and/or remediation of a suspected or established violation of Apla Contractual Documentation; and (d) any usage of Wallets, including APL Wallets, by Indemnifying Persons; and (e) suspension and/or cancellation of APL Wallets and other Wallets by Eligible Persons in accordance with Article 11.2.

10.5. *Force Majeure*

None of the Apla Users, including EGAAS and Apla Association, shall be liable for a failure to properly perform their duties under Apla Contractual Documentation and Applicable Laws if this non-performance or poor performance is resulted from force majeure events. Force majeure event means any event and/or circumstance, which is beyond the reasonable control of, and is not attributable to, the affected party resulting in the affected party being prevented from performing or being delayed in the performance of any of its obligations under Apla Contractual Documentation. Force majeure event may include, but not limited to, an act of a Public Authority or court of any state, interruption or unavailability of power supplies and telecommunication networks in addition to the acts of God.

11. Termination and Suspension of Wallets

11.1. Apla Users can withdraw and terminate their Wallets, including APL Wallets, at any time by giving a notice to Eligible Persons with whom they have established a direct contractual relationship.

11.2. Apla Users acknowledge and agree that Eligible Persons are entitled to suspend/or terminate Wallets opened by them by a written notice to Apla Users concerned, if, in the reasonable opinion of the Eligible Person, the following events occur:

- to prevent or resolve any information security incidents of Apla Platform;
- to comply with their commitments under Apla Contractual Documentation and Applicable Laws;
- if Apla User has committed a material breach or repeated breaches of Apla Contractual Documentation and/or Applicable Laws;
- if Apla User becomes insolvent or a receiver, manager, administrator, liquidator, or other similar officer or practitioner is appointed over the whole or any substantial part of Apla User's business or assets;
- in the other situations specified in Private Contractual Arrangements between Apla User and Eligible Person and Applicable Laws.

11.3. Apla Software License shall be automatically deemed terminated following the termination of the last Wallet of Apla User on Apla Platform.

11.4. Upon termination of its/his/her APL Wallet or other Wallet under any ground, Apla User shall immediately delete or otherwise destroy all information and materials (including Apla Software and data bases of any Apla Ecosystem) relating to the other Apla Users that it/he/she has got access to as a result of the usage of Apla Platform. This obligation shall be executed by the terminated Apla User in so far and to the extent, it/he/she is not obliged under Applicable Laws or Private Contractual Arrangements to retain certain information and materials for

reporting and other legitimate purposes. In the latter case, the terminated Apla User shall apply the confidentiality and non-disclosure regime in relation to the retained information as set forth by Apla Data Protection Policy.

12. Notices

Unless otherwise is expressly provided for in Private Contractual Documentation, all notices contemplated by Apla Contractual Documentation and Private Contractual Documentation, must be in English and in a written form.

The requirement as to the written form of the notice is deemed satisfied if the notice is sent in paper by courier with acknowledgement of receipt or electronically to the email address of the recipient.

All notices will be deemed effective upon their delivery to the intended recipient. The notice sent electronically shall be deemed delivered upon the notice leaving the server of the sender.

13. Electronic Signatures

13.1. Each Apla User acknowledges, represents and warrants to EGAAS, Apla Association and the other Apla Users that:

I. Any Content or other electronic document stored in any data base of Apla Ecosystem and signed with Private Key of Apla User is authentic copy of the original document that have the same force and legal effect as if in writing or paper form; and

II. Apla User while signing Transaction or other electronic document with Private Key that is linked to the specific public key (Wallet) on Apla Platform has the authority to do so on behalf of the true owner of Wallet; and

III. Signature of Transaction or other electronic document with Private Key in the Apla Platform environment has the same force and legal effect as a hand-written signature; and

IV. Any Transaction and other electronic document signed with Private Key in the Apla Platform environment by Apla User can be used by EGAAS, Apla Association and the other Apla Users as an evidence in court, in arbitration proceedings or in dealings with Public Authorities; and

V. Apla User had sufficient knowledge in the area of information technology or had engaged a third party who had such knowledge to assess the accuracy and reliability of Smart contract signed with Private Key of such Apla User and its conformity with the original intentions of the parties to the signed Smart contract;

VI. Apla User has read Apla Contractual Documentation and has full knowledge and understanding of its rights and obligations contemplated by it.

14. Severability

If any part of the Apla Contractual Documentation is recognized invalid, unlawful, or unenforceable, the other part will continue to be valid and enforceable to the fullest extent permitted by Applicable Law. The invalid, unlawful, or unenforceable part shall be construed and further negotiated by the parties concerned in a manner compliant with Applicable Law and consistent with original intentions of the parties.

15. No Agency

Unless otherwise is expressly stated in Private Contractual Arrangement, the relationship between Apla Users, EGAAS and Apla Association shall not be treated as that of agent and principal.

16. Apla Contractual Documentation

16.1. Apla Users can find the latest version of Apla Contractual Documentation at GitHub.com/AplaProject, including all amendments and additions thereto.

16.2. The rules set forth in Apla Contractual Documentation are deemed to be incorporated in Apla Software License as the material terms and conditions of the Apla Software usage.

16.3. Eligible Persons shall ensure that during client onboarding process and before opening APL Wallet or other Wallet on Apla Platform, Apla Users acknowledge and agree with the latest version of Apla Contractual Documentation. Eligible Persons must be ready to present proofs of obtaining such acknowledgment letters from their direct counterparties that will be capable of being admitted as documentary evidences in court or arbitral proceedings under Applicable Laws.

16.4. Apla Users agree and acknowledge that Apla Contractual Documentation may be amended or supplemented by EGAAS at any time upon notice to Apla Users delivered in the following manner:

- Notices to Supervised Financial Institutions are delivered by EGAAS directly by electronic means to the addresses specified in Apla Software License agreements with such institutions;

- Notices to APL Wallet Owners are delivered by Supervised Financial Institutions by electronic and/or other means to the addresses specified in Private Contractual Arrangements between Supervised Financial Institutions and APL Wallet Owners;

- Notices to Apla Ecosystem Users are delivered by APL Wallet Owners by electronic and/or other means to the addresses specified in Private Contractual Arrangements between APL Wallet Owners and Apla Ecosystem Users.

Amendments and/or additions to Apla Contractual Documentation may only be introduced upon a request of and/or other written consent of Apla Association.

If Apla User does not close its Wallet or APL Wallet on Apla

Platform within 30 days following the receipt of the notice of changes in Apla Contractual Documentation, it shall deem agreed with such changes.

16.5. For the avoidance of any doubt, EGAAS do not collect and keep a record of the data that identifies the owners of public and private keys, except for the data on Supervised Financial Institutions. It is the obligation of Apla Users to keep the records of the data identifying their direct counterparties.

17. Applicable Law

17.1. The relationship between the parties and all contractual and non-contractual obligations arising out of Apla Contractual Documentation, including Apla Software License, or in connection with it shall be governed by and construed in accordance with Laws of Luxembourg to the extent EGAAS and/or Apla Association are involved as one of the parties to these relationships and obligations (without giving effect to any conflict of law rules that would cause the application of other laws).

In all other cases not mentioned in paragraph 1 above, Laws of Luxembourg shall govern the relationship between the parties, unless Apla Users agree upon a different applicable Law in Private Contractual Arrangement or a jurisdiction of a different state is asserted by operation of public law and policy rules of this state, as further described in Article 17.2 hereof.

17.2. In addition to the terms and conditions of Apla Contractual Documentation, Apla User must comply with public law and policy rules of a particular state that establish its jurisdiction (legislative and judicial) in respect of carrying out various activities on Apla platform. Specifically, the jurisdiction of a particular state can be asserted in one of the following cases:

- the activity is carried out on the territory of the state; or

- the activity is carried out outside the territory of the state but it is focused on the territory of this sate; or

- the activity involves consumers, property and other mandatory links to the territory of the state that cannot be derogated from by a contractual agreement between the parties in accordance with public and private international law rules of this state.

The activity shall be deemed to be carried out on the territory of the state, if it is executed by its resident who is the individual or legal entity having permanent establishment in the territory of the state. In the case of legal entities, international legislative and judicial practice of states[6] has developed the following

6. See. S. 418 UK Financial Services and Market Act 2000, art. 7 (1) of the OECD Model Tax Convention on Income and on Capital (28/01/2003), paras 7.2.2 / 7.2.3. of the Tax and the Internet Discussion Report of the Taxation Office Electronic Commerce Project Team, Somafer case of the European Court of Justice 33/78 Somafer SA v Saar-Ferngas AG [1978] ECR 2183

criteria of permanent establishment[7]:

- using the office and equipment located in the state;
- location of personnel, including agents; and
- the possibility of local staff to conclude commercial transactions on behalf of the legal entity with counterparties in the territory of this state.

Access to the Internet site in the territory of a particular state, as well as the physical location of the servers, including nodes in the blockchain, should not lead ultimately to the formation of a permanent establishment, provided that there are no personnel in this country with the authority to enter into commercial

transactions on behalf of the organization[8].

For the purposes of addressing the permanent establishment question, the nodes in the Apla blockchain should be considered similary to the server owned and controlled by third parties and not the organizations carrying out the regulated activity.

With regard to the remote provision of services, the legislative practice of some states has developed the following two approaches on how to define targeting of the action[9]:

- a person is considered to be directing its activity at customers of a particular state if the **advertisement** of the company and its activities is available to customers in this state (customers have the opportunity to open the Internet site of the foreign provider of services); or
- a person is considered to be directing its activities at customers of a particular state if the **service** of the organization is available to customers in this state. According to this approach, there is no assumed targeting of the customers if the organization has taken the appropriate measures for limiting access to services by the customers in this state[10].

7. Canada 'Minister of National Revenue's Advisory Committee on Electronic Commerce (April 1998), s. 4.2.2.4.
8. For the purposes of the T&C, we used an approach applicable to online banking. See. Commission proposal for a European Parliament and Council directive on certain legal aspects of electronic commerce in the internal market COM, 98/0325 (COD), 12 CER para 7.5008 of the US bank regulation

9. Christ Reed «Internet Law», Second Edition, p. 244.
10. Chris Reed «Internet Law», Second Edition, pp 241-248. "This approach is partly accepted in the UK, USA, Australia, Canada. In this case, adequate in the UK are not considered measures that allow access to remote services through a simple verification of user absence of the country of residence without the technical verification of users' IP addresses site operator. In the US, adequate measures will be considered as a message on the website that an offer does not apply to residents of the United States with an indication of a particular jurisdiction and its orientation in conjunction with the requirement to disclose information about users of residential address and phone number outside the US".

18. Dispute Resolution

The parties shall use their reasonable efforts to resolve any dispute arising from or in connection with Apla Contractual Documentation by way of negotiations. If they don't reach an amicable settlement agreement within 5 months from the first notification of the claim, the dispute shall be finally settled under the Rules of arbitration of the Arbitration Center of the Luxembourg Chamber of Commerce by one arbitrator appointed in accordance with said rules. The language of arbitration shall be English.

19. Languages

This T&C and Apla Polices can be translated into any world languages. The official language, however, binding the parties hereto, shall be English.

Annex A. Apla Admission Policy

*This Apla Admission Policy **("Apla Admission Policy)** describes categories of users and criteria for admission of Apla Users to Apla Platform.*

Revision History

Version	Date	Approved by	Summary of Changes

1. General information

Apla is a Blockchain platform for building digital ecosystems operated by Supervised Financial Institutions. The platform includes an integrated development environment with a multi-level system for the management of access rights to data, interfaces, and smart contracts.

Apla Association does not engage in the provision of financial services or in other commercial activities. Apla Platform is not a money transfer platform. Nevertheless, the members of the association recognise the need and demand for building a fully compliant blockchain platform that meets the requirements of FATF in relation to AML/CFT compliance. This Apla Admission Policy has been designed with a view to meet those requirements and standards for the benefit of Apla blockchain community.

2. Categories of users

2.1. Apla Platform has got four categories of users:

2.1.1. Apla Users that are eligible to open APL Wallets to third parties **("Supervised Financial Institutions")**

2.1.2. Validating Nodes that are engaged in the execution of Apla Consensus Protocol

2.1.3. Apla Users that have APL Wallets opened with Supervised Financial Institutions **("APL Wallet Owner")** and

2.1.4. Apla Users that have become members of Apla Ecosystems created by APL Wallet Owners **("Apla Ecosystem Users")**

3. Supervised Financial Institutions

3.1. An eligible candidate to Supervised Financial Institution is either (i) an entity that is licensed or otherwise authorised by the financial market regulator in the country of its establishment to be engaged in payment services or (ii) an international, national or intergovernmental body or institution that engage in payment services, including central banks.

3.2. A candidate must become a member of Apla Association prior to obtaining a status of Supervised Financial Institution and have necessary licenses and permits to engage in the activities set forth in clause 2.1.1 of Apla Admission Policy. The list of Supervised Financial Institutions on Apla Platform is administrated by Apla Association.

3.3. The admission to membership in Apla Association and its cancellation are governed by by-laws of Apla Association.

3.4. If the membership of Supervised Financial Institution in Apla Association is cancelled for any reason, it will no longer be able to open new APL Wallets. In such a case, APL Wallets of the clients of the terminated institutions, including Apla Ecosystems created by such clients, will temporarily be suspended, except for the transfer of APL Tokens and re-assigning of Apla Ecosystems to new APL Wallets with another Supervised Financial Institution. The expenses connected with the transfer of APL Tokens to new APL Wallets and re-assigning Apla Ecosystems to new APL Wallets shall be borne by APL Wallet Owners affected by membership cancellation.

4. Validating Nodes

4.1. Supervised Financial Institutions are by default obtain the status of a Validating Node. The other eligible candidate is

either (i) an entity that is licensed or otherwise authorised in the country of its establishment to offer data centre services to third parties or (ii) an entity that has a valid agreement for data storage and other processing services with the entity indicated in point (i) above.

4.2. A candidate must become a member of Apla Association prior to obtaining a status of Validating Node. The list of Validating Nodes on Apla Platform is administrated by Apla Association.

4.3. The admission to membership in Apla Association and its cancellation are governed by by-laws of Apla Association.

5. APL Wallet Owners

5.1. APL Wallet Owner can be any natural person or legal entity, including international, national or intergovernmental body or institution.

5.2. Admission criteria for becoming APL Wallet Owner shall be determined by each Supervised Financial Institution for its own clients.

5.3. In order to open APL Wallet on Apla Platform, a candidate must enter into Private Contractual Arrangement with any Supervised Financial Institution and adhere to Apla Policies and other Apla Contractual Documentation.

5.4. APL Wallet Owner may create one or more Apla Ecosystems. It is the responsibility of APL Wallet Owner to ensure compliance of such Apla Ecosystems with Apla Contractual Documentation, Private Contractual Arrangements and Applicable Laws. In case of non-compliance, APL Wallet can be suspended by Supervised Financial Institution until the breach is remedied.

6. Apla Ecosystem Users

6.1. Apla Ecosystem User can be any natural person or legal entity, including international, national or intergovernmental body or institution.

6.2. Admission criteria for membership in Apla Ecosystem shall be determined by APL Wallet Owner who created such ecosystem.

6.3. In order to become Apla Ecosystem User, the candidate must enter into Private Contractual Arrangement with APL

Wallet Owner who created the respective Apla Ecosystem.

6.4. In case of a breach of Apla Contractual Documentation or Applicable Law by Apla Ecosystem User, the membership in the ecosystem of said user can be suspended by APL Wallet Owner who created the respective ecosystem until the breach is remedied.

7. Know-Your-Customer (KYC) procedure

7.1. General approach

Apla Association, Supervised Financial Institutions and APL Wallet Owners shall apply a risk-based approach prior to onboarding of respective users to Apla Platform. KYC requirements shall depend on a number of factors, including (i) user category, (ii) country risk (i.e., country membership in FATF), (iii) anticipated use of Apla Platform (eg., enhanced KYC is required if the user deploys Apla Platform for rendering financial or other regulated services) and (iv) applicable sanctions. For the avoidance of any doubt, the FATF Guidance to a Risk-Based Approach to Virtual Currencies (as to be amended from time to time) shall be applied by Eligible Persons to develop internal KYC and onboarding rules.

7.2. KYC Procedure for Onboarding of Supervised Financial Institutions and other Validating Nodes

7.2.1. A candidate must submit to Apla Association the following set of documents along with completed application form:

a) certified copy of the certificate of incorporation and by-laws;
b) certificate of good standing;
c) latest extract from commercial register;
d) certified copy of the license or other authorization from the relevant financial market regulator or other Public Authority;
e) tax certificate;
f) declaration of ownership;
g) list of shareholders and members of supervisory and executive bodies;
h) opinion of the reputable law firm from the country of establishment of the candidate confirming that the candidate complies with eligibility criteria set forth in clause 3.1 or 4.1 hereof;
i) internal admission policy for APL Wallet Owners;

j) certificate of conformation of information security management systems to the ISO/IEC 27001;
k) Information about server locations;
l) other documents requested by Apla Association.

7.2.2. All documents shall be provided to Apla Association with certified English translation.

7.2.3. Apla Association may outsource the process of onboarding of new members and KYC process to a selected law or audit firm.

7.2.4. After the receipt of the required documents by Apla Association, executive body shall within 30 working days review the submitted documents and make a decision on whether the candidate complies with the admission criteria or not. If a result of KYC and due diligence process is positive, the file is submitted to General Meeting of Apla Association for a final decision.

7.2.5. After the candidate has become the member of Apla Association, Board of Directors may at its sole discretion review the compliance of Supervised Financial Institution with the admission criteria at any time. Supervised Financial Institution shall provide the necessary documents and information to Board of Directors if requested.

7.3. KYC Procedure for Onboarding of APL Wallet Owners

7.3.1. Each Supervised Financial Institution shall develop its own internal admission policy applicable to APL Wallet Owners. It shall be in line with the general approach set forth in clause 7.1 hereof and admission criteria indicated in Article 5 hereof. For the avoidance of any doubt, prior to onboarding and opening APL Wallet, all APL Wallet Owners shall be identified by the respective Supervised Financial Institution.

7.4. KYC Procedure for Onboarding of Apla Ecosystem Users

7.4.1. Prior to creating Apla Ecosystem, each APL Wallet Owner shall develop and agree with Supervised Financial Institution administrating APL Wallet of such user, its own internal admission policy applicable to Apla Ecosystem Users. It shall be in line with the general approach set forth in clause 7.1 hereof and the admission criteria indicated

in Article 6 hereof. Depending on the level of compliance risk, APL Wallet Owners may choose either to identify the members of Apla Ecosystems which they create or not.

Annex B. Apla Compliance Policy

*This Apla Compliance Policy **("Compliance Policy")** describes AML/CFT compliance commitments of Apla Users*

Revision History

Version	Date	Approved by	Summary of Changes

1. General information

Apla is a Blockchain platform for building digital ecosystems operated by Supervised Financial Institutions. The platform includes an integrated development environment with a multi-level system for the management of access rights to data, interfaces, and smart contracts.

Although Apla Platform is not a money transfer platform, Apla Users recognise the need and demand for building a fully compliant blockchain platform that meets the requirements of FATF in relation to AML/CFT compliance standards. This Apla Compliance Policy was designed with a view to meet those requirements and standards for the benefits of Apla blockchain community.

2. AML/CFT compliance

2.1. AML/CFT compliance procedures include (i) KYC procedures applicable to Supervised Financial Institutions, APL Wallet Owners and Apla Ecosystem Users and (ii) on-going monitoring

and compliance control measures.

2.2. *KYC Procedures*

Supervised Financial Institutions, other Validating Nodes, APL Wallet Owners and Apla Ecosystem Users shall comply with the requirements of Apla Admission Policy (Article 7) in relation to KYC procedures during client onboarding process.

2.3. *On-going monitoring and control by Supervised Financial Institutions*

2.3.1. Supervised Financial Institutions shall apply a risk-based approach to on-going monitoring and control of the transactions with APL Tokens by APL Wallet Owners. The level of control may depend on a number of factors, including (i) user category, (ii) the country risk (i.e., country membership in FATF), (iii) type of the transaction with APL Tokens and (iv) applicable sanctions. The FATF Guidance to a Risk-Based Approach to Virtual Currencies (as to be amended from time to time)[11] shall be applied by Supervised Financial Institutions to develop internal on-going compliance monitoring rules.

11. http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

2.3.2. A low-risk transaction with APL Tokens may be the remittance of APL Tokens by APL Wallet Owner to Supervised Financial Institution as a means of payment of the license fee for each transaction in Apla Platform initiated by APL Wallet Owner and/ or generated by a member of Apla Ecosystem created by APL Wallet Owner. Low-risk transactions do not have to be subject to enhanced ongoing monitoring and control.

2.3.3. Unless it is provided for differently by Supervised Financial Institution, a high-risk transaction with APL Tokens is the remittance of APL Tokens from one Wallet to another Wallet if none of the said Wallets are owned by Supervised Financial Institutions.

2.4. On-going monitoring and control by APL Wallet Owners

2.4.1. If APL Wallet Owner creates Apla Ecosystem, he/ she/it shall apply or ensure the application by a third party licensed institution of a risk-based approach to on-going monitoring and control of the transactions of Apla Ecosystem Users with Tokens generated by the respective Apla Ecosystem. The level of control may depend on

a number of factors, including (i) user category, (ii) the country risk (i.e., country membership in FATF), (iii) type of the transaction and category of Tokens and (iv) applicable sanctions. The FATF Guidance to a Risk-Based Approach to Virtual Currencies (as to be amended from time to time) shall be applied by APL Wallet Owners to develop internal on-going monitoring rules.

2.4.2 The approach to monitoring the low-risk and high-risk transactions can be similar to the one of Supervised Financial Institutions.

3. Compliance with Laws

3.1. Supervised Financial Institutions, APL Wallet Owners and Apla Ecosystem Users shall use Apla Platform for the activities that are not breaching Apla Contractual Documentation, Private Contractual Arrangements and are not regarded by Applicable Laws as illegal, illicit or fraudulent.

3.2. The commercial activity relating to organising the exchange of and/or trading with APL Tokens, including issue of and/or trading with any derivative instruments linked to APL Tokens, may only be conducted by Supervised Financial Institutions.

3.3. Apla Ecosystems may generate their own tokens and Wallets. Said tokens may legally be qualified as securities, financial instruments, loyalty tokens, etc., depending on the jurisdiction and specifics of the ecosystem and tokens. APL Wallet Owners shall ensure and be fully responsible for the compliance of Apla Ecosystems created by them and generated tokens by such ecosystems with Applicable Laws, Apla Contractual Documentation and commitments of APL Wallet Owners under Private Contractual Arrangements.

3.4. In no case Apla Platform can be used for any of the following activities:

- Money laundering and financing of terrorism as defined by the United Nation Conventions and Applicable Laws;
- Drugs and/or human trafficking;
- Other criminal activities defined as such by Applicable Laws.

4. Compliance Ombudsman

4.1. Apla Association shall appoint a law or audit firm to perform the function of Compliance Ombudsman.

4.2. The Compliance Ombudsman is appointed for a period of 3 years.

4.3. Compliance Ombudsman shall be entitled to (i) receive compliance related claims from all categories of Apla Users, (ii) initiate investigations as a result of such claims, (iii) instruct the relevant Supervised Financial Institutions to take legal actions against the users breaching the present Apla Compliance Policy, including suspension of their APL Wallets and making a reporting to Public Authorities, if required under Applicable Laws.

4.4. The investigations and handling of claims shall be governed by the Laws of the country where the Compliance Ombudsman is licensed and/or authorised to engage in the activity.

5. Non-compliance with this policy

5.1. If Apla Compliance Policy is breached by Supervised Financial Institution or other Validating Node, the latter will be given a 30-day period to remedy the breach. If the breach is still not remedied, the membership of Supervised Financial Institution or other Validating Node in Apla Association may be terminated by General Meeting of Apla Association.

5.2. If Apla Compliance Policy is breached by APL Wallet Owner, Supervised Financial Institution opened the respective APL Wallet to APL Wallet Owner, may either give a 30-day period to APL Wallet Owner to remedy the breach or suspend APL Wallet of such user until the breach is remedied. If the breach is still not remedied within a given period of time, APL Wallet of APL Wallet Owner in breach may be closed in accordance with the contractual arrangements between the parties.

5.3. If Apla Compliance Policy is breached by Apla Ecosystem User, APL Wallet Owner who created the relevant Apla Ecosystem, may either give a 30-day period to Apla Ecosystem User to remedy the breach or suspend membership in Apla Ecosystem until the breach is remedied. If the breach is still

not remedied within a given period of time, membership or Wallet of Apla Ecosystem User in breach may be terminated in accordance with the contractual arrangements between the parties.

Annex C. Apla Data Protection Policy

This Apla data protection and secrecy policy ***("Apla Data Protection Policy")*** *sets out the roles and responsibilities of Apla Users in connection with protecting personal and other data of the other Apla Users and third parties in the course of using Apla Platform.*

Revision History

Version	Date	Approved by	Summary of Changes

1. Introduction

Apla is a Blockchain platform for building digital ecosystems operated by Supervised Financial Institutions. The platform includes an integrated development environment with a multi-level system for the management of access rights to data, interfaces, and smart contracts.

Apla Platform is not a money transfer platform. Nevertheless, Apla Users recognise the need and demand for building a fully compliant blockchain platform that meets the requirements of applicable laws and regulation in the area of data security and personal data protection. This Data Protection Policy has been designed with a view to meet those requirements and standards for the benefits of the Apla blockchain community.

Apla Association, Supervised Financial Institutions and other Validating Nodes, APL Wallet Owners and Apla Ecosystem Users ("Apla Users") deploy the software, processing, storage and other elements of Apla Platform to develop applications and execute smart contracts and smart laws. It may happen

that certain Apla Users may get access to and make use of a variety of data about identifiable living individuals. This includes the data collected by Apla Users for the purposes of KYC/CFT compliance and admission of a user to the Apla Platform.

In collecting and using these data, Apla Users may be subject to the Laws of different jurisdictions controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

This policy applies to all systems, people and processes that constitute the information systems of Apla User, including board members, directors, employees, suppliers and other third parties who have access to the Apla User's systems.

The following policies and procedures are relevant to this document:

- Information Security Incident Response Procedure;
- Roles, Responsibilities and Authorities;
- Data Breach Notification Procedure.

2. Data Protection Policy

2.1. Application of this policy

Apla Users shall adhere to the requirements of this policy in so far as they act as administrators, users, data controllers or data processors in accordance with Schedules 1 and 2 hereto. If the indicated Apla Users develop their internal data protection policies, the latter shall not contradict with this policy.

The purpose of this policy is to set out the relevant standard and to describe the steps Apla Users must take to ensure that they comply with it. It is based on the General Data Protection Regulation of the European Union 2016 **("GDPR")**, that is regarded as one of the most comprehensive and data subject protective industry standard worldwide. If the Law applicable to a specific Apla User implies the application of additional requirements, the compliance with those requirements must be the responsibility of the respective Apla User.

Furthermore, each Apla User must assess individually whether the requirements of the GDPR and this policy comply with the Laws applicable to such user. In case of a contradiction, the

respective user must terminate or suspend the use of Apla Platform until and if the policy has been adjusted to the Laws applicable to the specific Apla User.

2.2. Definitions

There are a total of 26 definitions listed within the GDPR that are to be considered as a part of this policy. The most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

'processing' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

'controller' means:
the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

2.3. Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR and this policy are based and which shall be complied

with by all Apla Users.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('Walletability').
Apla Users must ensure that they comply with all of these principles both in the processing they carry out and as part of the introduction of new methods of processing such as new IT systems.

The information security management systems of Supervised Financial Institutions and other Validating Nodes, which are in charge of forming blocks and storage of the full version of Apla Blockchain, shall conform to the ISO/IEC 27001 international standard as a key part of their commitment to the other Apla Users.

2.4 Rights of the data subjects

2.4.1. The data subject also has rights under this policy. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The responsibility of each Apla User for realisation of the above-mentioned rights of a specific data subject shall be defined on the basis of the roles and responsibilities set forth in Schedule 2 hereto.

Each of these rights must be supported by appropriate procedures within organisation of Apla User that allow the required action to be taken within the timescales as provided in the table below:

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Placement of non-anonymised and/or non-pseudo-anonymised personal data in Apla Platform is not allowed under this policy. Nevertheless, it may happen accidently or otherwise in breach of this policy. If this happens and personal data has been added to Apla Ecosystem, the data controller of the specific ecosystem shall immediately upon having received a request from its counterparty (eg., from a client of Supervised Financial Institution or client of APL Wallet Owner) generate the smart contract in the form pre-validated by Apla Association to erase the data concerned from the specific ecosystem. The generated smart contract will have to be validated by all Supervised Financial Institutions and other Validating Nodes. The erasure of the personal data will be executed in the form of restricting access to the data concerned to all Apla Users so that it becomes invisible to them. The data controllers and Validating Nodes will have a right to object to erasure of the personal data on the grounds set forth by the GDPR.

If the request to erase the personal data relates to the public key (Wallet) of a natural person and Apla transactions attributable to this public key, the same procedure as described above shall be applicable to restricting access of Apla Users to this information.

2.5. Consent

Unless it is necessary for a reason allowable in the policy, explicit consent must be obtained from a data subject to collect and process their personal data. In case of children below the age of 16 parental consent must be obtained. Transparent information about usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.
If the personal data are not obtained directly from the data subject then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

The responsibility of each Apla User for obtaining a consent of a specific data subject shall be defined on the basis of the roles and responsibilities set forth in Schedules 1 and 2 hereto. Each Apla Ecosystem generating public keys of the users must maintain a register of consents of the owners of the public keys in Apla Platform.

2.6. Privacy by Design

Apla Users shall adhere to the principle of privacy by design and ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

None of the Apla Users shall be entitled to store and/or allow storage of personal data of any natural person in any of the data base forming part of Apla Platform, except for those data that is secured with the use of the anonymization technology approved by Apla Association (i.e., certain types of cryptography). Supervised Financial Institutions and APL Wallet Owners that create Apla Ecosystems shall include the respective contractual clause in their agreements with the counterparties before authorising the admission of new users to Apla Platform. Failure to comply with the above-mentioned prohibition shall entail the immediate restriction of the user in breach to Apla Platform.

As a possible solution for using the Apla systems for the processing of personal data, Apla source code allows for the creation of Virtual Dedicated Ecosystems (VDE), which have the full set of functions of standard ecosystems, but work outside the blockchain. VDE can be used for the creation of registration forms and sending verification information to users' emails or phones and storing personal data out of public access.

Public Keys of a natural person can be in some cases treated as personal data if they may help identifying such natural person. Depending on access rights, public keys of APL Wallet Owners and Apla Ecosystem Users will be visible to and electronically stored on the computer devices of certain categories of Apla Users. The data controllers must ensure that the data subjects explicitly agree to the processing of their public keys by another Apla Users, including the transfer of this data and its storage outside of the country of residence of the data subject. The responsibility for obtaining such a consent from a new user shall be with a Supervised Financial Institution or APL Wallet Owner authorising the access of a specific APL Wallet Owner or Apla Ecosystem User to Apla Platform.

2.7. Transfer of Data

Pubic keys of the users and the other data placed by the users in

various data bases of Apla Platform will electronically be stored on the computer devices of Apla Users that have got access rights to the specific ecosystem of Apla Platform. Considering the fact that the computer devices of Apla Users may be located anywhere in the world, the users must be aware of the risks and explicitly agree to the transfers to and/or distributed storage of their data on the devices of the other Apla Users regardless of their location. Each Apla ecosystem generating public keys of the users must maintain a register of consents of the owners of the public keys in Apla Platform.
The current policy and data protection measures must be complied with by all Apla Users to ensure that they fall within the limits imposed by the GDPR and this policy.

2.8. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR and this policy for all Validating Nodes and Apla Association. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

A DPO shall be appointed by APL Wallet Owners and Apla Ecosystem Users if it's required by the GDPR.

2.9. Breach Notification

It is Apla Users' policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal and other data. In line with the GDPR and this policy, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals and controllers' counterparties, the relevant Data Protection Authority (DPA) will have to be informed within 72 hours by a data controller in charge. This is to be managed in accordance with the Apla Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

2.10. Addressing Compliance with the policy

The following actions shall be undertaken to ensure that Apla User complies at all times with the Walletability principle of the GDPR and this policy:

- The legal basis for processing personal and other data is

clear and unambiguous;

• A Data Protection Officer is appointed, where required, with specific responsibility for data protection in the organization;

• All staff involved in handling personal and other data understand their responsibilities for following good data protection practice;

• Training in data protection has been provided to all staff;

• Rules regarding consent are followed;

• Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively;

• Regular reviews of procedures involving personal and other data are carried out;

• Privacy by design is adopted for all new or changed systems and processes;

• The following documentation of processing activities is recorded:

  • Organization name and relevant details

  • Purposes of the personal and other data processing

  • Categories of individuals and personal and other data processed

  • Categories of personal and other data recipients

  • Personal data retention schedules

  • Relevant technical and organisational controls in place

These actions shall be reviewed on a regular basis as part of the management review process of the information security management system.

Schedule 1

Apla Platform Access Rights

Apla blockchain platform consist of a number of ecosystems that have been created and/ or will be created by Apla Users. The type of data contained in each ecosystem is to be determined by the administrator of the respective Apla environment.

Apla Users will have either the rights of an administrator or user in relation to the data stored in the Apla ecosystems (i.e., an administrator or user).

The rights of an administrator include any of the following:

• Creating an ecosystem;

• Defining admission and usage rights of the ecosystem (smart laws);

• Issuing public and private keys to the members of the ecosystem and creating Wallets for them if internal tokens are generated by the ecosystem;

• Validating the source code of interfaces of the ecosystem;

• Validating the source code of smart contracts of the ecosystem;

• Validating access to the ecosystem (smart contracts) in accordance with pre-defined rules;

• Restricting/removing access to the ecosystem to new and existing users in accordance with pre-defined rules;

• Viewing the information stored in the data base of the ecosystem;

• Storage of the data forming part of the ecosystem on a computer device that is owned by the administrator or owned by a third part but is kept under the control of the administrator in accordance with the contractual arrangement between the administrator and such third party.

The rights of an user include and of the following:

• Getting access to the Wallet of the user, interfaces and other

data of the ecosystem by electronic means within the limits determined by the administrator of the ecosystem;

• Generating smart contracts in the respective ecosystem within the limits set forth by the administrator;

• Viewing the information stored in the data base of the ecosystem;

• Other rights assigned by the administrator of the ecosystem;

• Storage of the data pertaining to the ecosystem on a computer device that (i) is owned by the user or (ii) owned by a third part but is kept under the control of the administrator in accordance with the contractual arrangement between the administrator and such third party.

The below table contains information on specific data bases (ecosystems) and access rights of different categories of platform users:

№	Apla User category	Access right	Apla platform data base
1	Apla Association	Administrator	Ecosystem with a list of Supervised Financial Institutions and other Validating Nodes
2	Supervised Financial Institution	User Administrator (in relation to clients of each institution) User	Ecosystem with a list of Supervised Financial Institutions and other Validating Nodes Ecosystem with a list of APL Wallet Owners and transactions with APL Tokens Other Apla ecosystems
3	Validating Nodes other than Supervised Financial Institutions	User User User	Ecosystem with a list of Supervised Financial Institutions and other Validating Nodes Ecosystem with a list of APL Wallet Owners and transactions with APL Tokens Other Apla ecosystems

№	Apla User category	Access right	Apla platform data base
4	APL Wallet Owner	User	Ecosystem with a list of Supervised Financial Institutions and other Validating Nodes
		User	Ecosystem with a list of APL Wallet Owners and transactions with APL Tokens
		Administrator	Ecosystem created by the APL Wallet Owner
		No access rights by default	Ecosystem created by another APL Wallet Owner
5	Apla Ecosystem User	User	Ecosystem with a list of Supervised Financial Institutions and other Validating Nodes
		No access rights	Ecosystem with a list of APL Wallet Owners and transactions with APL Tokens
		User	Apla Ecosystem with membership rights
		No access rights by default	Apla Ecosystem with no membership rights

Schedule 2

Users' Data Processing Roles and Responsibilities

1. Data controller and data processor functions

Each user of Apla Platform is assigned with the function of a data controller and/or data processor depending on his/her/its status, role and access rights to the specific ecosystem.

№	Apla User category	Data Controller	Data Processor Function
1	Apla Association	Defining the scope and processing means of KYC/ Admission information and documents for Supervised Financial Institutions and other Validating Nodes Defining the scope and processing means of the data in the course of handling specific data protection claims and security issues raised by Supervised Financial Institutions Defining the scope and processing means of the data included in the smart contracts/smart laws generated by Apla Association	Collection and storage in a paper and electronic form of information and documents relating to Supervised Financial Institutions and other Validating Nodes, including data protection officers, other officers, board members and beneficiaries Executing the rights of the administrator of the ecosystem with a list of Supervised Financial Institutions Collection and storage of data relating to specific Apla Users for the purposes of handling specific data protection and platform security issues, including personal data of natural persons affected by such issues, transfer of such data to supervisory authorities and Supervised Financial Institutions to the extent required by the applicable law and this policy
2	Supervised Financial Institution	Defining the scope and processing means of KYC/Admission information and documents for APL Wallet Owners (APL Wallet holders) Defining the scope and processing means of the data in the course of on-going AML/CFT compliance monitoring of transactions of the clients of Supervised Financial Institutions with APL Tokens (APL Wallet Owners) Defining the scope and processing means of the data in the course of handling specific data protection claims and security issues raised by the clients of such Supervised Financial Institutions (APL Wallet Owners) Defining the scope and processing means of the data included in the smart contracts/smart laws generated by the Supervised Financial Institution	Electronic storage of data of all Apla ecosystems Blocks formation and transactions validation in accordance with the Apla Consensus Protocol Collection and storage of information and documents relating APL Wallet Owners, including data protection officers, other officers, board members and beneficiaries for on-boarding of such users to Apla Platform Collection and storage of data relating to specific APL Wallet Owners and Apla Ecosystem Users for the purposes of handling specific data protection and platform security issues, including personal data of natural persons affected by such issues, transfer of such data to supervisory authorities and Apla Association to the extend required by the applicable law and this policy Executing the other rights of the administrator or user of the respective ecosystem

№	Apla User category	Data Controller	Data Processor Function
3	Validating Node other than Supervised Financial Institution	None	Electronic storage of data of all Apla ecosystems Blocks formation and transactions validation in accordance with Apla Consensus Protocol Collection and storage of data relating to specific APL Wallet Owners and Apla Ecosystem Users for the purposes of handling specific data protection and platform security issues, including personal data of natural persons affected by such issues, transfer of such data to supervisory authorities and Apla Association to the extend required by the applicable law and this policy Executing the other rights of the user of the respective ecosystem
4	Apla Ecosystem User	To be further defined by Data Protection Policy of the Ecosystem	Electronic storage of the data of the ecosystems to which the Apla Ecosystem user has got access rights

№	Apla User category	Data Controller	Data Processor Function
5	APL Wallet Owner	Defining the scope and processing means of KYC/Admission information and documents for Apla Ecosystem Users if such ecosystem is created by the APL Wallet Owner Defining the scope and processing means of the data in the course of on-going AML/CFT compliance monitoring of transactions of Apla Ecosystem Users if such ecosystem is created by the APL Wallet Owner Defining the scope and processing means of the data in the course of handling specific data protection claims and security issues raised by the members of the Apla Ecosystems created by the APL Wallet Owner Defining the scope and processing means of the data included in the smart contracts/smart laws generated by the APL Wallet Owner	Electronic storage of the data base of the ecosystem to which the APL Wallet Owner has got access rights Collection and storage of information and documents relating Apla Ecosystem Users if ecosystem is created by the APL Wallet Owner, including data protection officers, other officers, board members and beneficiaries for on-boarding of such Apla Ecosystem users to the Apla platform Collection and storage of data relating to specific Apla Ecosystem Users (for ecosystems created by the APL Wallet Owner) for the purposes of handling specific data protection and platform security issues, including personal data of natural persons affected by such issues, transfer of such data to supervisory authorities and respective Apla Users to the extend required by the applicable law and this policy

2. Responsibilities of data controller

2.1. In so far as the processing of personal data is concerned, the data controller shall owe the following duties towards his direct contracting parties and data subjects whose personal data will and/or has been collected upon a request of such data controller:

2.1.1. Compliance with the principles of the personal data processing set forth in clause 3.3 of the Data Protection Policy;

2.1.2. Electronic storage of the personal data off Apla Platform, except for the public keys and personal data that has been secured with the use of anonymization or pseudo-anonymization technologies approved by the Apla association;

2.1.3. Realisation of the data subject rights set forth in the Apla Data Protection Policy;

2.1.4. Obtaining explicit consent of the data subject on processing/and/or transfer of personal data;

2.1.5. Data breach notifications to the authorities supervising the data controller;

2.1.6. Other duties attributable to the controller under the GDPR rules.

2.2. In so far as the processing of non-personal data is concerned, the data controller shall owe the following duties towards his direct contracting parties:

2.2.1. Not to use and not to disclose any of the data and documents received from the existing or potential users by the controller, except for the purposes of executing the KYC/Admission procedure and on-going AML/CFT monitoring process.

Specifically, the controllers agree not to, directly or indirectly, (i) use any of the received information and documents for any purpose except to evaluate and engage in discussions and contractual relationship and carry out on-going business processes concerning the use of Apla Platform, (ii) divulge or disclose any of the received information and documents to third parties, or (iii) permit any of the received information

and documents to be divulged or disclosed to or examined or copied by any third party; provided, however, that the data controller may disclose the received information and documents to its employees, agents, representatives, assignees or subcontractors on a «need to know» basis (each such person, a ***«Permitted Disclosee»***). The controller will (i) inform each Permitted Disclosee of the requirements of this arrangement, (ii) ensure that each Permitted Disclosee complies with the controller's non-disclosure obligations, as set forth herein, and (iii) obtain written agreements from each Permitted Disclosee requiring such Permitted Disclosee to abide by the requirements set forth herein.

2.2.2. The controller shall take all reasonable measures necessary to protect the secrecy and confidentiality of the information received from the disclosing party.

2.2.3. The obligation of the controller not to disclose and not to misuse the information and documents received from the counterparty shall not apply in case the controller is obliged to disclose these information and documents to supervisory and other governmental authorities in accordance with Applicable Law.

2.2.4. Data breach notifications to the authorities supervising the data controller and its contractual parties, if required by Applicable Law.

2.2.5. After the termination of the contractual relationship, all documents submitted by the client of the controller, including all copies, embodiments or derivatives thereof that are in the possession of the controller, shall be promptly returned to the client upon written request. For the avoidance of any doubt, certain controllers (eg., Supervised Financial Institutions) have the obligation to maintain records of their relationships with the clients during a certain period of time under the applicable Law. If it is required by the applicable Law, the controllers may keep received documents and information in their possession to comply with statutory requirements.

2.3. As regards the data being processed by the data controller in Apla Platform, the controller shall not be responsible for the secrecy and disclosure of this data to the other Apla Users that have got access rights to the data contained in the specific Apla ecosystems.

3. Responsibilities of data processor

3.1. A Validating Node that processes the data for the purposes of the execution of Apla Consensus Protocol and electronic storage of the data contained in Apla ecosystems, shall owe the following duties towards the other Apla Users:

3.1.1. Validating Nodes may use the data that has been received by them from the other Apla Users and/or to which they have got access to in the course of execution of the Apla Consensus Protocol, including electronic storage of the data contained in any ecosystem of Apla Platform, only for the purposes directly connected with the listed activities.

3.1.2. Validating Nodes shall take all reasonable measures necessary to protect the secrecy and confidentiality of the data being processed. This does not apply to the disclosure of the data to a Permitted Disclosee on the conditions set forth in clause 2.2.1 hereof and disclosure of such data to the other Apla Users that have got access rights to the specific ecosystem.

3.1.3. In case of termination or cancellation of its access rights as an administrator and/or processor for any reason, the Validating Node shall without undue delay delete the data from its IT systems that has been processed by it in connection with the terminated administrator's and/or processor's rights. If it is required by the applicable Law, Validating Node may not delete this data for as long as it is required to comply with statutory requirements.

3.2. An APL Wallet Owner or Apla Ecosystem User that store the data on their computer devices, shall owe the following duties towards the other Apla Users:

3.2.1. APL Wallet Owner or Apla Ecosystem User may use the data of the other Apla Users to which they've got access to only for the purposes directly connected with the storage of such data on their computer devices and/or other legitimate purposes consented by the ecosystem owners.

3.2.2. An APL Wallet Owner or Apla Ecosystem shall take all reasonable measures necessary to protect the secrecy and confidentiality of the data being processed. This does not apply to the disclosure of the data to a Permitted Disclosee on the conditions set forth in clause 2.2.1 hereof

and disclosure of such data to the other Apla Users that have got access rights to the specific ecosystem.

3.2.3. In case of termination or cancellation of the access rights as an administrator and/or processor for any reason, the respective APL Wallet Owner or Apla Ecosystem shall without undue delay delete all the data from its IT systems that have been processed by them if this data is attributable to the terminated administrator's and/or processor's rights. If it is required by the applicable Law, the APL Wallet Owner or Apla Ecosystem User may not delete this data for as long as it is required to comply with statutory requirements.

Annex D. Apla Information Security Incidents Procedure

This Apla Information security incidents procedure ***("Apla Information Security Incidents Response Procedure")*** *sets out the rules and guidance to responding to an information security incident and coordinating the activities of Apla Users in this regard.*

Revision History

Version	Date	Approved by	Summary of Changes

1. Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of any of Apla Ecosystem, including those potentially affecting personal and other data for which Apla User is a controller. It is intended to ensure a quick, effective and orderly response to an information security breach.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

• provide a concise overview of how Apla User shall respond to an incident;

• set out who shall respond to an incident and their roles and responsibilities;

• describe the facilities that are in place to help with the management of the incident;
• define how decisions shall be taken with regard to a response to an incident;

• explain how communication within Apla Users network and with external parties will be handled;

• define what will happen once the incident is resolved and the responders are stood down.

All personal information collected as part of the incident response procedure and contained in this document shall be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

2. Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.

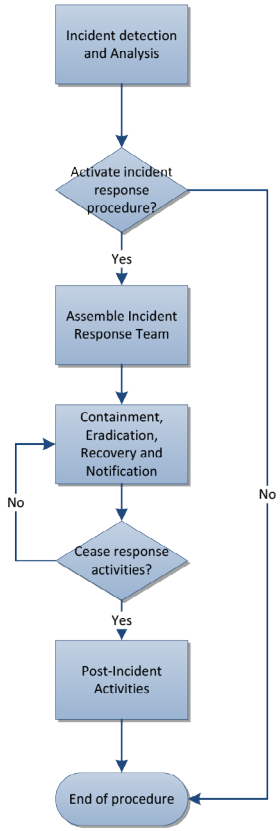

Figure 1 – Incident response flowchart

These steps are explained in more detail in the rest of this procedure.

3. Incident Detection and Analysis

An incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within an organisation of Apla User or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of a proactive approach to information security is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment must be carried out by a data controller in charge in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation;
- The information assets (including personal data) that may be at risk or have been compromised;
- The likely duration of the incident i.e. when it may have begun;
- The ecosystems and the extent of the impact to them;
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects;
- Initial indication of the likely cause of the incident.

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data),

business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

4. Activating the Incident Response Procedure

As a result of this initial analysis, a DPO of the data controller or an executive body of the data controller if no DPO has been appointed ("Team Leader") has the authority to decide whether the Incident Response Procedure should be activated. If more than one data controller is responsible for making a decision on activation of the specific incident response procedure, a DPO of Apla Association shall act as Team Leader and coordinate the actions of the team members of the other data controllers affected by the incident.

Guidelines for whether a formal incident response should be initiated for any particular incident of which the Team Leader has been notified are if any of the following apply:

- There is significant actual or potential loss or changes of classified information, including personal data in any of Apla Ecosystem for which Apla User acts as a data controller;

- The incident may affect the accuracy of information stored in the data base with a list of Supervised Financial Institutions and other Validating Nodes and data base with APL Tokens and transactions with APL Tokens;

- There is significant actual or potential disruption to business operations;

- There is significant risk to business reputation of Apla User and Apla Platform in general;

- Any other situation which may cause significant impact to the organization.

In the event of disagreement or uncertainty about whether or not to activate an incident response the Team Leader shall consult with the DPO of Apla Association.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower level response to the incident within normal management channels.

If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

5. Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) must ensure that the DPO of Apla Association and the Data Security Officer of EGAAS are involved in the IRT if the incident relates to the source code of the Apla blockchain platform, smart-contract or smart-law. If DPO of Apla Association acts as a Team Leader, the DPOs of data controllers affected by the incident shall be appointed as his/her deputies.

The below contact details shall be used to contact the DPO of the Apla Association and Data Security Officer (DSO) of EGAAS:

5.1. Incident Response Team Members

The Incident Response Team will generally consist of the following people in the roles specified and with the stated deputies, although the exact make-up of the team will vary according to the nature of the incident.

Role/Business Area	Main role holder	Deputy
Team Leader		
Team Facilitator		
Information Technology		
Business Operations		
Communications (PR and Media Relations)		
Legal and Regulatory		
DPO of Apla Association		
DSO of EGAAS		

Table 1 – Incident response team members

5.2. Roles and Responsibilities

The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides whether or not to initiate a response

- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement

Team Facilitator

- Supports the incident response team
- Co-ordinates resources within the command centre
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command centre
- Facilitates communication via email, fax, telephone or other methods
- Monitors external information feeds such as news Information Technology
- Provides input on technology-related issues
- Assists with impact assessment

Business Operations

- Contributes to decision-making based on knowledge of business operations, products and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization

Communications (PR and Media Relations)

- Responsible for ensuring internal communications are effective

• Decides the level, frequency and content of communications with external parties such as the media

• Defines approach to keeping affected parties informed e.g. customers, shareholders

Legal and Regulatory

• Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks

• Assesses the actual and potential legal implications of the incident and subsequent actions

DPO of Apla Association

• Responsible for ensuring communications with Supervised Financial Institutions are effective where necessary

• Contributes to decision-making based on knowledge of IT Systems of Supervised Financial Institutions

DSO of EGAAS

• Provides input on technology-related issues in connection with the operation of the Apla blockchain platform in general

• Assists with impact assessment

5.3. Incident Management, Monitoring and Communication

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minuted by the Team Facilitator.

5.4. Communication Procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, both landline and mobile. Email should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
    - Ask if the contact is available elsewhere
    - If they cannot be contacted leave a message to contact you on a given number
    - Do not provide details of the Incident
- Always document call time details, responses and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action at a later date.

5.4.1. Communication to the Data Protection Supervisory Authority

It is a requirement of the GDPR that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. The Apla Personal Data Breach Notification Procedure must be used for this purpose. In the event that the 72-hour target is not met, reasons for the delay must be given.

5.4.2. Communication with Personal Data Subjects

Where an incident affects personal data, a decision must be taken by the IRT regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".

The Apla Personal Data Breach Notification Procedure must be used for this purpose.

5.4.3. Other External Communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact. These may include:

- Customers;
- Suppliers;
- Shareholders;
- Regulatory bodies.

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

5.4.4. Communication with the Media

In general the communication strategy with respect to the media will be to issue updates via top management. No members of staff of Apla User should give an interview with the media unless this is pre-authorised by the IRT.
The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media the following guidelines

should be observed:

• Personal information should be protected at all times

• Stick to the facts and do not speculate about the incident or its cause

• Ensure legal advice is obtained prior to any statements being issued

The following members of staff will be appointed spokespeople for the organization if further information is to be issued e.g. at a press conference.

6. Incident Containment, Eradication, Recovery and Notification

6.1. Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting and/or restricting access the affected parts of the network, including Wallets; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g. by waking up a laptop. It is recommended that specialist advice should be obtained at this point.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines.
The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional

circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g. time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene.

Principle 4 – The person in charge must ensure that the guidelines are followed.

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

6.2. Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes require the updates of the source code of Apla Platform and affected smart-contracts. If it is necessary, such updates may be proposed to Apla Association by any Apla User. The proposed updates have to be installed by Apla User if they are voted for by 75 % of the Supervised Financial Institutions included in the data base of Supervised Financial Institutions.

6.3. Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that

were exploited as part of the incident.

If the incident has affected the accuracy of the data stored in any of the ecosystems, Apla Platform source code deploys the smart-laws mechanism whereby Supervised Financial Institutions and other Validating Nodes may vote to restore the data to the pre-incident condition without the need of creating a fork of the blockchain. In this case, the recovery smart-contract is generated by the DPO of Apla Association. This smart-contract is to be validated by at least 75 % of the Validating Nodes included in the data base of Validating Nodes.

6.4. Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

Apla Users acting as data controllers during the incident response procedure shall always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and the Apla user concerned shall cooperate in full with such proceedings.

Annex E. Apla Consensus Protocol

This Apla consensus protocol ***("Apla Consensus Protocol")*** *describes transaction validation and block formation procedure by Validating Nodes in Apla Platform.*

Revision History

Version	Date	Approved by	Summary of Changes

1. Introduction

This document sets out an overview of the Apla consensus protocol. By getting access to Apla Platform, Apla User shall be assumed to review and agree to the transaction processing and validation procedures described below.

2. Network

Apla Platform is built based on a peer-to-peer network. Full nodes of the network (i.e., Validating Nodes) store the up-to-date version of Apla Blockchain and the database, in which the current state of the platform is recorded. The network users receive data by requesting it from databases of Validating Nodes using the software client (or REST AP commands). New data is sent to the network in the form of transactions signed by Apla Community members. Such transactions are in essence commands for modification of information in the database. Transactions are aggregated in blocks, which are then added to the blockchain on the network nodes. After a new block is added to the blockchain, each Validating Node processes the

transactions in this block, thus making changes to data in its database accordingly.

3. Generation of new blocks

Supervised Financial Institutions and other Validating Nodes have the right to generate new blocks. The number of Validating Nodes is limited and is defined with the count_of_nodes parameter in the platform's configuration settings.

The list of Validating Nodes is stored in the full_nodes parameter in the following format:
[["host1:port»,"-1222»,»nodepub1»], [«host2:ip»,»-1222», «nodepub2»]], where

host1:port – is the address of the host, to which the transactions and new blocks are sent; also, the whole chain of blocks (starting from block #1) can be requested and received from this address

-1222 – the node's Wallet to which the fee for transaction processing is sent; if this Wallet does not exist, the fee will not be charged
nodepub1 – the node's public key used for verification of signatures of blocks, created by this node

Validating nodes form and sign blocks subsequently one after another in accordance with a sequence list, in time intervals set in the gap_between_blocks parameter (one second, by default). If a validating node was not able to create a block in the allotted time, the right to sign a new block is passed to the next validating node in the list.

4. Transactions

A transaction is formed by the software client (or by the contract REST API command) and includes data for execution of a special program controller – contract («smart contract»), called by an Apla User. Each transaction has the following format:

Type	ID of the executed contract
Data	Parameters passed to the contract
KeyID	ID of the user who sent the transaction
PublicKey	User's public key (optional)
BinSignatures	Transaction signature
Time	Transaction timestamp

EcosystemID	ID of the ecosystem, where the transaction was initiated
TokenEcosystem	ID of the ecosystem, the tokens of which should be used for the transaction payments
MaxSum	Maximum transaction fee
PayOver	Additional payment for priority processing in the transaction queue

A transaction is signed by the private key of an Wallet holder. Both the key and the signing function can be stored in a browser, in the software client, on a SIM card, or on a specialized physical device. In the current implementation, private keys are kept in the Molis software client encrypted by the AES algorithm. Transactions are signed using the ECDSA algorithm.

5. Network Protocol

A transaction is sent by Apla User to one of the validating nodes, where it undergoes a basic verification to ensure the correctness of its format and then is added to the transaction queue. This transaction is also sent to other validating nodes on the network, where it's also added to the transactions queue.

The validating node, at a particular moment of time that has the right to generate a new block (according to the full_nodes parameter), retrieves transactions from the queue and sends them to the block generator. Simultaneously with the formation of a new block, the processing of transactions which are added to this block is carried out: each transaction is sent to the virtual machine that executes a corresponding contract with parameters, passed in the transaction, resulting in modification of the information in the database.

A new block is checked for errors, and if it is recognized as valid, it is sent to other validating nodes on the network.
Validating nodes add this newly received block to the blocks queue. After having been validated, a new block is added to the blockchain, and the transactions in this block are processed, thus updating the database.

6. Block and Transaction Verification

The verification of a new block, carried out by a validating node after it has created a new block, and the verification of such block on all other validating nodes after they receive this block, includes the following checks:

• The first byte should be 0; if not, the received data is not considered a block;

• Received block's generation timestamp should be before the current time;

• The block's generation timestamp should correspond to the time interval when the validating node had the right to sign a new block;

• The new block's number should be greater than that of the last block in the existing chain;

• The total fee limit for transactions in the block should not be exceeded;

• The block should be correctly signed with the key of the node that created it; the following data should be signed: BlockID, Hash of the previous block, Time, Position in full_nodes, MrklRoot from all transactions in the block.

Each transaction in the block is checked for correctness in the following ways:

• Each transaction's hash should be unique;

• The limit of transaction signed with one key should not be exceeded (max_block_user_tx);

• The transaction size should not be exceeded (max_tx_size);

• The time when the transaction was sent should not be greater than the time of the block formation and not less than the block formation time minus 86400 seconds;

• Transactions should be correctly signed;

• The tokens which are assigned to be used for payment of transaction fees should exist in the sys_currencies list;

• The user who executed the contract should have a sufficient number of tokens in their Wallet to pay for resources required for execution of the transaction.

7. Platform's Database

The platform's unified database, copies of which are stored and maintained up-to-date on every full node of the network, is used for storing large volumes of data (registers) and quick retrieval of data by contracts and interfaces. In the formation of a new block and its addition to the blockchain, all full nodes of the platform carry out a simultaneous update of database tables. Thus, the database stores the current (up-to-date) state of the blockchain, which ensures the equivalence of data on all full nodes and unambiguousness of contract execution on any validating node. When a new full node is added to the network, the up-to-date status of its database is reached by way of subsequent execution of all transactions recorded in the blocks of the blockchain.

Apla Platform uses PostgreSQL as its database management system. Apla Association is entitled in the future at any time to make a decision about the transition to a hybrid (SQL / NoSQL) database, in order to provide for expansion of the platform's functions (particularly, for implementation of semantic tools), and to increase the speed of the platform's operation though optimization of storage of various types of data.

Annex F. Apla Software Technical Paper

*This Apla software technical paper **("Apla Technical Paper)** describes software resources made available to Apla Users by EGAAS corporation. .*

Revision History

Version	Date	Approved by	Summary of Changes

1. Platform's Ecosystems

The data space of Apla Platform is divided into many relatively independent clusters – ecosystems, in which the activities of the network's users are implemented. An Apla Ecosystem is an autonomous software environment that consists of a certain number of applications and users, who create these applications and work with them. Any APL Wallet Owner can create a new ecosystem.

The software basis of an ecosystem is a collection of applications, which are systems of interfaces, contracts, and database tables. The specific ecosystem to which application elements belong is indicated by prefixes in their name (for example, @1name), where the ecosystem's ID is indicated after the "@" sign. When addressing application elements within the current ecosystem, the prefix can be omitted.

The Molis software client provides access to database management tools, contracts editor, interface editor, and other functions required for the creation of applications in

an ecosystem, without resorting to any additional software modules.

Subject to compliance with the terms and conditions of Apla Admission Policy, a person can become a user of Apla Platform only after receiving a private key for accessing one of the ecosystems (by default, ecosystem #1). A user can be a member of any number of ecosystems. Switching between ecosystems is carried out using a specialized menu of the software client.

2. Integrated Development Environment

The Molis software client includes a full-scale integrated development environment (IDE) for creation of blockchain applications. The IDE is comprised of:

Ecosystem parameters table

Contracts editor

Database tables administration tools

Interface editor and a visual interface designer

Language resource editor

Application import / export service

Applications on Apla

An application on Apla Platform is a system of tables, contracts and interfaces with configured access rights. Such applications perform useful functions or implement various services.

Applications do not imply the presence of a unifying and coordinating contract (master contract) – separate contracts are called by user actions (for example, by a click on a button in the user interface). The results of work of contracts are the records in database tables.

To initiate user events a notification system is employed (which in essence is an application, installed by default on all ecosystems). To notify an ecosystem member (or a user role representative) about the need to carry out a specific action (sign a contract, approve data, etc.) they are sent a message with a link to a related interface page. The notification system allows for modeling complex activities. Furthermore, by

embedding the notification system in applications, software developers can simplify and speed-up their creation and subsequent improvement.

Each ecosystem creates its own set of tables for development of applications. This, however, does not exclude the possibility of accessing tables from other ecosystems by specifying those ecosystems' prefixes in table names. Tables are not in any way bound (nor belong) to specific contracts, and can be used by all applications. The permissions for entering data into tables are set by way of configuring the access rights. Specialized smart contracts – smart laws – can be used for rights management.

3. Ecosystem's Tables

An unlimited number of tables can be created for each ecosystem on the platform's database. As mentioned earlier, tables belonging to a specific ecosystem can be identified by a prefix that contains the ecosystem ID, which is not displayed in the software client while working within that specific ecosystem. Making records in tables of other ecosystem's tables is possible in cases where the access rights are configured to allow such actions.

4. Tools for Tables Administration

Tools for administration of an ecosystem's tables are available from the Tables menu of the administrative tools in the Molis software client. The following functions are implemented:

- Viewing the list of tables and their contents;
- Creation of new tables;
- Adding new table columns and specifying the data type in columns: Text, Date/Time, Varchar, Character, JSON, Number, Money, Double, Binary;
- Management of permissions for entering data and changing the table structure;
- Access Rights.

Rights can be set for adding new rows, new columns, for changing values in the table or it's certain columns, and to change all the aforementioned rights. The access rights can be defined in a number of ways using the Permissions table fields:

• Specifying true for granting free access, or false for complete denial of access to everyone;

• Specifying access conditions in the form of logical expressions, the result of which shall be true or false;

• Describing complex access rights conditions (using requests to database tables) in special contracts; to do this, the ContractConditions function should be placed in the Permissions field with a contract name as an argument;
• Granting access to perform operations only to certain contracts, listed in the ContractAccess function parameters; this option is used to grant exclusive rights to access data, and allows for adding operations that will be forcefully executed with every access request.

5. Operations with Data in Tables

To organize the work with the database, the Simvolio contract language and the Protypo template language both have the DBFind function, which provides for retrieving values and data arrays from tables. The contract language has a function for adding rows to tables, DBInsert, and a function for changing values in existing entries, DBUpdate (when a value is changed, only the data in the database table is rewritten, whereas the blockchain is appended with a new transaction while preserving all previous transactions). Data in tables can be modified but not deleted.

In order to minimize the time of contracts execution, the DBFind functions cannot address more than one table at the same time, thus the requests with JOIN are not supported. That is why it is not advisable to normalize the application tables, but rather include all available information to the rows, thus duplicating data available in other tables. This, however, is not just a coercive measure, but a necessary requirement for blockchain applications, where what is saved (signed by a private key) should be a full, complete, up-to-date for a specific moment in time set of data (document), which cannot be modified due to the change of values in other tables (which is inevitable in relational databases).

6. Smart Contracts

A smart contract is a basic element of applications, which performs a single action (typically, makes a record in a database

table), initiated from the user interface by a user or by another contract. All operations with data in applications are formed as a system of contracts, interacting with each other through database tables or by call functions in a contract body.

Smart contracts can be edited, but only if editing was not forbidden by way of putting false in the contract editing rights. Operations with data in the blockchain are performed by the most up-to-date (current) version of the contract. The complete history of changes made to contracts is stored in the blockchain and available from the software client.

7. Smart Contract Structure

A smart contract is comprised of three sections:

• *Data* – is used for description of data passed to the contract (names and types of variables).

• *Conditions* – in this section the verification of incoming data is implemented with the option to display error messages in the user interface using the following commands: error, warning, info. These commands generate an error that stops the work of the contract, but display different messages in the user interface: critical error, warning, and information error.

• *Action* – contains the main program code of the contract that executes the retrieval of additional data and recording the result in the database tables.

8. Simvolio Contracts Language

Smart contracts in Apla are written using Turing-complete script language called Simvolio, with compilation into bytecode. The language includes a set of functions, operators and constructions that can be used for implementation of data processing algorithms and operations with the database. The Simvolio language provides for:

• Declaration of variables with different data types, as well as simple and associative arrays: var, array, map;

• Use of the if conditional statement and the while loop structure;

• Retrieval of values from the database and recording data to database DBFind, DBInsert, DBUpdate;

• Work with contracts CallContract, ContractAccess, etc.;

• Conversion of variables HexToBytes, Int, Str, etc.;

• Operations with strings Size, Replace, Substr;

• Predefined Variables;

• The following predefined variables are available in contracts:

• Current Wallet's numeric ID ($key_id);

• Current Ecosystem's ID ($ecosystem_id);

• Time specified in the transaction, which executed the contract ($time);

• Time when the block with this transaction was formed ($block_time), and other ones;

• Predefined variables are available not only in contracts, but also in Permissions fields (where conditions for access to application elements are defined), where they are used in construction of logical expressions. When used in Permissions fields, variables related to block formation ($time, $block, etc.) always equal zero;

• Predefined variable $result is used to return a value from a nested contract.

9. Nested Contracts

A nested contract can be called from the conditions and action sections of the enclosing contract. A nested contract can be called directly with parameters specified in parenthesis after its name (NameContract(Params)), or using the CallContract function, for which the contract name is passed using a string variable.

10. Contracts with Confirmation

Since the contracts language allows for execution of nested contracts, there is a possibility that such a nested contract will be called without informing the user who executed the original (enclosing) contract. This may result in signing transactions initiated by nested contracts with the user's key without their

knowledge (unauthorized signing). To avoid the emergence of such situations, an additional confirmation – signature of a contract – should be received from the user when important/ critical contracts (for example, contracts that transfer tokens from the user's Wallet) are executed from other contracts. For this purpose, an additional field Signature should be added in the data section of a critical contract. When called directly, such a contract with confirmation will operate similar to a standard contract, but when called from another contract, it will require the user to additionally verify the action initiated by it.

The work of contracts with confirmation can be configured in the Signatures area of the administrative section of the Molis software client, where the following information can be defined:

- Contract name;
- Text which will be displayed in a verification pop-up window;
- Names and text description of fields (the values of which will be shown to the user);
- Contract Editor.

Contracts can be created and edited in a special editor which is a part of the Molis software client. Each new contract has a typical structure created in it by default with three sections: data, conditions, action. The contracts editor helps to:

- Write the contract code (highlighting key words of the Simvolio language);
- Format the contract source code;
- Bind the contract to an Wallet, from which the payment for its execution will be charged;
- Define permissions to edit the contract (typically, by specifying the contract name with the permissions stipulated in a special function ContractConditions or by way of direct indication of access conditions in the Change conditions field);
- View the history of changes made to the contract with the option to restore previous versions.

11. User Interfaces

Integrated Development Environment of the Molis software client includes an interface editor and a virtual interface designer. Interface pages are the essential part of applications that provides for retrieval and display of data from database tables, creation of forms for receipt of user input data, passing data to a contract, and navigation between application pages. Interface pages, just as contracts, are stored in the blockchain, which ensures their protection from falsification when loading them in the software client.

12. Protypo Template Language

Protypo is a functional template language, which was developed for description of interface pages structure, as well as obtaining and processing data at the client side.

Protypo functions provide for implementation of the following operations:

- Retrieving values from the database: DBFind;
- Representation of data retrieved from the database as tables and diagrams;
- Assignment and display of values of variables, operations with data: SetVar, GetVar, Data;
- Display and comparison of date/time values: DateTime, Now, CmpTime;
- Building forms with various sets of user data input fields: Form, ImageInput, Input, RadioGroup, Select;
- Validation of data in the form fields by displaying error messages: Validate, InputErr;
- Display of navigation elements: AddToolButton, LinkPage, Button;
- Calling contracts: Button;
- Creation of HTML page layout elements – various containers with an option to specify css classes: Div, P, Span, etc.;

• Embedding images onto a page and uploading of images: Image and ImageInput;

• Conditional display of page layout fragments: If, ElseIf, Else;

• Creation of multi-level menus: MenuGroup, MenuItem;

• Interface localization: LangRes.

13. Calling Contracts

Protypo implements contract calling by clicking on a button in a form (Button function). Once this event is initiated, the data entered by the user in the fields of the interface forms is passed to the contract (if the names of form fields correspond to the names of variables in the data section of the called contract, data is transferred automatically). The Button function allows for opening a modal window for user verification of the contract execution (Alert), and initiation of redirect to a specified page after the successful execution of the contract, and passing certain parameters to this page.

14. Use of Styles

By default, interface pages are displayed using Angular Bootstrap Angle classes. If needed, users can create their own styles. Storage of styles is implemented using a special stylesheet parameter of the ecosystem configuration table.

15. Page Editor

Pages are created and edited in the Interface administrative section of the specialized editor, which provides for:

• Writing codes of interface pages with highlighting of keywords of the Protypo template language;

• Selection of a menu, which will be displayed on the page;

• Editing of the page menu;

• Configuration of permission to edit the page (typically, by way of specifying the name of the contract with permissions in the ContractConditions function, or by direct indication of access rights in the Change conditions field);

- Launching a visual interface designer;
- Page preview;
- Page Blocks.

To use typical code fragments on multiple interface pages there is an option to create page blocks and embed them in the interface code using the Insert command. Such blocks can be created and edited on the Interface page of the administrative section in Molis. For blocks, just as for pages, permissions for editing can be defined.

16. Visual Interface Designer

Visual Interface Designer allows for creating page designs without resorting to the interface source code in Protypo language. The Designer allows for setting the positions of form elements and text on the page using drag-and-drop, as well as configuring sizes and design of page blocks. The Designer provides a set of ready-to-use blocks for displaying typical data models: panels with headers, forms, and information panels. The program logics (receipt of data and conditional constructs) can be added in the page editor after the page design is created. (In the future, we plan to create a full-scale visual interface editor.)

17. Language Resources Editor

The Molis software client includes a mechanism for interface localization using a special function of the Protypo template language – LangRes, which substitutes the language resource labels on the page with corresponding text lines in the language selected by the user in the software client (or browser for the web-version of the client). A shorter syntax $lable$ can be used instead of the LangRes function. Translation of messages in pop-up windows, initiated by contracts, is carried out by the LangRes function of the Simvolio language.

Language resources can be created and edited in the Language resources section of the administrative tools of the Molis software client. A language resource consists of a label (name) and the translations of this name into different languages with the indication of corresponding two-character language identifiers (EN, FR, JP, etc.).

Rights to add and change language resources can be configured using the same way as for any other table in the languages table (Tables section of the Molis administrative tools).

18. Application Import and Export Service

The Molis software client allows for the export of application elements (tables, contracts, pages, menus, page blocks, language resources, and involved ecosystem parameters). The source code of exported elements is saved to *.sim files. When exporting tables, their structure and content can be exported separately or together.

Import of application elements and ecosystem configuration parameters can be performed in a specialized section of the Molis administrative tools, where data from an exported file can be imported and, in the case that some of its elements are already installed in this ecosystem, they can be deleted.

The export and import service can be used for the exchange of applications between ecosystems, but above all, it is necessary for the transfer of applications created on local computers or dedicated ecosystems to working ecosystems.

19. Access Rights Control Mechanism

Apla has a multi-level access rights management system. Access rights can be configured to create and change any element of an application: contracts, database tables, interface pages, and ecosystem parameters. Permissions to change access rights can be configured as well.

By default, all rights in an Apla ecosystem are managed by its founder (this is defined in the MainCondition contract, which every ecosystem has by default). However, after specialized smart laws are created, access rights control can be transferred to all ecosystem members or a group of such members.

20. Controlled Operations

Permissions can be defined in the Permissions field of contracts, tables and interface (pages, menus, and page blocks) editors, available from the Molis administrative tools section. Permissions for the following operations can be configured:

Table column permission – permission to change values in the table column.

Table Insert permission – permission to add a new row to the table.

Table New Column permission – permission to add a new column.

Conditions for changing of Table permissions – permission to change rights, listed in items 1-3.

Conditions for change smart contract – permission to edit the smart contract.

Conditions for change page – permission to edit the interface page.

Conditions for change menu – permission to edit the menu.

Conditions for change of ecosystem parameters – permission to change a certain parameter in the ecosystem configuration table.

21. Ways to Manage Permissions

Rules, that define the access rights, should be entered in the Permissions fields as arbitrary expressions in Simvolio language. Access will be granted in the event that at the moment of request the expression was true. If the Permissions field is left blank, it is automatically set to false, and the execution of related actions is blocked.

The easiest way to define permissions is to enter a logical (boolean) expression in the Permissions field. For example, $member == 2263109859890200332, where the ID of a certain ecosystem member is given.

The most versatile and recommended method for defining permissions is the use of the ContractConditions function, to which a contract name can be passed as a parameter. This contract should include the conditions, in which formulation of the table values (for example, user roles tables) and ecosystem parameters can be used.

Another method of permissions management is the use of the ContractAccess function. The list of contracts that are eligible to implement a corresponding action can be passed to the ContractAccess function as parameters. For example, if we take the table that lists the Wallets in the ecosystem's

tokens, and put ContractAccess("TokenTransfer") function in the Permissions field of the amount column, then the operation of changing the values in the amount column will be allowed only to the TokenTransfer contract (all contracts that perform token transfer operations between Wallets, will be able to perform such operations only by calling the TokenTransfer contract). Conditions for accessing the contracts themselves can be managed in the conditions section. They can be rather complex and can include many other contracts.

22. Exclusive Rights

To resolve conflict situations or those critical for the operation of an ecosystem, the Ecosystem parameters table has a number of special parameters (changing_smart_contracts, changing_tables, changing_pages), where the conditions for obtaining exclusive rights to access any smart contracts, tables and pages are defined. These rights are set using special smart contracts, for example, executing a voting of ecosystem members or requesting the availability of a number of signatures of different user roles.

23. Ecosystem Parameters

The ecosystem parameters are available for viewing and editing from the Ecosystem parameters section in the administrative tools of the Molis software client. Ecosystem parameters can be divided into the following groups:

- General parameters: name of the ecosystem (ecosystem_name), its description (ecosystem_description), Wallet of its founder (founder_Wallet), and other information

- Access parameters, which define exclusive rights to access application elements (changing_tables, changing_contracts, changing_page, changing_menu, changing_signature, changing_language);

- Technical parameters: for example, user stylesheets (stylesheet);

- User parameters of the ecosystem, where constants or lists (separated by commas), required for the work of applications are stored.

24. Rights to edit can be specified for every ecosystem's parameter.

In order to retrieve values of certain ecosystem parameters, both the contracts language Simvolio and the template language Protypo have the EcosysParam function, where an ecosystem parameter name can be specified as an argument. To retrieve an element from a list (entered as an ecosystem parameter and separated by commas), you should specify you desired element's counting number as a second argument for the function.

25. Parameters of the Platform Configuration Ecosystem

- All parameters of the Apla blockchain platform are stored in the parameters table of the platform configuration ecosystem. These are the following parameters:

- Time period for creation of a block by a validating node;

- Source codes of pages, contracts, tables, and menus of new ecosystems;

- List of validating nodes;

- Maximum transaction and block sizes, and the maximum number of transactions in one block;

- Maximum number of transactions sent by the same Wallet in one block;

- Maximum amount of Fuel spent on one transaction and one block;

- Fuel to APL exchange rate, and other parameters.

Managing the parameters of the platform configuration ecosystem on the program level is the same as managing the parameters of any other ecosystem. Unlike in other ecosystems, where all rights to manage ecosystem parameters belong to the ecosystem founder, changing the parameters of the platform configuration ecosystem can only be performed using the UpdSysContract contract, the management of which is defined in the platform's smart law mechanism. Contracts (smart laws) are created before the network is launched and implement the rights and standards.

26. Virtual Dedicated Ecosystems

Apla source code allows for creation of Virtual Dedicated Ecosystems (VDE), which have the full set of functions of standard ecosystems, but work outside the blockchain. In VDE full-scale applications can be created using the contract and template languages, database tables and other software client functions. Contracts from blockchain ecosystems can be called using API.

27. Requests to Web-Resources

The main difference between VDE and standard ecosystems is the possibility to make requests from its contracts to any web-resources via HTTP/HTTPS using the HTTPRequest function. Arguments passed to this function should be: URL, request method (GET or POST), header, and request parameters.

28. Rights to Read Data

Since data in VDE are not saved to the blockchain (which, however, is available for reading), they have an option to configure rights to read tables. Read rights can be set for separate columns, and for any rows using a special contract.

29. Using VDE

VDE can be used for the creation of registration forms and sending verification information to users' emails or phones, storing data out of public access, and writing and testing the work of applications with their further export and import to blockchain ecosystems. Also, in VDE you can schedule contract execution, which allows for the creation of oracles, which are used for receiving data from the web and sending it to the blockchain.

30. Creating a VDE

VDE can be created on any full node on the network. Node Administrator defines the list of ecosystems that are allowed to use the functions of dedicated ecosystems, and assigns a user who will have the rights of the ecosystem founder and will be able to: install applications, accept new members to the ecosystem, and configure access rights to the ecosystem's resources.

31. REST API

All functions, available from the Molis software client, including authentication, receipt of data about ecosystems, error handling, operations with database tables, interface pages, and execution of contracts (network transactions) are available through REST API of the Apla platform. Thus, by using REST API developers can access any function of the platform without using the Molis software client.

Command calls are performed by addressing /api/v2/command/[param], where command is a command name, and param is an additional parameter (for example, the name of the resource to change or receive). Request parameters should be sent with Content-Type: x-www-form-urlencoded. The server response will be sent in JSON format.

32. Error Handling

In case of successful execution of the request, status 200 is returned. In case of an error, in addition to the error status, a JSON object is returned with the following fields: error – error ID (see documentation)

msg – error message

params – array of error additional parameters, which can be embedded in the error message

Authentication

The JWT token (www.jwt.org) is used for authentication. After having received a JWT token, it should be passed with every request in the header: Authorization: Bearer TOKEN_HERE.

Initially, the getuid command gets a temporary token, which is used in authorization (login command). The token, received in response to getuid command should be passed with every request in the header Authorization. Sessions can be extended using the refresh function.

33. Work with Ecosystems

Commands for work with ecosystems allow for obtaining the following data:

- Number of ecosystems;
- List of parameters of an ecosystem or its certain parameters;
- List of ecosystem's tables, information about certain tables;
- List of rows in a certain table;

- A certain table row by its ID, with specification of column names to be returned;

- Work with Contracts and Pages;

- Commands for work with contracts allow for:

    - Receiving the list of contracts;

    - Receiving information about a contract by its name;

    - Sending a transaction to the network, that is executing a contract by its name and passing parameters to it; in case of a successful execution of the transaction, its hash is returned, which can be used to identify the block number, in which it was included, or an error message otherwise;

    - Receiving the source code (in JSON format) of a page or menu by specifying its name.

34. Concurrent Transactions Processing

Smart contracts, executed by transactions from one ecosystem, in most cases, don't have links to other ecosystems (do not refer to tables of other ecosystems). Therefore, after having verified the absence of such links, sequences of transactions from different ecosystems can be included in different groups, and processed in parallel threads (sequence of these transaction groups within one block does not matter). Processing of transactions on other validating nodes is also carried out in parallel threads.

35. Partial Nodes

If it is known that contracts and interfaces of some ecosystems work with tables only inside those ecosystems, then it is possible to create and maintain a special (partial) node, which will store partial versions of the blockchain and the database: the blockchain will be complemented only with blocks that contain transactions of the current ecosystem, and only such transactions will be processed. Operating such a partial node may significantly increase the speed of the receipt of interfaces by the members of this ecosystem and sending transactions to the network. (Note: the creation of such partial nodes is feasible only for ecosystems in which applications do not have special security requirements.)

Annex G. Apla Personal Data Breach Notification Procedure

This Apla personal data breach notification procedure ***("Apla Personal Data Breach Notification Procedure")*** *sets out the rules and guidance to responding to a personal data breach incident.*

Revision History

Version	Date	Approved by	Summary of Changes

1. Introduction

This procedure is intended to be used when an incident of some kind has occurred that has resulted in, or is believed to have resulted in, a loss of personal data for which Apla User is a controller. This document should be used in conjunction with the Information Security Incident Response Procedure which describes the overall process of reacting to an incident affecting the information security of the Apla blockchain platform.

It is a requirement of the GDPR that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. In the event that the 72-hour target is not met, reasons for the delay must be given.

Where an incident affects personal data, a decision must be taken regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the

breach is likely to result in "a high risk to the rights and freedoms of natural persons".

The actions set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding what to do. However, it is intended that the steps set out here will prove useful in ensuring that our obligations under the GDPR are fulfilled.

2. Personal Data Breach Notification Procedure

Once it has been decided that a breach of personal data has occurred, there are two parties who may be required by the GDPR to be informed. These are:

1.. The supervisory authority

2.. The data subjects affected

It is not a foregone conclusion that the breach must be notified; this depends upon an assessment of the risk that the breach represents to "the rights and freedoms of natural persons" (GDPR Article 33). The following sections describe how this decision must be taken and what to do if notification is required.

2.1. The Supervisory Authority

The supervisory authority for the purposes of the GDPR shall depend on the laws applicable to the Apla Community member acting as data controller in relation to the data breach occurred. If more than one data controller is responsible for the safety of the data affected by the breach, there may be more than one supervisory authorities.

2.1.1. Deciding whether to notify the Supervisory Authority

The GDPR states that a personal data breach shall be notified to the supervisory authority "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33). This requires that the organization assess the level of risk before deciding whether or not to notify Factors to be taken into Wallet as part of this risk assessment should include:

- Whether the personal data was encrypted;
- If encrypted, the strength of the encryption used;
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data);
- The data items included e.g. name, address, bank details, biometrics;
- The volume of data involved;
- The number of data subjects affected;
- The nature of the breach e.g. theft, accidental destruction;
- Any other factors that are deemed to be relevant.

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Top management;
- Business area(s);
- Technology;
- Information security;
- Legal;
- Data protection officer.

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by top management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification;

2. The personal data breach requires notification to the supervisory authority only;

3. The personal data breach requires notification both to

the supervisory authority and to the affected data subjects.

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

2.1.2. How to notify the Supervisory Authority

In the event that it is decided to notify the supervisory authority, the GDPR requires that this be done "without undue delay and, where feasible, not less than 72 hours after having become aware of it" (GDPR Article 33). If there are legitimate reasons for not having given the notification within the required timescale, these reasons must be given as part of the notification.

The notification should be given via appropriate secure means to Supervisory Authority in the form required by the laws applicable to the data controller in charge of notification.

Nevertheless, the following information must be given as part of the notification:

a) The nature of the personal data breach, including, where possible:

i. Categories and approximate number of data subjects concerned;

ii. Categories and approximate number of personal data records concerned;

b) Name and contact details of the data protection officer or other contact point where more information may be obtained;

c) A description of the likely consequences of the personal data breach;
d) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects;

e) If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier.

Written confirmation should be obtained from the supervisory authority that the personal data breach notification has been received, including the date and time at which it was received. Where necessary, the GDPR allows the information to be provided in phases without undue further delay.

Documentation of the personal data breach, including its effects and the remedial action taken, will be produced as part of the Information Security Incident Response Procedure.

2.2. Data Subjects

2.2.1. Deciding whether to notify data subjects

The GDPR states that a personal data breach shall be notified to the data subject *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34)*. Note the addition of the word "high" over and above the definition given in Article 33.

The risk assessment shall be carried out to determine whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR.

Notification to affected data subjects is also not mandated by the GDPR where it *"would involve disproportionate effort" (GDPR Article 34)*. However, in this case a form of public communication should be used instead.

Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

2.2.2. How to notify data subjects

Once it has been decided that the breach justifies communication to the data subjects affected, the GDPR requires that this be done without undue delay.

The communication to the affected data subjects *"shall describe in clear and plain language the nature of the personal data breach" (GDPR Article 34)* and must also cover:

a) Name and contact details of the data protection officer or other contact point where more information may be obtained;

b) A description of the likely consequences of the personal data breach;

c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

In addition to the points required by the GDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

In most cases it will be appropriate to notify affected data subjects via letter or email or both in order to ensure that the message has been received and that they have an opportunity to take any action required.