ANNEX 5

PROCESSING TERMS

PREAMBLE

These Processing Terms ("**Terms**") are a policy governing the processing and security of Personal Data and form an integral part of the Agreement. By installing and/or using Creditinfo Products and/or Support Services the Customer confirms that it has duly read, understood and agrees with the Support Services Terms. Terms not otherwise defined under these Support Services Terms shall have the meaning given to them and defined in the Agreement.

1. **Definitions**

The below mentioned terms used herein and starting with capital letter shall have the below established content and meaning:

"Affiliates"	an entity that: (a) is majority-owned or controlled by either of the Parties, or (b)owns the majority of and/or controls either of the Parties. "Control" or "controlled" means the right to control and direct the management and operations of the entity, whether by majority ownership, contract or the ability to appoint a majority of directors;
"**Agreement"**	an agreement concluded between the Parties which incorporates the Terms by referring to them. The Agreement can be, for example, a Software Supply Agreement, License Agreement, Support & Maintenance Agreement, Agency Agreement, or NDA;
"Creditinfo"	the Creditinfo entity identified in the Agreement;
"Data Protection Legislation"	as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland);
"**EEA"**	the European Economic Area;
"**GDPR"**	the Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

THE TERMS "**CONTROLLER**", "**DATA SUBJECT**", "**PERSONAL DATA**", "**PERSONAL DATA BREACH**", "**PROCESSING**", "**PROCESSOR**" AND "**SUPERVISORY AUTHORITY**" SHALL HAVE THE MEANING GIVEN TO THEM IN THE GDPR.

1. **Terms and their application**

1.1. **Purpose of the Terms.** The Terms govern the processing and security of Customer Personal Data.

1.2. **Application of the Terms**. The Terms shall only apply to the extent that the Data Protection Legislation applies to the processing of Customer Personal Data, including if:

1.2.1 The processing is in the context of the activities of an establishment of Customer in the EEA; and/or

1.2.2 Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering of goods or services to them or the monitoring of their behavior in the EEA.

2. **Roles and data processing instructions**

2.1. **Roles and Regulatory Compliance; Authorization.**

2.1.1 **Processor and Controller Responsibilities**. The Parties acknowledge and agree that:

(a) Creditinfo is a processor of Customer Personal Data under the Data Protection Legislation;

(b) Customer is a controller or processor, as applicable, of Customer Personal Data under the Data Protection Legislation; and

(c) each Party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Customer Personal Data.

2.1.2 **Authorization by Third Party Controller**. If Customer is a processor, Customer warrants to Creditinfo that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of Creditinfo as another processor, have been authorized by the relevant controller.

2.2. **Data Processing Instructions.** By entering into these Terms, Customer instructs Creditinfo to process Customer Personal Data only in accordance with applicable law: (a) to provide the Processor Services; (b) as further specified via Customer's use of the Processor Services (including in the settings and other functionality of the Processor Services); (c) as documented in the form of the Agreement, including these Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Creditinfo as constituting instructions for purposes of these Terms.

3. **Duration of personal data processing**

3.1. **Duration of Personal Data Processing**. Processing of Customer Personal Data shall be performed for the duration of the Agreement plus the period until the deletion of all Customer Personal Data in accordance with the Terms.

4. **Nature and purpose of personal data processing**

4.1. **Nature and Purpose of Personal Data Processing.** Creditinfo shall process Customer Personal Data through means of automated processing for the purpose of providing Processor Services to the Customer.

5. **Types of personal data**

5.1. **Types of Personal Data.** The Customer Personal Data may include types of personal data described at www.creditinfo.com.

6. **Categories of data subjects**

6.1. **Categories of Data Subjects.** Customer Personal Data will concern the following categories of data subjects:

6.1.1 data subjects about whom Creditinfo collects personal data in its provision of Processor Services; and/or

6.1.2 data subjects about whom personal data is transferred to Creditinfo in connection with Processor Services by, at the direction of, or on behalf of Customer.

6.2. Depending on the nature of the Processor Services, these data subjects may include (a) Customer's or Customers Affiliates' employees, contractors, members of bodies; (b) Customer's or Customers Affiliates' clients.

7. **Rights and obligations of the Parties**

7.1. **Mutual Notification Obligation.** If any third person, particularly a data subject or supervisory authority, requests any Party to provide any information in relation to personal data processing under the Agreement or the Terms, or in this relation makes any claim or exercises any right against any Party, the Party undertakes to inform the other Party about such procedure without undue delay.

7.2. **Customer's Obligations.** The Customer is liable for fulfilling all controller's obligations in relation to Customer Personal Data processing, particularly for informing data subjects about Customer Personal Data processing, obtaining consent with Customer Personal Data processing if necessary, dealing with data subjects' requests relating to exercise of their rights (such as right to information, access, rectification, erasure, process limitation, right to object etc.). The Customer is further liable for fulfilling all notification obligations towards any supervisory authority relating to Customer Personal Data processing, especially for notifying the supervisory authority on any personal data breach.

7.3. **Customer's Security Assessment.** Customer is solely responsible for reviewing the Terms and evaluating for itself whether the security measures, and Creditinfo's commitments hereunder meet Customer's needs, including with respect to any security obligations of Customer under the generally binding legal regulations applicable to the Customer.

7.4. **Customer's Acknowledgement**. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Personal Data as well as the risks to individuals) the security measures implemented and maintained by Creditinfo as set out in the Terms provide a level of security appropriate to the risk in respect of the Customer Personal Data.

7.5. **Data Subject Requests.** For the duration of Customer Personal Data processing, if Creditinfo receives any request from a data subject in relation to Customer Personal Data, Creditinfo shall advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request.

7.6. **Creditinfo's Obligations.** For the purpose of the Customer Personal Data protection Creditinfo undertakes, for the duration of processing Customer Personal Data under the Agreement and the Terms, that it:

7.6.1 Shall take appropriate steps to ensure compliance with the security measures by its employees, contractors and subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality;

7.6.2 Shall implement and maintain technical and organizational measures to protect Customer Personal Data against any personal data breach described in Appendix A to the Terms;

7.6.3 Shall not engage another processor without prior authorization of the Customer, except for the providers ensuring data transfer between Parties, service staff and SW developers of Creditinfo, and in case of engaging the abovementioned processors, Creditinfo shall ensure to obligate them to adhere to these Terms;

7.6.4 In the scope appropriate to the nature of processing and available information, Creditinfo shall be supportive of the Customer with ensuring appropriate technical and organizational measures to secure the Customer Personal Data, notifying personal data breach to any supervisory authority or data subject, assessing data protection impact and with prior consultations with the supervisory authority;

7.6.5 Shall provide the Customer with necessary information, which the Customer can fairly demand, to fulfil the Customer's obligation to react to the data subject's request to exercise its rights under the Data Protection Legislation;

7.6.6 Shall provide the Customer with all information necessary to demonstrate Creditinfo's compliance with the obligations stated in the Terms and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer according to audit terms stipulated in Appendix B to the Terms.

8. FINAL PROVISIONS

8.1. **Language**. These Terms are made only in the English language. If there is any conflict in the meaning between the English language version of these Terms and any version or translation of it in any other language, the English language version shall prevail.

8.2. **No Waiver of Rights.** No failure or delay by either Party in exercising any right, power, or remedy under the Terms shall operate as a waiver of any such right, power or remedy and does not constitute an established practice between the Parties for the future.

8.3. **Interpretation**. The titles, captions and headings of the Terms are included for ease of reference only and shall be disregarded in interpreting or construing the Terms or the Agreement.

8.4. **Reference to Clauses.** Any reference to a Clause in the Terms refers to the specified Clause of the Terms, unless explicitly referring to another document.

8.5. **Severability.** If any provision of the Terms is or will become invalid or unenforceable the validity and enforceability of all other provisions of the Terms shall not be affected. In such case the Parties undertake to replace within 14 (fourteen) days from the day that one of the Parties gives notice to the other Party the invalid or unenforceable provision with a valid and enforceable provision with the same business and legal meaning.

8.6. **Revision of the Terms.** In the event of changes to the Data Protection Legislation or any other applicable legislation or changes to the interpretation rules or practices for interpretation of the legislation, Creditinfo may amend the Terms within a reasonable scope. The amendment of the Terms shall be reported by Creditinfo on its website and by email to the last known e-mail address of the Customer used for the communication with Creditinfo. Unless rejected by the Customer within 1 (one) month after sending the notification to the Customer, the Customer is deemed to have adopted the amended Terms. Should the Customer reject the amended Terms within the aforementioned period, this fact shall constitute the termination of these Terms with a 2 (two) months termination period following the delivery of the rejection to Creditinfo; during this period the last Terms accepted by both Parties shall apply to the Agreement. However, notwithstanding the foregoing, by continuing to access or use Creditinfo Products and/or Support Services the Customer agrees to be bound by any such revised Terms.

APPENDIX A

SECURITY MEASURES

As from the Terms effective date, Creditinfo will implement and maintain the security measures set out in this Appendix A. Creditinfo may update or modify such security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the processing.

1. DATA CENTER AND NETWORK SECURITY

1.1. DATA CENTERS

1.1.1 **Infrastructure.**

Creditinfo servers are placed either in the datacenter within rented racks or Creditinfo is paying for resources in cloud environments provided by international companies (e.g. Microsoft Azure, Amazon Web Services etc.).

1.1.2 **Redundancy.**

When server places in datacenters, then standard redundancy measures are put in place, which mainly means:

- Redundant power supply
- Redundant internet connection
- Cluster virtualization with n+1 hosts and switches

When resources purchased from international companies providing cloud technologies, then redundancy is managed by them and provided already as standard part of paid service.

1.1.3 **Power.**

In general, described in previous point as it is dependent on the chosen data center. Nevertheless, the following minimum must be guaranteed:

- Protection against power outages by transformer stations including circuit breakers
- Diesel generators to overcome a longer power outage
- UPS units with separate battery modules to overcome a shorter power outage

1.1.4 **Server Operating Systems.**

Creditinfo is mainly Microsoft based company, so in most of the cases MS Windows Server OS is used. Versions are dependent on the solution nevertheless it must be always correctly licensed and covered by software assurance for further updates.

When resources purchased from international companies providing cloud technologies, licenses for OS are already standard part of paid service.

1.1.5 **Businesses Continuity.**

Creditinfo is responsible for making and keeping up-to-date relevant continuity plans for all selected medium- and high-risk threats to hosted solutions on its own servers. Part of each continuity plan must be description of responsibilities, situations which are impulse for initiation of such plan, description of critical/emergency situation, report method and description of personal activities during critical/emergency situation solving.

1.2. NETWORKS AND TRANSMISSION

1.2.1 **Data Transmission.**

Creditinfo in cooperation with customer ensure the data transmission security. This is by minimum done via firewall solution, which is top element of a layered approach in network security. The purpose of such Firewall is to filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for users.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the firewall rule set.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide virtual private network (VPN) connectivity (if applicable and required)

1.2.2 **External Attack Surface.**

Hosted solutions by Creditinfo are protected against external attacks with appropriate Firewall solutions including advanced extensions (e.g. Web application firewall, GEO IP filtering, Botnet filtering etc.) if applicable and required. When resources purchased from international companies providing cloud technologies, similar or higher protection is also applied.

1.2.3 **Intrusion Detection.**

Hosted solutions by Creditinfo are protected against intrusion incidents with appropriate Firewall solutions including advanced extensions (e.g. Web application firewall, GEO IP filtering, Botnet filtering etc.) if applicable and required. When resources purchased from international companies providing cloud technologies, similar or higher protection is also applied.

1.2.4 **Incident Response.**

Creditinfo is accountable for monitoring and solving all security incidents and vulnerabilities regarding the hosted solutions. Each incident has to be recorded in appropriate system sorted out without delay based on the incident severity. Such process should be described in internal guidelines (usually within ISO 27001 documentation if applied).

1.2.5 **Encryption Technologies.**

Hosted solutions by Creditinfo which are exposed to internet should always primarily used crypted HTTPS protocol for data transfers of all confidential information. When resources purchased from international companies providing cloud technologies, similar or higher protection is also applied.

2. ACCESS AND SITE CONTROLS

2.1. SITE CONTROLS

2.1.1 **On-site Data Center Security Operation.**

When Creditinfo servers are placed in the datacenter within rented racks, these racks need to be locked and accessible only by authorized persons. The perimeter of datacenter must be monitored by video surveillance system and all visits logged.

2.1.2 **Data Center Access Procedures.**

Depends if the datacenter is with 24/7 technical on-site support which then monitor all visits and unlocks the racks after the identification of authorized person. If datacenter is self-managed, then usually additional security measures appliers such as: finger print access to datacenter perimeter, advanced monitoring via surveillance system with remote security service etc.

2.1.3 **On-site Data Center Security Devices.**

When Creditinfo servers are placed in the datacenter within rented racks, these racks do not allow to connect any external devices by any unauthorized persons. Each device has to be labeled with its own ID and documented in list of placed devices. It is not possible to bring or take any device without the knowledge of authorized personnel responsible for placed HW.

2.2. ACCESS CONTROL

2.2.1 **Infrastructure Security Personnel.**

Physical access to servers and active network components by Creditinfo hosted solutions on its own HW is permitted only to competent persons. The room with placed servers and active network components is under regime of obligatory locking. The room is either locked by electronic lock with possibility of entrances logging or logging is done by responsible person.

2.2.2 **Access Control and Privilege Management.**

Access rights to Creditinfo hosted systems are assigned by Role-Based Access Control (RBAC) to the greatest extent possible. Only in exceptional situations it is possible to assign access right by user account. To roles are allocated only strictly necessary permissions. Access Control is managed only by authorized System Administrators and all accesses must be created or altered only on basis of approved request by relevant owner in desired system (typically Service desk).

2.2.3 **Internal Data Access Processes and Policies – Access Policy.**

The following rules shall be applied as much as possible (if technically applicable). User password has to consist of 8 characters (at least); Administrator's password shall contain at least 12 characters. All passwords must fulfill (where technically possible) the requirement on complexity, which is at least 3 of following 4 conditions: 1. capital letters (A to Z); 2. small letters (a to z); 3. numbers (0 to 9); 4. non-alphanumeric character (e.g. !, $, #, %). System has to require the change of temporarily assigned password during first login to the system. Password must be changed after defined period of time (typically 90 days).

3. DATA

3.1. DATA STORAGE, ISOLATION AND LOGGING

Each hosted Creditinfo system is having its own separated servers (either physical or virtual). Access rights are then set to strictly protect and isolate such systems from each other. Audit logs are then set-up on Creditinfo servers to record default privileged operations, monitors the system operation and its outage and all attempts on unauthorized accesses and errors.

3.2. DECOMMISSIONED DISKS AND DISK ERASE POLICY

During the liquidation and removing of devices on the data processing it is needed to observe that all memory medium (e.g. computer and servers hard discs, memory cards with the saved configuration of network elements, cell phones memory cards etc.) which contain the sensitive/secret data and configuration data were before removing or liquidation irrecoverable deleted. When electronic data medium is erased there have to be done reformat and rewriting of random data, minimally in three consecutive cycles. It is convenient to use specialized SW tools which ensure given process.

If it is not possible to do secure erasing or given device has to be physically destroyed from different reasons, then it is needed to do the destruction so that it would not be possible to use given device or to read information from this device. Carrying out the liquidation ensures responsible person through a contractual partner.

4. PERSONNEL SECURITY

4.1. PERSONNEL CONDUCT

Every user has a unique user name in order to be able to trace individual's responsibility for the performed activity. Sharing the user names is not allowed. For each user then has to be applied password policy described in point 2.2.3 above. User has to always follow all defined internal rules and security guidelines which are part of internal documentation applied within Creditinfo company (usually within ISO 27001 documentation if applied). Such documentation should include at least clear desk and screen policy, rules for usage of SW on end user stations, malicious code protection, rules for handling IT equipment and rules for usage of information and communication services.

4.2. PERSONNEL TRAINING

Training of the security measures and rules must be completed by all workers at least once a year. (this is usually done within ISO 27001 yearly mandatory training).

5. SUBPROCESSOR SECURITY

5.1. SUBPROCESSORS

A physical or logical access of third parties (subprocessors) to information assets cannot be allowed until all the risks that may threaten these assets are considered. The identified risks related to the access of third parties have to be covered with appropriate measures. Creditinfo is responsible for the identification of such risks and proposal of measures. It is necessary there exists a record about the access of the third party which is verified by responsible Creditinfo worker.

In contracts with external parties should be, in cases where it makes sense, included at least the following requirements:

- General information security rules
- Description of the services that will be available to the third party
- Procedures which ensure return of all assets and its disposal after the termination of contractual relation
- Responsibility for the security of assets
- The right to monitor and to prohibit activities of third party
- Target level of service and unacceptable level of services
- Terms of cooperation with third party subcontractors
- The right to audit contractual obligations also through external organizations
- Security incident reporting system
- Penalties for breaking the rules
- Responsibility which arises from valid legal requirements
- Responsibility for installation, technical maintenance and for the software
- Clear and specified procedure of change management
- Description of a verifiable criteria of performance and a way of their observation

The above described requirements for the contract with the third party may be settled by signing a non-disclosure agreement.

APPENDIX B

ADDITIONAL RULES FOR AUDITS

a. Customer must send any requests for the audit under Clause 8.6.6. of the Terms solely to the Creditinfo's email address ciaudit@creditinfo.com.

b. Following receipt by Creditinfo of a request under Clause 8.6.6. of the Terms, Creditinfo and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any audit; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.

c. Creditinfo may charge a fee (based on its reasonable costs) for any audit requested by the Customer. Creditinfo shall provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. Creditinfo may object in writing to an auditor appointed by Customer to conduct any audit under if the auditor is, in Creditinfo's reasonable opinion, not suitably qualified or independent, a competitor of Creditinfo, or otherwise manifestly unsuitable. Any such objection by Creditinfo will require Customer to appoint another auditor or conduct the audit itself.