DATA PROTECTION AND INFORMATION MANAGEMENT

CREDITFORTE KFT.

Totth Benedek
ügyvezető igazgató

Introductory provisions

Goal and effect of the Data Protection and Data Security Policy

Creditforte Kft. (1118 Budapest Gombocz Z.u.14. Cg.:01-09-345193, VAT-number: 14656257-2-43, represented by: Ágnes BALÁZS, with individual signatory powers) (henceforth called: the Company) as Data Processor defines by the present Policy the lawful frames of the processes carried out at it as at a Data Processor. The Company ensures the enforcement of the constitutional principles of data protection and informational self-determination based on what is set down herein. We deem it extremely important to protect the personal data of customers availing themselves of our services and the obligors', too, and to respect their informational self-determination. We manage personal data confidentially and take every step that can facilitate the safe storing of electronic and other data. The goal of the present policy is to secure compliance with the requirements set to data transfer, data security and data security, with special emphasize on the role of our employees in the latter.

The present Policy covers the following:

- data flow between the various organizational units;
- data flow between the Data Controller (Principal) and the Data Processor (the Company);
- all operations at the Company's seat involving data;
- The personal scope of the present Policy embraces_
- all the organizational units and the employees employed thereat and
- all others, who are in any contractual and other relation with the company and may get in contact in any form with personal data as a result.

When elaborating the Policy the Company took into account the relevant statutory provisions in force, and the most important international recommendations. These were:

- the Constitution of Hungary;
- Act CXII/2011 on Information Self-Determination and the Freedom of Information (Info tv., by the Hungarian abbreviation);
- Act I/2012 on the Labour Code (új Mt., by the Hungarian abbreviation);
- Act V/2013 on the Civil Code (új Ptk., by the Hungarian abbreviation);
- Act CCXXXVII/2013 on Credit Institutions and Financial Enterprises (új Hpt., by the Hungarian abbreviation);
- Act VI/1998 on the Protection of Private Persons during the Automated Processing of their Personal Data;
- the provisions of the Hpt. regulating the protection of IT systems;
- Methodological Guidance No. 162007 of PSZÁF on the protection of the IT systems of financial organizations;
- IT Security Policy of the Company and other relevant policies (such as: Document Management Policy, Emergency Policy);
- the present Policy is to be interpreted and enforced together with the statutory provisions in force;
- DECREE (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL
- Szabályzat kialakítása során a Társaság figyelembe vette a vonatkozó hatályos jogszabályokat, illetve a fontosabb nemzetközi ajánlásokat, különös tekintettel az alábbiakra:

Activities of the Company

As its core activity, our Company is engaged in the collection of debts, an activity figuring under No. 8291'08 of TEÁOR (the branch-based classification of activities) on the basis of contracts of agency as such are defined by Section 6:272 of Act /2013 on the Civil Code. We proceed in the name and for the benefit of the principal (hereinafter called: **Principal**) and collect overdue debts that have emerged from various consumer relations, from Clients detailed later in this information material. As part of this, we execute the following activities:
We

- receive from the Principal data of the Clients in conformity with what is set down in the contract of appointment,
- check, clarify and transmit the data of the Clients,
- search for new contact data (exclusively from public data bases, e.g., the Telekom records, Residence Register of the Ministry of the Interior, Trade Register),
- establish and maintain contact with the Clients,
- participate in the enforcement of the claim before law.

Our Company perform debt collection activities solely on the basis of contracts of agency, and processes only the data and does not develop data bases during the discharge of its duties. We shall help the parties, as representative of the Principal, to find a solution according to which the debt the Debtor owes to our Principal is settled in a way acceptable for both parties. Based upon a proxy from the Principal the Company may also transmit data to others, if, according to the contract of agency concluded with

the Principal, the Company is authorized to involve cooperating parties (e.g., a printing house, personal visitors, postal services provider – hereinafter collectively called: **Subcontractor**) for the discharge of its duties.

Supervision and control

The present Policy is approved by the managing director of Creditforte Kft. and is stored by its data protection officer. It is revised, at the maximum, annually and following the modifications introduced, it must be approved again. The Policy is public and anyone can inspect it: it is accessible in electronic format on the www.creditforte.hu website and in hard copy, at the data protection officer.

Reporting and accountability

Within the organization the top management is accountable for the observance of the present Policy. Each employee shall immediately report to his/her direct superior if he or she detects an actual or attempted infringement of the present Policy. If the employee's direct superior is not available, then he/she should report to the data protection officer.

Terms and basic principles

Data controller: the natural person, legal entity or organization without a legal personality which individually or jointly with others determines the goal of data control, passes and executes the relevant decisions (including also the one regarding the means to be used for data control) or has them executed by others, (e.g., the data processor commissioned by him/her. The data controller is thus the person who performs the activities of the merits in connection with the data – e.g., determines the collected data, sets the goals, collects data, etc.)

Data control: irrespective of the procedure used, any action or operation executed on the data or the totality of these procedures and actions, and, especially collecting, recording, archiving, storing, changing using data, searching for them, plus the systemization, transmission and publication thereof; their harmonization linking, blocking, erasing, destruction, impeding their future use, making photos, audio and visual recordings of them and recording physical properties (e.g., finger and palm prints, DNA-samples, iris-photos) based on which individuals can be identified.

Data transmission: making data available to specified third person(s).

Data processing: presuming that the tasks are performed on data, irrespective of the methods or tools used or their place, execution of the technical tasks associated with the data processing acts.

Data processor: the natural person, legal entity or organization without a legal personality who or which, based on a contract concluded by and between him/her and a data controller (including also contracts concluded by the operation of law) performs the processing of data.

Special data: personal data relevant to race, nationality, political views or party affiliation, religious or other worldview beliefs, union membership, sexual life, health, addiction or criminal data.

Personal data: data that can be linked to the data subject and, especially, the name, identification code and one or more physical, physiological mental, economic, cultural or social knowledge/characteristics and also the conclusions that can be drawn from the data regarding the data subject.

Publication: making the data available to anyone.

Erasure of data: the making of data unrecognizable in a way that their restoration shall not be possible.

Destruction of data: complete physical destruction of the data carrier.

Entitledness: the Company is entitled to process personal data, if

- the data subject consented to it, or
- it is impossible to obtain the consent of the data subject or obtaining it would entail disproportionate costs and the control of personal data is necessary
    - for the fulfilment of any obligation concerning the data processor under the law, or
    - for enforcing the rightful interests of the data processor or third person, and the enforcement of this and the limitation of the rights to personal data are proportionate with one another.

Data minimization principle: Under the present Policy only such personal data can be controlled in connection with the Debtor as are inevitable and suitable for the realization of the purpose of the data control and achievement of the goal. Personal data can be controlled to the extent and for the period necessary for achieving the goal only.

Data quality requirement: During data control and processing the Company shall provide for the data to be accurate, complete and if necessary for the purpose of the data control, also update them. It shall be also the Company's duty to see to the data subject to be identifiable only for the duration necessary for data control. All data must be obtained and controlled fairly and lawfully. With regard to the data to be provided by the Principal, the data quality requirement means that the Company shall not be responsible for the accuracy and completeness of the data received and if any problem regarding the quality of the data comes to the Company's attention then it shall notify the Principal about it within the framework of their regular contacts.

Goal and extent of and the legal basis for data control

How does Creditforte come in possession of the personal data?

The personal data are transmitted to us on the basis of the contract of agency concluded by and between the Principal and Creditforte Kft. for in their contract with the Principal the Obligor consented to his/her/its data to be transmitted for the purposes of debt management or because the law allows us to receive data for managing the debts of obligors:

The following statutory provisions authorize the involvement of debt managers and transmitting to them data for this purpose:
Section 33/B, Subsections (4)-(5) of Act I/1988 on Road Traffic;
Section 161(1)(c) of Act CCXXXVIII/2003 on Credit Institutions and Financial Enterprises (**Hpt.**), by the Hungarian abbreviation);
Act CXX/2001. on the Capital Market (**Tpt.**, by the Hungarian abbreviation);
Act LX/2003 on Insurers and Insurance Activities (**Bit.,** by the Hungarian abbreviation);
Section 157 (9)(a) of Act C/2003 on Electronic Communications;
Sections 45(1)(b) and 45(4)(b) of Act XVIII/2005 on District Heating;
Section 151, Subsection (4), items "a" and "b" of Act LXXXVI/2007;
Section 118(2)(c) of Act CXXXVIII/2007 on Investment Firms and Commodity Dealers and on the Regulations Governing Their Activities;
Section 125(4)(a) of Act XL/2008 on Natural Gas Supply and
Section 61(3)(a) of Act CCIX/2011 on Waters Supply.
In the cases when data control is carried out by operation of the above statutory provisions, no consent from the Debtors (data subjects) is needed.

Legal basis for data control

Depending on the legal basis of data control, the scope of data may be different, and also, the legal basis may change for the whole or a part of the data depending on:

- the controlling of which data of yours you have consented to?
- which of your personal data may be controlled based on the statutory provisions?
- or if the data are controlled on the basis of a legitimate interest opinion then which data are inevitable for the achievement of the goal.

Basic principles

- personal data can be controlled only for a specified purpose, for exercising a right or meeting an obligation;
- data control shall in all of its phases be in compliance with its goal i.e., the specified purpose mentioned above;
- data collection and control shall be fair and lawful;
- personal data can be controlled only to the extent and for the period as is necessary for the achievement of the purpose. In addition to the purpose, unambiguous information should be furnished to the data subjects on who shall process and control their data.
- data shall be stored securely and in a manner and for a period proportional to the purpose of data control;
- the data controller shall provide for the security of the data and take all technical and organizational measures and prepare all the procedural rules as may be necessary for complying with the applicable statutory provisions;
- special attention shall be paid to the protection of data against unauthorized access, tempering, publication, erasure, injury and destruction;
- during data control the data subject can ask for information at any time and check the contents of his/her data and ask for their rectification;
- as a rule, data processing is automated;

- after the realization of the purpose of data control, the data shall be immediately erased as such is prescribed by the statutory provisions, taking into consideration also the instructions of the principals.

Consent by the data subject: when we control your personal data either based on your consent, given at the time when you have concluded a contract with our Principal or if you gave your explicit consent to our Company to control your data at some other (later) point of time) (see Section 5(1)(a) of the info tv.).

Data control by the operation of the law: based on Section 5(1)(b) of the Info tv. according to which the Principal may transmit the personal data of the Client to our Company, and on those provisions of the law that apply to our company with regard to the given assignment e.g., you incur a debt for using any of the above services and then the public utilities services provider is entitled to disclose to us your name, place and date of birth, your mother's name in order to enforce the public utilities services provider's rightful interests.

Legitimate interest opinion: When we do not have the data subject's consent to or the authority by operation of the law to control the data, the legal basis shall be the Principal's interest and this interest can be enforced proportionally to the limitation of the right of the data subject to the protection of his/her personal data.

Our Company can record the personal data of such person only who can act in the case as a representative with full power and authority (e.g., heir, guarantor, attorney (proxy). If we find that the data of a third party have been recorded in the administrative system, then we shall provide for their immediate erasure.

It is possible, that your personal data are controlled by our Company for several different reasons (we control them in connection with a complaint of yours and for the collection of your debt). If you ask us, we shall furnish you accurate information on how your data are controlled and which are the specific ones controlled.

Purpose of data control by the Company: The purpose of data control shall be to collect the receivables shown in the contract of agency concluded with the Principal, to reach settlement agreements with the Debtors, to keep records of the Debtors, tell apart the debtors, perform the assignments, keep records of the debts, document reimbursements and fulfil accounting obligations. The Company shall manage data solely and exclusively for the purposes described in the present Policy, for exercising the rights detailed herein and executing the obligations it has assumed. Data control shall comply in all stages with the purpose indicated.

Scope of data controlled by the Company: The Company shall control the following data of the Debtors and the persons acting as the Debtors' lawful representatives:
- name; birth name; mother's name; place and date of birth; phone number; residence; mailing address; e-mail address; tax identifier; data concerning the invoices with the payment of which the Debtor is in arrear: (contract identifiers, amount, securities established to guarantee the repayment of the debt, legal basis, previous correspondence, if necessary) (hereinafter called: **Personal Data**).

Data source: The Company receives the personal data from the Principal, mostly in electronic format and protected by password. The password is kept by the Data Protection Officer. When discussing any issue by phone or in person the Company shall record additional personal data only after the debtors have been informed of their choices and have given their explicit preliminary voluntary consents. The Company shall ask for and receive from the Principal original documents related to the claim against the Debtor only in exceptional cases, when these are absolutely necessary for the reconciliation with the Debtor. Data sources can also be the Ministry of the Interior as keeper of the Residence Records and Telekom (as the data base for phone numbers) and public data sources accessible to everyone, such as the Company Register.

At the concrete request of and based on the proxy issued by the Principal, except that the taking of a photo of the asset in question is prohibited by law, occasionally, an employee or another cooperating partner acting for the Company may take photo of the asset of the Debtor serving as security for the repayment of the receivables of the Principal. The Company shall pay special attention to not showing individuals on the photos, or if showing their not being identifiable. One can be identifiable only if he/she gave his/her explicit consent. The representative of the Company shall inform those present of taking photos. If they protest, then no photos can be made. The Company shall transmit the photos using personal data in such a manner that based on them the asset and the Debtor could be identified beyond doubt and could be linked to each other. When taking the photos, the Company or the third party participating partner cannot enter the private property without permit. The sole purpose of the photo is to document the state of the security listed among the personal data and to inform the Principal respectively. The Company shall inform the Debtor of the possibility that photos may be taken of the asset serving as security for the receivables prior to attempting to take any photos. The Company shall always act in conformity with and within the limits as laid down in the Company's contracts with the Principals. These are these limits within which the Company shall enforce the Debtor's debts towards the Principal and, if the assignment covers these, too, the costs of debt management, as well. This means that the Principal shall be the third person in the rightful interests of whom the right to the protection of the Debtor's personal data shall be curbed and limited. The limitation shall be that

the Company shall get from the Principal data subject's personal data and control the without the data subject's explicit preliminary written consent. The limitation and the control of personal data shall not have any impact on the life, private sphere or reputation of the data subject; it can be linked solely and explicitly to the facilitation of the payment of the outstanding debt. It must be emphasized that the other principles of data control – and among them, first and foremost, the principle of purpose – shall be realized in such cases, too.

Under contracts of assignment the Company is engaged in the collection of debts incurred by the Debtor by reason of having purchased the goods, or availing himself/herself of the services of the Principal and having not paid for them. In the contract of agency the Principal declared under the Principal's liability that the debt in fact existed, the Principal informed the Debtor of having assigned the debt and that it was legitimate to place the Debtor's data at the Company's disposal.

It is a rightful interest of the Principal, as creditor, to get consideration for the goods provided or the services rendered under the contract concluded by the Principal. To strictly observe the obligations set down in contracts is also the basis of the economic system relying on the freedom to entrepreneur. In view of this the limitation of the Debtors' right to the protection of their personal data is proportional. The limitation mentioned, i.e., that the Company can control the Debtor's personal data without the Debtor's consent, shall not result in any detrimental consequence to the Debtor afterwards. According to the present Policy the Company controls the data confidentially, using multiple protective tools; the data controlled cannot be accessed by any third person and shall not be made public, either. The data control shall not entail negative consequences for the Debtor neither in his/her private, nor in is/her public life and, especially, nothing such threatens him/her as a result of the activities of the Company as intermediary.

Data control and transmission under the present Policy to the Principal and the Sub-contractors are thus justified by the above.

Duration of Data Control

Creditforte Kft. shall determine active and passive data control periods:

Active data control period: is the period of time fined in the individual contracts of agency during which the personal data of the clients can be used to enforce claims in conformity with what have been laid down in the contract.
Passive data control period: a 90 days' period calculated from the end of the active data control period during which the Agent can still store the personal data of the Principal's clients in the Agent's records with a view to fulfil the Agent's contractual obligations but no action of active case management is performed, only the reasonable requests of the clients in connection with the management of their cases are fulfilled (e.g., certificates of settlement are issued and sent, information by phone is rendered on the closing/settlement/cancelation of the case and letters received following the elapse of the case management period are filed). Following passive case management, the very cases and the related personal data shall be irretrievably erased from the case management records. Following the elapse of the passive case management period, minutes shall be sent to the Principal with all documents received during the management of the case enclosed, and the minutes drawn up of the handing over shall be archived and kept.

The Company shall store the data until the earliest of the following dates:

- the end of the passive case management period following the active case management period, or if no passive case management period has been defined, then until the end of the appointment.
- the data of lawful representatives shall be stored until the end of their respective mandates or until the term prescribed by law, or
- until the data subject withdraws his/her consent

Data processors

Data processing, sending out text messages	Name: Dream Interactive Kft. Address: 1027 Budapest, Medve u. 24. processed: phone numbers
Data processing to check and identify phone numbers	Name: Magyar Telekom Nyrt. Address: 1013 Budapest, Krisztina krt. 55. Data processed: names, addresses, phone numbers
Checking of residential addresses	Name: Ministry of the Interior, Deputy State Secretariat Responsible for Keeping Records Address: 1094 Budapest, Balázs Béla u. 35. Data processed: names, addresses, mothers' maiden names, places and dates of birth

Operating and system manager	Name: Exis.hu Kft. Address: 1195 Bp. Nagysándor u. 3. Data processed: all data Name: Tóth Balázs ev. Address: 1195 Bp. Nagysándor u. 3. Data processed: all data
Book-keeping	Name: Trimova Kft. Address: 1191 Bp. Üllői út 206. Data processed: all data

Recording phone conversations

Our Company records all conversations by phone, without exception (recording cannot be switched off). This is partly to allow our clients to exercise their rights as clients in connection with the management of complaints, partly to fulfil the obligations we have to.We store these audio recordings for the period prescribed and if we are asked to, we furnish them free of charge and they may be handed over to the Principal, too.
The legal basis for the data control is: Section 17/B(e) of Act CLX/1997 (Fgytv., by the Hungarian abbreviation) and Section 288 (3) of the Hpt.
Data source: consent by the data subject.
Data processed: the audio recording.
Data control period: 5 years based upon Section 17/B(3) of Act CLV/1997 (Fgytv., by the Hungarian abbreviation) and Section 288(3) of the Hpt.
Data transmission: to the Principal, the Obligor and the party, if any proceeding lawfully in the case.

Storage of data furnished through the website

The same guidelines and principles shall apply if you contact us through the www.creditforte.hu website as in case of contacting us by e-mail or phone. The period of data storage (duration of data control) shall also be the same. The website dos not store any personal data, but the inquiry shall be recorded in the file of the case concerned (if the source of the inquiry can be identified), and at the end of the case management period it shall be erased from the records just as all the other data.

Accounting and taxation

In order to be able to make our accounts with the Principal and also because it is mandatory under law, our Company keeps all the accounting documents related to the debt, on which the name and address of the Obligor and all other data as may be prescribed by law can be seen.
Legal basis for data control: Section 169 of Act C/2000 (the Act on Accounting, Számv.tv., by the Hungarian abbreviation).
Data source: the persons fulfilling their obligations
Data controlled: name of the payer, amount paid, date and method of payment.
Duration of data control: 8 years, according to Section 169 of Számv.tv.
Data processors: see in the section entitled “Data processors”
Data transmission: the legal basis for data transmission can be a legitimate interest opinion, or if data transmission is to the NAV (Hungarian Tax and Customs authority, then Section 98.§(1) c) of the Art.

Complaint handling

The data controlled in the course of handling complaints shall serve only this purpose and to be able to answer to the complaint.
Legal basis for data control: Section 17/A of Act CLV/1997 (Fgytv., by the Hungarian abbreviation) and Section 288(3) of Hpt.
Data controlled: name, case number, customer number and all other identification data as the complainant may give in the complaint or the documents and instruments which form an inseparable part of the complaint in each case. Duration of data control: Pursuant to Section 17/a(7) of the Fgytv., our Company stores the minutes drawn of the complaint and the response thereto for 5 years. Where the complaint falls under the effect of Hpt. our Company stores the complaint in its archives for a period of 5 years. The Company sends without delay to the Principal all complaints which do not relate to the Company’s activities. Data transmission: if the supervising authorities ask for them, we transmit the data to them.

Data storage, data security

Depending on how they have emerged, our Company shall store data in the following manners:

- we shall store the data included in written statements or contracts during the data control period in their original written forms or as duplicate copies of the original, and
- those data that are not part of a written declaration or written contract shall be stored in electronic format.

Data security tasks: The Company shall provide for the security of the data and take all such technical or organizational measures and elaborate all such procedural rules as may be necessary for compliance with the Infotv., or any other data security or confidentiality regulations. The Company shall provide for the protection of personal data against the following: i) unauthorized access and data entry, ii) tempering and unauthorized transmission, iii) unauthorized transmission, iv) unauthorized publication, v) unauthorized erasure or destruction, vi) accidental destruction and damage, vii) becoming inaccessible (unreadable) due the amendment in the technology applied. In addition to protection the Company shall i) make it controllable to what organizations have the personal data been or can be transmitted by the help of data transmission equipment; ii) make it controllable and ascertainable what personal data and when have been entered into the automated data processing systems; iii) secure that in case of malfunction the installed system can be restored and retrieved and that v) reports should be made of the errors that occur during automated processing.

Impeding data connectivity: In order to protect the data controlled electronically in the various records, the Company shall ensure by the help of various technical solutions that the personal data stored in the various records (e.g., arranged by the various Principals) could not be connected to the data subject.

Physical and electronic protection: In order to comply with the principle of data security, the Company stores the data at its seat on a server with physical protection (the server is accommodated in a room with special security door with restricted access: it is only the Company's Data Protection Officer who is authorize to open it. Beside this restricted access the server is protected by a multi-level password system. Daily savings are made of the data stored on the server and the saved material is archived encoded.

Archiving and erasing of personal data: After the conditions set down in the Infotv. have been fulfilled, the Company shall archive the data in unidentifiable form in a way that they cannot be restored or retrieved. The archived personal data shall be erased from the electronic system used by the Company for and in connection with its debt collecting activities and shall be saved, encoded, on storage units also physically distinct from the above. It is in this way that the Company secures that the data archived encoded and erased from the active system cannot be linked to the active system. The anonymized encoded form can be reversed and retrieved only for the purposes set down in law (e.g., in case of official requests, check, judicial proceedings, revision by the tax authorities, etc. and only the Company's Data Protection Officer shall have the authority to reverse them. It is the duty of the Data Protection Officer to elaborate the technology of encoding and retrieving personal data, as well as monitoring and developing this technology.

Duration of the control of archived data: The data control period for the archived data and the recorded calls for the Company as data controller shall be calculated in the same way as the prescription period, that is, according to the provisions of the Civil Code (Ptk. by the Hungarian abbreviation) and the rules of consumer protection; it shall typically be 5 years. For the invoices for which the Act on Accounting prescribes a longer period, the period of data control shall be this longer period, i.e., 8 years calculated from the date of closure).

Data transmission records: As data controller, following the checking of the lawfulness of data transmission the Company shall keep record of data transmissions, so that the data subjects could be informed. Such records shall include the dates when personal data controlled by the Company were transmitted, the legal basis for and the addressee of the data transmission, the scope of personal data transmitted and other data as may have been prescribed in the statutory provision prescribing data transmission.

Data transmissions: In the skeleton of data transmission the Company shall transmit the following data and for the following purposes: i) in case that service upon the debtor by postal services was impossible, then the name, place and date of birth and mother's maiden name of the data subject to the Residence Records of the Ministry of the Interior (Belügyminisztérium, Lakcímnyilvántartó (1094 Budapest, Balázs Béla u. 35.)) either online or in hard copy, ii) if the debtor could not be found by phone, to then persons entrusted with paying to them personal visits. They will get the data inevitable for managing the claim, iii) if the debt shall be recovered by legal way, all data relevant to it to the law office entrusted with the plea, iv) all data related to the claim to the beneficiary thereof (i.e., the Principal. In the later case an explicit consent by the data subject concerned is a must.

Data protection and secrecy

Secrecy of the data controlled by the Company: The personal data controlled by the Company according to the Policy also classify as bank secrets under the Hpt., insurance secrets under the Bit., securities secrets under the Tpt., business secrets or private secrets under Act IVT1959 (**Ptk.,** by the) Hungarian abbreviation. With these in mind, in the course of data control under the present Policy the Company shall take the following measures to prevent that third parties accessing without proper authority the Personal Data controlled. The various levels of data protection and secrecy measures are as follows:

1) intra-company measures;
2) contact with the Principals;
3) data transmission to sub-contractors;
4) communication with debtors.

Intra-company measures: Based upon Act I/2012 on the Labour Code (**Mt.,** by the Hungarian abbreviation) employees must keep the Personal Data they come in possession of during their work secret and this obligation shall survive the termination of their employment. The Company shall have its employees sign a declaration in the form and with the contents as shown in the template enclosed as annex 1 hereto (this is the so-called **Employees' Data Protection and Secrecy Declaration**.

The Company shall elaborate various levels of authorities (various access levels) for their employees for the electronic and physical access to Personal Data. The technical details of this are laid down in the IT Policy. The principles of elaborating the various access levels are: i) employees contacting only a specific circle of debtors should be made familiar only with the Personal Data handed over by the Principal affected, would work only with these data and have only a limited authority to amend, erase or archive data; ii) unrestricted access to Personal Data shall have only the senior officers of the Company (a more detailed description of who the senior officers are can be found in the Organization and Operating Policy. The term "full access" shall mean such authorities that allow modification, erasure and archiving of Personal Data. It is the duty of the management to set the access levels; to implement, check and regularly supervise the access levels is the task of the Data Protection Officer who shall report quarterly on the operation of the access levels, practical experiences and problems, if any.

Contracts with the Principals: The Company shall use its best efforts to observe the secrecy provisions of the contract of agency concluded with the Principal and have its employees and sub-contractors fully observe them, too. During the operations it executes on the Personal Data and when entering into contact with the Debtors, the Company shall comply with the instructions of the Principal. If the instruction received is unprofessional or unlawful, the Company may refuse to obey it. Should this be the case, then the Company shall inform the Principal respectively. If the Company detects any problem in connection with the Personal Data or the physical or electronic data carriers on which they are, it must notify the Principal immediately. The Company shall provide for the physical or electronic data connection with the Principals to be protected. The forms elaborated for data transmissions with the Principals shall be supervised by the Data Protection Officer who shall also make motions for their development.

Contact with the sub-contractors: Irrespective of the form under which they contract with the Sub-contractor (service contract or some other legal relation to regulate a labour relation) the Company can engage in the completion of the assignment given to it by the Principal only persons/entities who have signed a Supplier's Data Protection Declaration. The Company's Data Protection Officer shall keep records of the Data Protection Declarations signed by Sub-Contractors. The Sub-Contractors' access to Personal Data shall be on a need-to-know basis. Prior to actually making any data transmission, the Company shall notify the Principal of the Company's intent to transmit the Personal Data of the Principal's Debtors to a Sub-Contractor and shall indicate which data to whom it wishes to transmit.

Contacting Debtors: The Company may contact Debtors in writing (by postal letter, e-mail text message) or verbally (by phone or in person). When entering into touch with the Debtors the Company shall pay utmost attention to hindering unauthorized parties learning any Personal Data that may classify as secret and/or confidential information. To ensure this, the Company shall ascertain the identities of Debtor as set down in the part discussing the regulations of client identification in the Debt Management Policy.

CREDITFORTE

CREDITFORTE Kft.
VAT No.: 14656257-2-43
Company No.: 01-09-345193
Seat: 1118 Budapest Gombocz Z.u.14.
Data control identifier: 02807-0001

CONTACT DATA:
Mailing address: 1506 Budapest Pf.74.
E-mail: info@creditforte.hu
Web: http://awww.creditforte.hu

The rights of Debtors and the enforcement thereof

Applications and request by the Debtors: A Debtor may ask the Company a) to furnish to him/her information on the control of his/her personal data, b) to rectify the Debtor's Personal Data c) and with the exception of those that are obligatory to be controlled, erase or block his/her Personal Data. At the Debtor's request the Company shall inform the Debtor (data subject) of the Debtor data controlled and processed by the Company, the source(s) of these data, purpose, legal basis and duration of data control of if the data subject's personal data has been transmitted, then on the addressee and the legal basis of the data transfer.

Information to the Debtor: The Company shall answer in writing to all the questions of the data subject the soonest practicable after the receipt of his relevant request. The maximum term available for answering is 30 days. The answers shall be clear, unambiguous and free of charge.

Replacement (rectification) of the data: If, based on the Debtor's declaration or otherwise the Company comes to the conclusion that the Personal Data of the Debtor are no more true or correct, but the true and correct Personal Data are available to the Company as data controller, then the Company can replace the erratic Personal Data with the correct ones and rectify them.

Erasure or blocking of Personal Data: The Personal Data shall be erased a) if their control is unlawful, b) the data subject asks for their erasure based on Section 14(c) of the Infotv; c) if they are incomplete or erratic and it cannot be lawfully remedied. However, erasure is not possible even in this case if it is prohibited by law; d) the purpose of the data control no more exists or the statutory storage period of the data has elapsed; e) if any court or authority so orders. Instead of erasing, the Company shall block the personal data if the data subject so requests or, based on the information available, erasure would probably breach the rightful interests of the data subject. The Personal Data so blocked can be controlled only as long as the purpose of data control which makes the erasure of personal data impossible subsists.

Information on rectifications, erasures, blockings and markings: The data subject (Debtor), Principal and all those to whom the data were sent previously shall be notified of rectifications, blockings, markings and erasures No notification must be sent if, taken the purpose of the data control, this will not curtail the rightful interests of the data subject. If the Company rejects the Debtor's request for rectification, blocking or erasure, then it shall notify the Debtor in writing within 30 days after having received the application of the factual and legal reasons and grounds of the rejection. If the application for rectification, erasure or blocking has been rejected the Company must brief the Debtor also of the judicial legal remedy and of the opportunity to apply to the Authority.

Protest against the control of Personal Data: The Debtor may protest against the control of the Debtor's Personal Data, if a) the control or transmission of personal data serves only the fulfilment of a legal obligation of the Company, or except that data control is obligatory it is necessary for enforcing the rightful interests of the data controller, data receiver or a third person; b) the personal data are used or transmitted for the purposes of direct marketing, or making opinion polls or scientific research c) in other cases determined by law. The Company, as data controller shall examine the protest against data control the soonest possible, but within 15 days, at the latest decide, if the protest is well-founded or not, take it decision and inform the applicant thereof in writing. If the Company, as data processor, rules that the protest was well-founded, then the data control, including also the taking of newer data, shall be stopped the data blocked and the Company shall notify of the protest and the measures taken based on it all, to whom the Personal Data forming the subject-matter of the protest have been transmitted previously and warn them that they are obliged to take appropriate measures to enforce the rights of protestor.

If the Debtor does not agree with the decision of the Company, or the Company does not keep the deadline for answering then, within 30 days after communicating to him/her the decision or within 30 days calculated from the last day of the term during which the Company ought have answered to him/her, the Debtor may turn to court or can lodge a complaint with the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information.

According to the provisions of the Infotv. NAIH shall consider your complaint only insofar you have already asked our Company to settle your complaint and you disapprove the answer we have sent.

Creditforte Kft.
Seat: 1118 Budapest Gombocz Z. u.14.
Mailing address: 1506 Budapest, Pf. 74.
Website: www.creditforte.hu
Phone number: 06 1 5100 832
E-mail: panaszkezeles@creditforte.hu

Requirement to inform the Debtor

Written information: The Company shall inform the Debtor at the start of the data control, after the Personal Data received from him/her have been entered into the IT system of debt management that his/her data are recorded in the system. The respective notification shall be sent in writing, by mail.

Processing of the data

The Company can carry out technical operations with or on the Personal Data also without the approval of the data subject, if during this the Company is not going to take on its own any decision of the merits. When recording their data, Data Processors or their Principals shall inform the data subjects of the persons of the data processors involved.
An appointment to process data must be laid down in writing, in the form of a contract that shall include the following elements:

- names of the data controller and data processor
- description of the data processing activity
- scope of the personal data to be transmitted and if data processing shall be automated then the method applied and its logics
- the data controller's guarantee for the data transmitted and their lawful control
- a statement by the data processor that the data cannot be used for any purpose other than set down in the contract
- a covenant by the data processor to comply with the data security regulations
- provisions regulating what shall happen with the data in case that the contract terminates or is terminated
- a provision stipulating that it shall depend on the instruction given by the data controller to this end, whether the processor can or not involve other data processor(s) in data processing.

Automated data processing

During the automated processing of Personal Data the following shall be secured

- no unauthorized data entries can be made
- no unauthorized persons can use the systems
- should there be a malfunction, the systems installed can be retrieved

When determining and applying the measures of data protection the data controller shall take into consideration the technical level of that time and shall chose to apply – if the costs are not disproportionate – the one offering the highest level of data protection.

Circle of people authorized to have access to the data grouped as per legal bases of data control

Titles of data control	Description of jobs and positions with access to the data	Description of activities
Management of the receivables of the Principal in the Principal's name and for his/her account	call centre operators personal case managers complaint handling staff administrative staff operative, IT and customer service staff	registering, recording, systemizing, identification, maintenance and anonymization of data, making of inquiries and searches for data, data transmission to the authorities, data collection according to the purpose limitation principle
Personal visit, study of the environment with a view to settle the claim	call centre operators, personal case managers, visitors	registering, recording, systemizing and identification of data
Recording conversations by phone	call centre operators, complaint handling staff, operative, IT and customer service staff	systemizing, storage, transmission to the Principal or the authority, audio-recording of the phone conversations.
Accounting and fiscal regulations	financial staff, personal case managers	Issuance of invoices, keeping records of the financial transactions, rectification of the data of the audits find it necessary and data transmission to Principal and the authorities
Handling of complaints	complaint handling staff, administrative staff	collection, registering, recording, systemizing, maintaining, erasing, anonymization, data or transmitting them to the authorities

The Data Protection Officer and the Controlling Team shall have full access to the data but can perform no operations on them.

The Data Protection Officer and the Data Protection Policy

The Data Protection Officer of the Company is Balázs TÓTH, (phone No.: +36 1 5100832 e-mail: panaszkezeles@creditforte.hu

The tasks of the Data Protection Officer are: i) operative implementation and regular (at least quarterly) revision of the access levels of employees, report on the findings to the management; ii) supervision of the forms of transmission elaborated with the Principals, and the tabling of motions for their development if their improvement is necessary; iii) keeping records of the Data Protection Declarations made by the suppliers; iv) elaboration and supervision of the coding and de-coding (retrieval) anonymized Personal Data; v) at the request of data subjects informs them of the data subjects' data controlled and processed thereby, their source, the purpose, legal basis, duration of data control, and if the Personal Data of the data subject are transmitted, then the legal basis and the addressee of the transmission; vi) keeping records of data transmissions

Effect of the Policy

The effect of the Policy extends to all data control, data transmission and data processing activities that are performed by the Company in Hungary with respect to the Personal Data of natural persons. The Policy in force at a given point of time can be found on the **www.creditforte.hu** website. The Company reserves the right to amend the present Policy.

In view of the continuously changing legal environment and practice of the authorities the Company shall revise the present Policy annually and implement the changes necessary. During the revisions the Company shall incorporate into the Policy also the changes that took place in its own practice.

Budaörs, 30 June 2020