

PRIVACY POLICY

RELEASE VERSION: **NC-GDPR-03**

EFFECTIVE DATE OF ORIGIN: 2019.11.30.

DATE OF LAST MODIFICATION: 20 25.10.12.

RESPONSIBLE FOR UPDATE: Zoltán Fekete

Prepared by:

Földvári György
Data Protection Officer
Beszerző Központ Kft

Approved by:



Fekete Zoltán
Managing director
Noire Consulting Ltd

TABLE OF CONTENTS...

I. PURPOSE OF THE NOTICE	4
II. DEFINITIONS	4
III. PRINCIPLES OF DATA PROCESSING	7
III.1. Legality, due process and transparency	7
III.2. Principle of purpose limitation	7
III.3 Principle of data minimisation	8
III.4 Accuracy	8
III.5. Principle of limited storage	8
III.6. Integrity and data security	8
III.7. Accountability	8
IV. LEGAL BASIS FOR DATA PROCESSING	9
V. DATA PROCESSING PROCESSES	9
V.1. Processing of personal data related to employees and contributors	10
V.2. Processing of personal data of job applicants	14
V.3. Processing of personal data related to the employees of potential and actual customers acquired in the course of its business activities	15
V.4. Processing of personal data related to the sending of business newsletters	17
V.5. Data Subjects who have come into contact with the data controller's own data backup for their own purposes,	18
V.6. Processing of the personal data of Data Subjects who are not in contact with the management and monitoring of postal, email, calendar and network traffic as employees of the Data Controller	19
V.7. Data processing related to quality assurance, education, complaint handling, enforcement of the rights of Data Subjects	20
V.8. Data processing related to Google Adwords and other Cookie management of the website	22

V.9. Data processing in the Facebook application _____	26
V.10. In the course of its business activities, as a Data Processing activity, the processing of personal data _____ with orders, agency and business contracts	28
VI. PROCESSING OF PERSONAL DATA FOR STATISTICAL PURPOSES _____	30
VII. DATA PROCESSING AND ACCESS BY THIRD PARTIES _____	31
VIII. DECISION MADE BY AUTOMATED PROCESSING _____	31
IX. RIGHTS OF DATA SUBJECTS AND THEIR ENFORCEMENT _____	31
X. GENERAL DATA SECURITY MEASURES _____	35
XI. WHAT TO DO WHEN AN INCIDENT IS DETECTED _____	35
XII. REDRESS, DATA PROTECTION OFFICER AND OFFICER _____	36
XIII. AUDIT _____	37
XIV. CITED LEGISLATION _____	37
XV. FINAL PROVISIONS _____	37
ATTACHMENTS _____	38
No. 1: Records of data processing activities _____	39
No. 2: List of data processors _____	40
REGISTRATION OF CHANGES _____	41

PRIVACY POLICY

Noire Consulting Kft. (hereinafter referred to as: Data Controller, and in certain cases specified in the given data processing, Data Processor, address: 1173 Budapest, Gheorgheni utca 45. (place of data processing is the same as the registered office); tax number: 23749562-2-42, Central E-mail: info@smartmaster.hu Telephone number: +36-70-319-7843, Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: Info-oAct) and the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the GDPR Regulation) in compliance with its obligation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the GDPR Regulation).

I. PURPOSE OF THE NOTICE

The purpose of this information is to enable the Data Subject to become acquainted with all the essential circumstances of the data processing activities carried out by the Data Controller, as well as the related rights, such as the legal order of the operation of the records kept by the Data Controller, as well as the legal basis of the data processing, the storage period, the enforcement of the requirements of data security, and the possibilities for measures related to incidents.

The Data Controller undertakes to ensure that all data processing related to its activities complies with the requirements set out in this information and the effective legislation.

II. DEFINITIONS

Data: personal data processed by the Data Controller.

Data processing: the performance of technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data.

Data processor: a natural or legal person or an organisation without legal personality, who or which performs the processing of data on the basis of a contract concluded with the data controller, including the conclusion of a contract based on the provisions of the law.

Data processing: any operation or set of operations performed on data, regardless of the procedure used, in particular the collection, recording, organisation, storage, alteration, use,

retrieval, transmission, disclosure, alignment or combination, blocking, erasure and destruction of data, as well as the prevention of further use of data, the taking of photographs, audio or video recordings, and the use of data by a person, as well as the recording physical characteristics that can be identified (e.g. fingerprints or palm prints, DNA samples, iris images).

Principles of data processing: the principles listed in the GDPR regulation, which must be complied with by all data processing processes. These are, in a list, as follows: Legality, fair trial and transparency; Purpose limitation; Data minimization; Accuracy; Limited shelf life; Integrity and data security; Accountability. These concepts are detailed in Chapter III of this document.

Purpose of data processing: the data controller must always determine the purpose of the data processing and the data subject must be informed about it.

Legal basis for data processing: each data processing process must have one of the legal bases set out in the GDPR. In the absence of this, the data processing is not lawful. These legal bases are: Consent of the Data Subject; Initiation of a contract by the data subject or necessary for the performance of a contract; Legal Compliance; Protection of the vital interests of the data subject; Within the framework of a public authority; To protect the legitimate interests of the Data Controller or a third party.

Data controller: a natural or legal person, or an organisation without legal personality, who, either independently or jointly with others, determines the purpose, legal basis and method of data processing (storage period, scope of data to be collected, method of processing), makes and implements decisions concerning data management (including the means used), or has it implemented by a data processor commissioned by it.

Data marking: the identification of data for the purpose of distinguishing it.

Data destruction: the complete physical destruction of the data carrier containing the data.

Data deletion: making data unrecognizable in such a way that it is no longer possible to recover it.

Data transfer: making data available to a specific third party.

Data Protection Officer: an employee of the Data Controller appointed by the organization to deal with the protection of personal data.

Data Protection Officer (DPO): an expert appointed by the organisation with knowledge of the general and sectoral legislation affecting the protection of personal data. It can be an external agent or an internal employee.

Data blocking: the identification of data for the purpose of restricting its further processing permanently or for a specified period of time.

Data subject: any specific natural person identified or identifiable – directly or indirectly – on the basis of personal data.

GDPR Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The Regulation is directly applicable in all EEA Member States, including Hungary.

Third party: a natural or legal person, or an organisation without legal personality, who or which is not the same as the data subject, the data controller or the data processor.

Consent: a voluntary and explicit expression of the data subject's wishes, based on appropriate information and giving his or her unambiguous consent to the processing of personal data concerning him/her, in full or in the case of certain operations.

Incident: an incident is when data security is breached, which results in the accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access of the stored, processed or transmitted data.

Contributor: A natural person who participates in the given data processing process as an employee of the data controller, or as an employee, agent or sole proprietor of a subcontractor working on behalf of the data controller.

Sensitive personal data: the scope of personal data defined by the GDPR regulation that must be strictly protected. Such data are only the following: health data, political, sexual, religious orientation, ethnicity, trade union affiliation, genetic data, criminal involvement). This type of data is particularly valuable and must be protected in a higher degree of protection, and the GDPR Regulation imposes specific administrative requirements on the processing of this data.

Record-keeping: the organization and storage of data according to a principle.

Personal data: data that can be directly or indirectly linked to the data subject, in particular the data subject's name, identification number, and one or more knowledge specific to his or her physical, physiological, mental, economic, cultural or social identity, and the conclusions that can be drawn from it concerning the data subject. It is considered personal data even if the data controller is not able to establish an indirect connection between the data and the data subject with its own tools, but it is already possible with the help of one or more databases collected by third parties.

Objection: A statement by which the data subject objects to the processing of his or her personal data and requests the termination of data processing or the deletion of the processed data.

III. PRINCIPLES OF DATA PROCESSING

Personal data retains this quality during data processing as long as its relationship with the data subject can be restored, even indirectly with the help of data held by a third party or parties. The Data Controller's data processing is lawful if it complies with all the basic principles set out in this chapter in the course of data processing.

In the course of data processing, the Data Controller ensures the accuracy and exactibility, integrity and security of the data, and that the data of the Data Subject can only be stored for the time necessary for the purpose of data processing.

Personal data may be processed by the Data Controller if the Data Controller has the appropriate legal basis for the data processing.

The Data Subject may become acquainted with all the essential circumstances of the given data processing, the primary source of which is this Policy.

The GDPR requires that all data processing processes comply with all of the following principles:

- Legality, fair trial and transparency
- Purpose limitation
- Data minimization
- Accuracy.
- Limited storage
- Integrity and data security
- Accountability

III.1. Legality, fair procedure and transparency

Personal data can only be processed with the appropriate information of the Data Subject.

Before the start of data processing, the Data Subject shall be informed whether the provision of data is voluntary or mandatory as prescribed by law. The data subject must be informed – in a clear, comprehensible and detailed manner – of all facts related to the processing of his or her data, in particular the purpose and legal basis of data processing, the person entitled to data management and data processing, the duration of data processing, and who may have access to the data (contributors and data subjects, 3rd party). The information must also cover the rights and legal remedies of the data subject in relation to data processing.

III.2. Principle of purpose limitation

The Data Controller processes personal data only for pre-communicated and specified purposes, for the exercise of rights and the fulfilment of obligations. The Data Controller

strives to process only such personal data that is essential for the achievement of the purpose of data processing and is suitable for achieving the purpose. Personal data may only be processed to the extent and for the time necessary for the achievement of the purpose.

III.3. Principle of data minimisation

The Data Controller is only entitled to collect those Data that are essential for the achievement of the purpose set by it. The legitimacy of these data processing ceases when the purpose is fulfilled, so the Data must be destroyed and/or deleted immediately.

III.4. Accuracy

The Data Controller shall endeavour to preserve the accuracy and up-to-date nature of the Data it manages. To this end, you must plan your data processing in such a way that this principle is met. Such procedures may include automatic data checks from other databases, and/or the possibility for the Data Subject to report changes, etc. The Data Controller provides the Data Subject with the opportunity to specify his or her data in all data processing procedures.

III.5. Principle of limited storage

The storage of data is only permitted until the purpose specified in the data processing documentation is met. If the purpose of data processing has been achieved, it is necessary to delete or destroy the data.

III.6. Integrity and data security

The organization is obliged to develop the processes of data management in such a way that the accessibility, modification and deletion of the personal data processed therein is ensured only for the designated contributors and the given data subject with appropriate data security procedures (e.g. passwords, lockable cabinets, clear-desk-policy, etc.). In addition, the data managed by the organization should not be accessible to anyone else. The fulfilment of this principle is primarily detailed in the chapter on the General Data Security Requirements of the Notice.

III.7. Accountability

The organization performing the data processing is obliged to document all data processing procedures in the manner specified in the GDPR law. This documentation must be submitted to the control authority upon request.

IV. LEGAL BASIS FOR DATA PROCESSING

Each data processing process must have one of the legal bases set out in the GDPR. In the absence of this, the data processing is not lawful.

Pleas in law:

- a) Consent of the Data Subject;
- b) Initiation of a contract by the data subject or necessary for the performance of a contract;
- c) To comply with a legal obligation;
- d) To protect the vital interests of the data subject or other third parties;
- e) Within the framework of a public authority;
- f) To enforce the legitimate interest of the Data Controller or a third party.

The transfer of data to a third party other than the Data Controller and the connection of the databases created in the course of different data processing may be carried out if:

- The data subject has consented to this or is required by law, and
- if the conditions of data processing are met for each personal data.

Personal data may also be processed if obtaining the consent of the data subject would be impossible or would entail disproportionate costs, and the processing of personal data is necessary for the fulfilment of a legal obligation to which the Data Controller is subject, or is necessary for the enforcement of the legitimate interest of the Data Controller or a third party, and the enforcement of this interest is proportionate to the restriction of the right to the protection of personal data.

The Data Controller is obliged to comply with the legal provisions related to the processing of the personal data of the data subjects at all stages of data processing.

The data processing carried out by the Data Controller shall be governed by the provisions laid down in the prevailing legislation in force.

V. DATA PROCESSING PROCESSES

The Data Controller processes the personal data collected from its employees or from the Data Subjects who come into contact with it as non-employees, in the course of its activities, in the following cases:

- Processing of personal data related to employees and contributors
- Processing of personal data of job applicants

- Processing of personal data related to the employees of potential and actual customers acquired in the course of its business
- Processing of personal data related to the sending of business newsletters
- Data Subjects who have come into contact with the data subject for their own purposes, about the processing of their personal data
- Processing of the personal data of Data Subjects who come into contact with postal, email and network traffic management and monitoring as an employee of the Data Controller
- Data processing related to quality assurance, Education, Complaint handling, enforcement of the rights of Data Subjects
- Data processing related to the processing of Google Adwords and other Cookies
- Data processing in the Facebook application
- Property protection of properties used for own purposes – with camera
- In the course of its business activities, as a Data Processing activity, it processes personal data through orders, agency and business contracts. (TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP, AICOSOFT AND OTHER ONLINE APPLICATIONS)

V.1. Processing of personal data related to employees and Contributors

Brief description of data processing: In the course of this data processing, the Data Controller performs the data processing procedures that are necessary for its internal operation to comply with the effective legislation, and for the ability to check its employees and other contributors that they achieve the objectives of the Data Controller with their work and that their activities comply with the effective laws in all respects.

Type of Data Subjects involved in Data Processing: Data Subjects who act as employees, external contributors, interns in order to achieve the Business Objectives of the Data Controller.

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing	Data Processors
name of employee, external contributor, trainee student; and contact details obtained during the employment	establishing, performing or terminating an employment relationship or other contractual relationship;	Fulfilment of a legal obligation (Article 6(1)(c) of the GDPR), In the case of	After the termination of the employment relationship, 5 years from the employee's retirement, and	Payroll and labour employee is the managing director of the data controller, the leader of the given working group according to the employee's/contributor's

relationship	ensuring pension entitlements; and compliance with the Accounting Act, and supporting its control.	an External Contributor, the legitimate interest of the Data Controller is a legal basis, which is the fulfilment of the Business and Ownership Goals of the Data Controller. (Article 6(1)(f) of the GDPR)	8 years from the termination of the Enterprise Contract.	position.
annual summary of employee, trainee payroll file, payroll data; personal data related to payroll accounting, accounting data related to the commission fee in the case of an external contributor				wage and labour workers; Managing Director of the Data Controller
birth name of the employee or external contributor;			8 years after the termination of the employment relationship or the Contract of Enterprise.	
employee, place of birth;				
employee, date of birth;				
the birth name of the employee's mother;			8 years after the termination of the employment relationship or the Contract of Enterprise.	
employee pensioner registration number (in the case of retired employees);				
residence of the employee or external contributor or trainee				
the place of residence of the employee or external contributor or				

trainee (if different from the place of residence);				
all details of the identity document of the employee or external contributor or trainee.;				
all data of the official address certificate of the employee or external contributor or trainee, except for the personal identification number;				
the current account number of the employee, external contributor or trainee;				
data of the documents certifying the qualifications of the employee and/or external contributor or trainee.			Until the termination of employment.	
membership in an employee representation organisation;	Statutory compliance with the rules of taxation	Fulfilment of a legal obligation (Article 6(1)(c) of the GDPR),	8 years after the termination of the employment relationship or the Contract of Enterprise.	wage and labour workers. Data Controller.
all data of the employee or	Statutory compliance with	Fulfilment of a legal	8 years after the termination	

contributor or trainee that are essential for the employer for the lawful operation (telephone accounting, journey log);	the rules of taxation	obligation (Article 6(1)(c) of the GDPR),	of the employment relationship or the Contract of Enterprise.	
Management, storage and control of the business e-mail account of an employee or trainee or an external contributor operating at a data controller, or the communication received from it, as well as postal traffic and web traffic.	Maintaining the data security of the data controller. and the fulfilment of the objectives of the Controller's business activities	Legitimate interest of the Data Controller: For the purpose of maintaining data security and fulfilling a business purpose (Article 6 (1) (f) of the GDPR),	End of the second calendar year from the date of data collection.	an employee performing IT tasks or an external contributor, the management of the data controller, as well as the group leader or deputy of the data subject, or a person working in the same position in the case of postal and e-mail mails, due to substitution or work organization.

The Data Controller stores the personal data specified in this section for the period specified in the table. With regard to the personal data of external contributors and underage apprentices, it collects only the data essential for the fulfilment of the contract and legal compliance from the above list.

A brief description of data processing, what would happen if the data subject failed to provide data: without providing the data required in this data processing, the Data Controller is unable to comply with the legal obligations from the point of view of the given employee or external contributor, and in the case of external contributors, the achievement of the Data Controller's goals is not ensured, and it is unable to check its employees on a random basis and to organize its business processes appropriately. In this case, the given employee, intern or external contributor will not be able to work for the Data Controller if he or she refuses to provide the requested personal data.

Description of the transfer of data and the access of organizations other than the data controller by data type: the Data Controller may use external data processors for payroll accounting, work aptitude tests, operation of its IT and security technology devices, which are indicated in the annex to this Notice. The Data Controller only discloses the data processed by

the Data Controller to a further 3rd party on the basis of a legal requirement or a court order, e.g. NAV.

Does the Data Controller carry out profiling with the data? The Data Controller evaluates the activities of the employees several times a year, during which it may also take into account the personal data listed here. Such data include business-related correspondence and other IT traces of employees, interns, contributors.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

V.2. Processing of personal data of job applicants

Brief description of data processing: in this data processing procedure, the Data Controller processes the data necessary for the application of the persons applying to be employees and for the suitability of their jobs.

Purpose of data processing: the purpose of data processing is to assess the job application targeted by the applicant and to maintain contact with the applicant.

Legal basis for data processing: the legal basis for data processing is the data subject's voluntary consent (Article 6(1)(a) of the GDPR). This consent may be withdrawn at any time in writing by the Data Subject.

Type of Data Subjects Involved in Data Processing: Data Subjects who apply for the position advertised at the Data Controller.

Scope of processed data: personal data of the applicant:

- name of the applicant;
- birthplace;
- date of birth;
- mother's birth name;
- residence;
- habitation;
- contact information: phone number, e-mail address;
- a copy of the document(s) certifying your qualification;
- any additional personal data not requested by the data controller, but provided by the data subject;
- CV and cover letter
- an employer's record of the applicant during the recruitment process.

Duration of data processing: until the end of the evaluation of the job application or until the withdrawal of consent (whichever occurs earlier). After the evaluation, the Data Controller will only store the data collected in this way if the applicant has an explicit, unambiguous and voluntary, written consent.

A brief description of data processing, what would happen if the data subject failed to provide data: the Data Subject cannot apply for the jobs advertised by the Data Controller without providing the data required for this data processing.

Description of the transfer of data and the access of organisations outside the Data Controller by data type: the Data Controller may use an external service provider as a Data Processor in connection with its reported activity, which is indicated in the annex to this Notice. The Data Controller only discloses the data processed by the Data Controller to a further 3rd party on the basis of a legal requirement or a court order, e.g. NAV.

Does the Data Controller carry out profiling with the data? The Data Controller uses the data collected in this way to select the Data Subject who applies for its advertised jobs, and thus performs profiling.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Positions of data processors:

- finance, payroll employee(s);
- the professional manager related to the advertised position;
- Managing Director of the Data Controller

V.3. Processing of personal data related to the employees of potential and actual customers acquired in the course of its business activities

Brief description of data processing: the employees of the Data Controller contact potential customers in the course of their business activities. In such cases, contact is first made through the published contact details of potential customers. These contact details, even if they were originally personal data, lose their personal data character with their voluntary disclosure. The initial contact, if successful, is followed by further personal communication prior to the order, in addition to recording the personal data of the appropriate person, which is voluntarily provided by the Data Subject, so the Data Controller considers this as consent by implicit conduct, and then the order/contract is concluded and the related fulfillment takes place, and possibly warranty administration or the follow-up care of the given transaction.

Purpose of data processing: to achieve the business objectives of the Data Controller.

Legal basis of data processing:

- The legal basis for data collected prior to the order/conclusion of the contract is the consent of the Data Subject (Article 6(1)(b) of the GDPR), which can be revoked at any time in the absence of an order or contract.
- In the case of an order or conclusion of a contract, the legal basis for all personal data contained in the contracts is the conclusion of a contract initiated by the Data Subject or the performance thereof (Article 6(1)(b) of the GDPR),
- After the fulfilment of an order or contract, the legal basis for the processing of personal data included in the contract, performance documents and invoice is the fulfilment of a legal obligation (Article 6(1)(c) of the GDPR, Act CL of 2017, the Act on the Rules of Taxation, and Act C of 2000, the Accounting Act and the relevant parts of the Civil Code).

Type of Data Subjects Involved in Data Processing: Data Subjects who communicate with the Data Controller for business purposes.

Scope of processed data:

- Data collected prior to placing an order/contract: name, email, phone number, job title, area of interest, and any other data that the Data Subject provides about himself or his colleagues. These data are recorded by the Data Controller in a system or table supporting commercial processes.
- Data processed in the case of an order or conclusion of a contract: personal data contained in the contract, invoice, certificate of performance, technical documentation.
- After the fulfilment of the order or the conclusion of a contract, the processed data: the scope of personal data used in the contract, technical documentation, warranty administration and invoice

Duration of data processing:

- In the case of data collected prior to the conclusion of the order/contract, until the withdrawal of the consent valid for this data.
- In the case of data processed in the case of an order or the conclusion of a contract: This retention period is overridden by 8 years from the performance of the last invoice or, if other legal provisions specify a longer retention period.
- In the case of data processed after the fulfilment of the order or the conclusion of the contract: 8 years from the performance of the last invoice or, if other legal provisions specify a longer retention period, this retention period will be overridden.

A brief description of data processing, what would happen if the data subject failed to provide data: the Data Subject cannot enter into a business relationship with the Data Controller without providing the data required in this data processing.

Description of the transmission of data and access of organisations outside the data controller by data type: the Data Controller may use an external service provider as a data processor in connection with its present activity, which is indicated in the annex to this Notice. The Data Controller only discloses the data processed by the Data Controller to a further 3rd party on the basis of a legal requirement or a court order, e.g. NAV.

Does the Data Controller carry out profiling with the data? The Data Controller may group the personal data collected in this way according to business cases and according to the criteria of decision-making or influencing persons. This activity allows you to carry out profiling.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Positions performing data processing: the employees managing the given commercial activity, ordering/concluding contracts, as well as the employees participating in the performance and the managing director of the Data Controller.

V.4. Processing of personal data related to the sending of business newsletters

Brief description of data processing: the Data Controller sends out a mass business newsletter electronically a few times a year. The recipients of the newsletters can only be email addresses that are either public, so they have lost their personal data character, or the owner of the given email address, voluntarily, without any significant advantage or coercive factor, has given his consent to receive the newsletter. In such a case, it is the responsibility of the Data Controller to be able to prove this consent.

Purpose of data processing: to support your business activities and to initiate contact.

Legal basis of data processing: in the case of email addresses preserving the nature of personal data, the consent of the Data Subject. (Article 6(1)(a) of the GDPR),

Type of Data Subjects involved in data processing: Data Subjects who subscribe to the newsletter or receive them in any other way.

Scope of processed data:

- name;
- email address;
- area of interest;

Duration of data processing: until the withdrawal of the Data Subject's consent

A brief description of data processing, what would happen if the data subject failed to provide data: if the Data Subject does not give his voluntary consent, he will not receive a business newsletter from the data controller.

Description of the transmission of data and access of organisations outside the Data Controller by data type: the Data Controller does not use an external service provider as a Data Processor in connection with its reported activity. The name of the Data Processors can be found at the Data Controller's location or can be requested by email from the internal colleague dealing with data protection. 3. the Data Controller only transfers the data it processes on the basis of a legal requirement.

Does the Data Controller carry out profiling with the data? The Data Controller does not carry out profiling with the personal data collected in this way.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data collected in this way.

Positions of data processors:

- manager
- Employee in charge of marketing or finance.

V.5. Processing of the personal data of Data Subjects who have come into contact with the data recovery carried out by the data controller for their own purposes.

Brief description of data processing: in the present data processing, the Data Controller saves the IT data stored on all servers and personal computers managed by the Controller for its own business purposes. With the help of this data processing, you can recover a maximum of one year in time.

Purpose of data processing: the Data Controller prepares for the elimination of partial or complete IT disasters and data loss by data backup.

Legal basis of data processing: the legitimate interest of the Data Controller, which is to avoid an IT disaster. (Article 6(1)(f) of the GDPR)

Type of Data Subjects Involved in Data Processing: Data Subjects whose data have been electronically recorded by the Data Controller.

Scope of processed data: it affects all information on the Data Controller's server, as the Data Controller, in order to ensure the most complete restoration and easy handling, has developed its backup procedure in such a way that it makes complete backups of the given directory structure, so it is not possible to further segment it within the IT backup.

Duration of data processing: the duration of data processing is a maximum of 180 days, depending on the size of the server background, as previous backups are automatically overwritten.

A brief description of data processing, what would happen if the data subject failed to provide data: the Data Subject cannot perform any activity involving data processing at the Data Controller without providing the data required in this data processing, as all electronic data recordings are affected by the backup procedure. If the data is not saved, the Data Controller cannot prepare for the averting of an IT disaster or data loss, so its entire operation may be impossible.

Description of the transfer of data and access of organisations outside the Data Controller by data type: the Data Controller may use an external service provider as a Data Processor in connection with its reported activities. The name of the Data Processor can be found on the Data Processor's list at the Data Controller's location, or it can be requested by email to the internal colleague dealing with data protection. The Data Controller only transfers the data it processes to a further 3rd party on the basis of a legal requirement.

Does the Data Controller carry out profiling with the data? The Data Controller does not carry out profiling with the Data Subject's data in this procedure.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Positions of data processor: IT contributor, managing director.

V.6. Processing of the personal data of Data Subjects who are not employees of the Data Controller, who come into contact with postal, email, calendar and network traffic management and monitoring.

Brief description of data processing: due to the consent of the Data Controller or the Data Subject, or other data processing listed in the policy, or the legitimate interest of the Data Controller, the Data Controller checks the content of the email, calendar and network traffic provided by the Data Controller, with the help of the storage of IT logs and logs. It also stores personal data contained in emails received and/or sent by email and postal communications.

Purpose of data processing: to ensure communication between the Data Controller and the Data Subject, by storing and controlling it, and for the purpose of storing and controlling the traffic of the Data Subject through the Data Controller's network.

Legal basis of data processing: if the Data Subject sends a postal letter, email or calendar entry, or provides the Data Controller with his/her email and/or postal address in any other data processing procedure, and uses the IT network established by the Data Controller for the purpose of accessing the internet or any other closed network, he/she consents by implicit

conduct that the Data Controller may send these communications and the logs of network traffic, stored by the Data Subject until further written revocation. On this basis, the legal basis for this data processing is the voluntary consent of the Data Subject (Article 6(1)(a) of the GDPR). If the Data Subject's consent is the legal basis, the Data Subject may withdraw it at any time. If the communication of the Data Subject's postal letter and e-mail is related to any of the other data processing activities listed in this Policy, the legal basis for the processing of the personal data contained in the given communication is the same as that of the data subject instead of the consent of the Data Subject. If the communication or network traffic of the Data Subject violates the legitimate interest of the Data Controller and becomes known to the Data Controller (e.g. unlawful act, illegal content, etc.), then the legal basis for data storage, instead of the consent of the Data Subject, is the legitimate interest of the Data Controller, which is data security (Article 6 (f) of the GDPR). We would like to draw the attention of the Data Subjects to the fact that the data controller will save and archive the data generated in the course of this data processing, from which point onwards the data recorded in the General Data Backup section will be applicable to the data already duplicated in this way. If the legal basis of this data processing is the consent of the Data Subject, the Data Subject may request the deletion of the related entries and personal data, which may entail the immediate verification of the data subject prior to deletion for security reasons, and the Data Controller can only execute the request from the environment performing the data processing, not from the backup system.

Type of Data Subjects Involved in Data Processing: Data Subjects who wish to communicate with the Data Controller in writing.

Scope of data processed: the scope of letters, calendar entries, todos, other objects sent to the postal and email addresses of the Data Controller, as well as the log of network traffic on the Data Controller's IT network.

Duration of data processing: the data are stored from the moment they are generated until the withdrawal of the Data Subject's consent, or in the manner described in other data processing. If the legal basis for this data processing is the legitimate interest of the Data Controller as data security, then the Data Controller will store the personal data processed in this way for 90 days, during which time it will decide whether it is necessary or not to take further legal steps. If the Data Controller takes further legal steps, it shall determine the deadline for the storage of the data within 1 year after the final or final closure of the given case.

A brief description of data processing, what would happen if the data subject failed to provide data: the Data Subject cannot communicate with the Data Controller in writing without providing the data required in this data processing or, if possible, use its IT network.

Description of the transfer of data and access of organisations outside the Data Controller by data type: the Data Controller may use an external service provider as a Data Processor in connection with its reported activities. The name of the Data Processor can be

found in the list of the Data Processor at the Data Controller's location, or it can be requested by email to the internal colleague dealing with data protection. The Data Controller only transfers the data it processes to a further 3rd party on the basis of a legal requirement.

Does the Data Controller carry out profiling with the data? The Data Controller may perform profiling with the data collected in this way with regard to persons and dates by grouping communications and logs.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Positions performing data processing: managing director, IT employee or external contributor, and based on the content of the communication, the employee responsible for the given area is determined.

V.7. Data processing related to quality assurance, education, complaint handling, enforcement of the rights of data subjects

Brief description of data processing: due to legal compliance and its legitimate interest, the Data Controller stores the complaints and requests for enforcement of rights received by it, as well as the communication between Contributors and Data Subjects related to the data processing listed in this notice, investigates the complaints and enforcement of rights and takes measures based on them, and may subsequently check and analyze them. For quality assurance purposes, the head of the group performing the given activity of the Data Controller or his/her designated person may process the information generated in this way after the closure of the complaint handling and enforcement of rights for the purpose of verifying the work of the contributors and for educational purposes. In the latter case, they are anonymized when it is processed. Other participants of the training can only get acquainted with documents that have already been cleared of personal data.

Purpose of data processing: the purpose of the Data Controller is to manage and process the complaints and rights enforced received by the Data Controller, in order to take the necessary measures and to prove compliance with the law, as well as to subsequently analyze the stored communications for the purpose of improving its processes or training.

Legal basis of data processing: until the closure of the complaint or enforcement of rights, the legal basis is necessary to ensure the legal compliance of the Data Controller (Article 6(1)(c) of the GDPR). In the case of the subsequent analysis of closed complaints or enforcements of rights, the legal basis in the case of the preparation of educational material is the legitimate interest of the Data Controller (Article 6(1)(f) of the GDPR).

Type of Data Subjects Involved in Data Processing: Data Subjects who turn to the Data Controller with a complaint or enforcement of rights.

Scope of processed data: the complaint handling of the Data Controller and the enforcement of the Data Subject's rights are carried out in writing. This can be personal minutes, letters sent to his postal and e-mail addresses, and administrative forms. The scope of the processed data always covers the entire extent of the entire audio recording and written documents. Such personal data can be used to identify the Data Subject, to describe the complaint or enforcement of rights, to adjudicate on it, etc... Belong.

Duration of data processing: complaints and enforcement of rights are related to other data processing specified in the Policy, taking into account the deletion periods indicated therein, the specified retention period will be stored for an additional five years after the closure of the complaint. If no retention period is specified for the given documentation, the retention period is five years under the Consumer Protection Act.

A brief description of data processing, what would happen if the data subject failed to provide data: if the Data Subject does not consent to the written recording and management of his complaint or the enforcement of his or her rights in the manner specified in the Policy, he or she cannot file a complaint with the Data Controller or initiate the enforcement of rights.

Description of the transfer of data and access of organisations outside the Data Controller by data type: the Data Controller may use an external service provider as a Data Processor in connection with its reported activities. The name of the Data Processor can be found in the list of data processors at the location of the Data Controller, or can be requested by email from the internal colleague dealing with data protection. The Data Controller only transfers the data it processes to a further 3rd party on the basis of a legal requirement.

Does the Data Controller carry out profiling with the data? The Data Controller may carry out profiling with the data collected in this way by grouping the data related to the person, case or time.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Positions performing data processing: the managing director of the Data Controller and the leader or designated person of the group affected by the complaint.

V.8. Data processing related to Google Adwords and other Cookie management of the website

General purpose of data processing: the Data Controller uses cookies to ensure the daily operation of the website, to prepare website visitor analytics, and for its marketing activities. Cookies are used to:

- Technical operation of the website
- Improving the user experience of the website with convenience cookies

- Collection of data for marketing purposes using 3rd party cookies

Legal basis of data processing:

- In the case of cookies necessary for the operation of the website, the legal basis is the legitimate interest of the Data Controller (Article 6 (1) (f) of the GDPR)
- For all other types of cookies, the legal basis is the consent of the Data Subject (Article 6(1)(a) of the GDPR)

Type of data subjects participating in data processing: the Data Subject who visits the website of the data controller and clicks on the takmaster.hu, smarmaster.hu, homemaster.hu, hotelmaster.hu, hostelmaster.hu, serviceapp.hu, cleaningapp.hu, aicosoft.hu link appearing as an advertisement in Google search.

The name of the data types, the purpose of their use and their storage period: during the visit of the website and with the help of the use of cookies placed on the Data Subject's computer, the following may be automatically recorded:

- The start and end date of the Data Subject's visit,
- Your IP address,
- and in some cases, depending on the settings of the Data Subject's computer, the browser, the type and language of the operating system, the parameters of the Data Subject's device, the settings set by the Data Subject on the website, the subpages visited and the time spent on them.

The storage period of the personal data listed in this table depends on the type of cookie that the data is used. The Data Subject can check the exact name and retention period of their 3rd party cookies based on the table in the 3rd party's data processing policy, the link of which is indicated to help in this data processing. The 3rd party may change the parameters of the cookies without prior notice based on its own right, but the given Data Subject can check it at any time by clicking on the link in the table.

The most important data of cookies and their retention period by category are as follows:

It is essential for the proper functioning of the website

Essential cookies help make our website usable by enabling basic functions such as page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Name	Provider	Target	Expiry
------	----------	--------	--------

Name	Provider	Target	Expiry
www.smartmaster.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.takmaster.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.homemaster.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.aicoSoft.En	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.HotelMaster.En	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.hostelmaster.En	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.serviceapp.En	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.cleaningapp.En	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month

Convenience Cookies

Their cookies provide functionality that is convenient for the Data Subject to use the website, for example, when it remembers where the Data Subject is on a particular website or what their favorite settings are on the website... etc.

Name	Provider	Target	Expiry
www.smartmaster.hu	website development, hosting provider for tarhely.eu	Serves the convenience of using the relevant website	1 month
www.takmaster.hu	website development, hosting provider for tarhely.eu	Serves the convenience of using the relevant website	1 month
www.homemaster.hu	website development, hosting provider for tarhely.eu	Serves the convenience of using the relevant website	1 month
www.homemaster.hu	website development, hosting provider for tarhely.eu	Serves the convenience of using the relevant website	1 month
www.hotelmaster.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.hostelmaster.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.serviceapp.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month

Name	Provider	Target	Expiry
www.cleaningapp.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month
www.aicosoft.hu	website development, hosting provider for tarhely.eu	The goal is to enable basic functions such as navigating the page and providing access to secure areas of the website	1 month

Marketing, Statistical Cookies

These cookies are used to track visitors' website activity. The goal is to publish relevant ads for individual users and to encourage them to be active, which makes our website even more valuable to content publishers and third-party advertisers.

Name	Provider	Target	Expiry
www.smartmater.hu	website development, hosting provider for tarhely.eu	The goal is to publish relevant ads to individual users	1 month
www.takmaster.hu	website development, hosting provider for tarhely.eu	The goal is to publish relevant ads to individual users	1 month
www.homemaster.hu	website development, hosting provider for tarhely.eu	The goal is to publish relevant ads to individual users	1 month
www.aicosoft.En	website development, hosting provider for tarhely.eu	The goal is to publish relevant ads to individual users	1 month

3rd party cookies

When **viewing the Facebook** profile or when the Data Subject visits the application provided by the given service provider, the given service provider may place cookies on his device. The Data Subject can find out more about these at the link (<https://www.facebook.com/about/privacy>) provided in the section "Data processing in the Facebook application".

The Data Controller uses **the Google Adwords** service. In this case, when the Data Subject clicks on the Data Controller's advertisement offered by Google, Google may place a cookie on the Data Subject's computer while redirecting the Data Subject's web browser to the Data Controller's website. You can find more information on this topic on Google's website at <https://policies.google.com/privacy?hl=hu>.

Depending on the browser used by the Data Subject, the Data Subject can find help with the management of cookies at the following links:

- **Internet Explorer:** <https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies>
- **Firefox:** <https://support.mozilla.org/hu/kb/weboldalak-altal-elhelyezett-sutik-torlese-szamito>
- **Chrome:** <https://support.google.com/chrome/answer/95647?hl=en>

A brief description of data processing, what would happen if the data subject did not provide data: cookies are small text files that are downloaded to the Data Subject's computer when using the website. These files are capable of collecting further data from the metadata of the websites viewed by the Data Subject. This data is transmitted to the owner of the cookie.

- The website, without the cookies necessary for its operation, would not function properly or would not be secure enough.
- The website, without convenience cookies, requires the identification of the Data Subject again on each visit, and does not remember the pages viewed.
- The website, without marketing cookies, cannot advertise itself online and cannot collect analytical information.

Description of the transfer of data and access of organisations outside the data controller by data type:

- Tarhely.eu
- You may use an additional data processor based on the annex to the Policy.

Does the Data Controller carry out profiling with the data? If so, for what purpose. The Data Controller does not carry out profiling, as it does not collect historical data about website visitors.

Does the Data Controller carry out an automated decision-making procedure with the data? The Data Controller does not carry out an automated decision-making procedure with the data it processes.

Who has access to the personal data collected in the course of data processing within the data controller's organisation? The administrator of the Data Controller's website, the employee providing IT support, or an external contributor and managing director.

V.9. Data processing in the Facebook application

Brief description of data processing: in the present data processing, the Data Controller uses social applications provided by third parties for marketing purposes, in order to strengthen its presence in the online space, to strengthen customer loyalty, and to be able to present its marketing messages to its potential customers as widely as possible.

- Applications used: **Facebook.**

All applications operate on a similar principle, the Data Subject may indicate their liking/following/subscription to the Data Controller's profile, i.e. in general, their intention to interest the Data Controller. Upon indicating the intention to be interested, the Data Subject gives his/her voluntary consent to the use of his/her data for marketing purposes, and this is when this data processing begins. The Data Subject gives his/her consent voluntarily, and he/she does not suffer any substantial influence or significant, quantifiable business advantage or disadvantage in exchange for the provision or non-indication of interest.

In the course of Data Management, the Data Controller may get acquainted with those parts of the personal data stored in the application already indicated by the Data Subject who has already indicated his or her intention to be interested, which are set up in the given application as freely viewable data, and may group the interested Data Subjects according to geographical, temporal and other marketing aspects, and may be contacted with various marketing messages.

Data Processing shall continue until the Data Subject terminates his/her intention to interest linked to the Data Controller's profile in the given application, thereby withdrawing his/her voluntary consent as implicit conduct. The granting or withdrawal of the Data Subject's voluntary consent is handled separately by the Data Controller, so if the Data Subject withdraws his or her voluntary consent in one application, it only applies to that application and the marketing messages and contents contained therein. If the Data Controller has given its voluntary consent in another application, the Data Controller will still lawfully process its personal data through those applications and can conduct marketing communication with the Data Subject, until the voluntary consent for those applications is withdrawn.

Purpose of data processing: data processing is carried out for marketing purposes, in order to strengthen your presence in the online space, to strengthen customer loyalty, and to be able to present your marketing messages to your potential customers as widely as possible.

Legal basis for data processing: voluntary consent of the Data Subject (Article 6(1)(a) of the GDPR). This voluntary consent may be unilaterally withdrawn by the Data Subject at any time. The Data Subject may give voluntary consent by following/subscribing/liking the profile of the Data Controller, while the withdrawal of consent may be made by unfollowing/subscribing/liking.

Type of Data Subjects Involved in Data Processing: Data Subjects who have indicated their intention to like/follow/subscribe in the Facebook application, i.e. their intention to be interested in them in general, by which they have given their voluntary consent to the processing of their personal data for marketing purposes to the Data Controller.

Scope of processed data: in the given application, in the setting of the Data Subject's own profile, the Data Controller becomes aware of the authorized data.

Duration of data processing: until the withdrawal of voluntary consent in the given application.

A brief description of data processing, what would happen if the data subject failed to provide data: if the Data Subject does not give his or her Voluntary Consent to the Data Controller, he or she will not be informed about the Data Controller's marketing messages through these applications.

Description of the transfer of data and access of organisations outside the data controller by data type:

Each of the companies owning the respective applications, individually also as independent data controllers and, in conjunction with Noire Consulting Kft., are considered joint controllers with regard to the personal data of the Data Subject known by Noire Consulting Kft. and stored in the given application. Data Subjects are advised to carefully review their personal data settings for the respective application to see which ones they leave publicly viewable. The privacy policy for the respective applications is available at the links below.

- Facebook Inc. <https://www.facebook.com/about/privacy>

Does the Data Processor carry out profiling with the data? The Data Controller may carry out profiling with the personal data of the Data Subjects thus obtained from the point of view of the data subjects, whether in terms of time, geographical location, business activity and marketing.

Does the Data Processor carry out an automated decision-making process with the data? The Data Controller does not carry out an automated decision-making procedure with these data.

Positions performing data processing: Managing director, technical coordinator, system engineer of the data controller, and if they are listed in the annex containing the data processors, the webmaster's contributor and marketing contributor.

V.10. In the course of its business activities – as a Data Processor activity – the processing of personal data with orders, agency and business contracts.

Brief description of data processing: this section deals with data processing related to activities when Noire Consulting Kft., not as an independent data controller, but as a data processor, on the basis of an order, or on the basis of an agency or business contract, and during this period, with the authorization of its client/client, acts as a data processor. Only in this section Noire Consulting Kft. is hereinafter referred to as the Data Processor. On behalf of the Data Controller, the Data Processor provides the following online applications: TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT online applications to its customers/contractors, who in the current situation are the owners of the data uploaded to it, so they have the legal status of data controllers. In the course of these activities, the given application has access to the environment, which is considered data processing from the point of view of the personal data stored there. In the course of this data processing, you may have access to all data stored in the given application environment with the authorization of the Data Controller. After the termination of the order or the assignment/business contract, the Data Processor deletes the data stored in the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT environments and the access to the data stored in the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, and AICOSOFT environments on the basis of the contract, or, if this is not specified in the given legal relationship, within 3 i.e. three days from the date of invoicing.

The Data Processor keeps a Data Processor record of its orders, assignment/business contracts, and what personal data it has access to based on them. In the Data Processor Register, it keeps all orders, assignments/business contracts on the basis of which the given Data Controller has access to the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications.

Purpose of data processing: the purpose of the Data Controller can be found in the data processing information of the given Client. Noire Consulting Kft., as a data processor with an order or a contract/contract, provides the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications exclusively for the purposes specified therein, and does not use the data processed in this way as a data processor for any other purpose.

Legal basis of data processing: in the case of this data processing, Noire Consulting Kft. acts as a data processor, on the basis of a valid order, or an agency or business contract. In such cases, the client must provide the legal basis for data processing.

Type of Data Subjects involved in data processing: Data Subjects can be identified from the data processing information of the client/client.

Scope of processed data: In the course of its business and data processing activities, the data uploaded by the data controller to the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications is processed by Noire Consulting Kft. The exact knowledge of these data can be found in the data processing information of the client/client.

Duration of data processing: until the termination of the given order or assignment/contractor's contract, Noire Consulting Kft. may process the data processed in this way. After the termination of the legal relationship, or based on the provisions of the order/contract, within the deadline, or if this is not mentioned in the document establishing the legal relationship, it will be deleted after 3 days after the termination of the legal relationship, with the exception of the event logs of the online services. The Data Controller authorizes the Data Processor and accepts that until the dispute is resolved, the Data Processor may retain the personal data provided by the Data Controller and use it for the purpose of dispute resolution.

The event logs of the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications will be deleted by the Data Processor within 60 days after the guaranteed retention period specified below. The retention period of the logs provided by the Tárhely.eu service provider related to access to the server is a maximum of 14 months. The event log can contain information about which ip address and what activities were performed. however, the data owned by the customer and consciously uploaded by the data controller in the course of the provision of the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications are not recorded to the data processor.

If the individual legal relationship established with the client/client, i.e. the data controller, provides otherwise for the retention periods and deletion deadlines, the provisions of the given legal relationship shall apply, about which the data subject may request written information.

For its own purposes, the data processor does not store any data previously received within the framework of the given legal relationship, unless otherwise ordered by law.

Brief description of data processing, what would happen if the data subject failed to provide data: The Data Subject can learn about these circumstances from the data processing information of the organization ordering/commissioning the data processing activity. From the point of view of the data processor, if the data controller does not accept the terms and conditions of this data processing, it will not be able to use the data processor's service, i.e. the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications.

Description of the transmission of data and access of organisations outside the data controller by data type: the Data Processor may use an external service provider as a sub-processor in connection with its reported activity. This sub-processor has been accepted by its client/principal, provided that it does not raise a written objection against it. The name of the Sub-Processor can be found in the appendix to this Privacy Policy or can be requested by email from the internal colleague dealing with data protection. The Data Processor only discloses the data processed by the Data Processor to a further 3rd party on the basis of a legal requirement or a court order.

Does the Data Processor carry out profiling with the data? The Data Processor provides the opportunity to profile the data of the Data Subjects included in the TAKMASTER, SMARTMASTER, HOMEMASTER, HOTELMASTER, HOSTELMASTER, SERVICEAPP, CLEANINGAPP and AICOSOFT applications in a predetermined manner, such as the number and quality of the tasks assigned and performed for the given Data Subject, but it may only do so on the basis of the instructions of the Data Controller. The Data Subject can find out more about this from the data processing information of the client/client.

Does the Data Processor carry out an automated decision-making process with the data? The Data Processor does not carry out an automated decision-making process with the data it processes.

Positions performing data processing: contributors involved in the performance of the given contract and the managing director of the data processor. If the contributor is an external organisation, it is included in the Annex describing the data processors of the Prospectus.

The data processor shall carry out its data security measures in accordance with the provisions set out in the GENERAL DATA SECURITY MEASURES of point X.

VI. PROCESSING OF PERSONAL DATA FOR STATISTICAL PURPOSES

Unless otherwise provided by law, the Hungarian Central Statistical Office may take over the personal data processed within the framework of mandatory data processing for statistical purposes, in a manner suitable for individual identification, and may process them in accordance with the provisions of the law.

Personal data recorded, received or processed for statistical purposes may only be processed for statistical purposes, unless otherwise provided by law. The detailed rules of the processing of personal data for statistical purposes are determined by separate legislation.

VII. DATA PROCESSING AND ACCESS BY THIRD PARTIES

The Data Controller is entitled to use Data Processors to perform sub-tasks. The list of data processors, their activities and the list of data types available to them are included in the Annex to this Policy.

VIII. DECISIONS AND PROFILING BASED ON AUTOMATED DATA PROCESSING

A decision based on the assessment of the personal characteristics of the Data Subject may only be made by automated data processing if the Data Subject is provided with the opportunity to review during the decision, in which case the review is carried out by a natural person.

At the request of the data subject, the data controller shall provide information on the method used in the decision made by automated data processing and its essence. The data subject has the right to express his or her position.

The Data Controller does not carry out automated decision-making.

The Data Controller may carry out profiling activities in the data processing where it has indicated this in Section V of this Policy.

Profiling is not automated.

At the request of the data subject, the data controller shall provide information on the method used in the course of profiling and its essence. The data subject shall have the right to express his/her position and to request the Data Controller to change his/her decision. In such a case, the Data Controller is obliged to reconsider its decision to ensure that it has complied with the conditions and legal requirements set by it in all respects.

IX. RIGHTS OF DATA SUBJECTS AND THEIR ENFORCEMENT

The following chapter presents the rights of the Data Subjects and details the possibilities of enforcing them. As a basic rule, the Data Subject may exercise any of his rights only to the extent that does not infringe the rights of other Data Subjects. The Data Subject may request any enforcement of his rights in writing (email, postal letter, on-site report) from any employee of the Data Controller or from any data processor acting on behalf of the Data Controller, but in order to speed up the process, it is recommended to contact the person specified in Chapter XII. The Data Controller shall respond to the Data Subject's request on a mandatory basis, primarily in the format in which the request was received. (e.g.: it came by post - it is necessary to send the answer by post.) In all cases, the response must include the

result of the assessment of the application and, if it is negative, the detailed justification thereof, as well as the steps taken or planned on the basis of the application. If the Data Controller deems that further identification of the Data Subject is necessary, a report will be drawn up together with the Data Subject and may request the presentation of the Data Subject's photo ID. The report shall contain the personal data of the Data Subject, the fact that he/she has verified his/her identity, as well as his/her request and the steps taken to do so. If the fulfillment or rejection of the application consists of several steps that are protracted in time, several minutes may be issued for the given steps. The minutes are always made in two copies and one copy belongs to the Data Subject. If it is necessary to take future steps that affect the Data Subject, e.g. the deletion of data, the deadline for such data must also be indicated. The Data Controller shall attach the minutes completed and signed by the Data Subject, shall not use it for any other purpose, and shall make it available to the authority as evidence in the event of an official investigation.

RIGHTS OF DATA SUBJECTS

Right to transparent procedure: the Data Subject may become acquainted with the procedures of storing, processing and processing personal data concerning him/her, and may receive information about the data processing in full, without impairing the rights of other Data Subjects. The Data Subject may exercise this right even before the commencement of data processing, by becoming acquainted with the publicly available Data Processing Policy/Policy of the Data Controller, and may request further information from the person specified in Section XII.

Right of access: the Data Subject may inspect the records containing the personal data kept about him/her, in prior consultation with the Data Controller, without prejudice to the rights of other Data Subjects.

Right to request a copy: the data subject may request a copy of the data collected about him or her and not processed. The Data Controller shall provide a copy of the data collected about the Data Subject at the request of the Data Subject, however, the transfer of the copy of the further derived data is the Data Controller's own decision. The Data Subject may not cause unreasonable costs to the Data Controller with its repeated requests for copies, and if it does, the Data Controller may ask the Data Subject to reimburse the actual direct costs, but the fulfilment of the request is free of charge by default. The Data Controller must comply with the request in the form in which it was received. (E.g. if by post, then postal, if electronically, electronically) In the course of performance, the information must be easy for the Data Subject to read and can be processed with widely used solutions

Right to restriction of data processing: in the event of a legal dispute with the Data Controller, the Data Subject may request the restriction of data processing from the Data Controller, without impairing the rights of other Data Subjects. In this case, the Data Controller will block the data specified in the Data Subject's written request. The Data Controller shall not make any modifications to the blocked data after the blocking. After the

conclusion of the legal dispute, the data processing will continue or be terminated in accordance with the provisions of the resolution resolving the dispute.

Right to object to data processing: the Data Subject may object to any part or all of the data processing concerning him or her to the Data Controller. In such a case, the Data Controller is obliged to examine the lawfulness of the indicated data processing and, if it deems the objection justified, to terminate the data processing immediately.

Right to obtain acquaintance with the profiling procedure: if the Data Controller performs such activity with his/her data, the Data Subject may request the Data Controller to familiarize himself with the methods of the profiling procedure. In such a case, the Data Controller is obliged to provide information about the criteria on the basis of which the profile is created.

Right to access the automated decision-making procedure: if the Data Controller performs such an activity with his or her data, the Data Subject may request to know the aspects on the basis of which the automated decision-making procedure operates.

Right to challenge automated decision-making procedure, to a decision-maker of a natural person: if the Data Controller performs such activity with his or her data, the Data Subject may contest the result of the automated decision-making procedure. In such a case, it is mandatory for the Data Controller to re-examine and review the given procedure by a participating natural person. The result of the review may be the same as the result of the original procedure.

Right to data portability: the Data Subject has the right to request a copy of the personal data collected from him/her, without hindering the work of the Data Controller. The data obtained in this way must be accessible, legible and processable by the Data Subject.

Right to erasure: The Data Subject has the right to request the erasure of personal data concerning him/her, if the legal basis of the Data Processing:

- the Data Subject's consent, or
- the performance of a contract initiated by the Data Subject, which contract was not concluded in the end, or was concluded but has already been performed,
- and in each case, there is no other legal basis for the Processing.

If the legal basis of the Data Processing:

- Statutory provision,
- Legitimate interest of the Data Controller,
- Exercising a public authority or public interest license,
- It is based on the vital interest of the data subject,

it is not possible to delete the personal data relating to the Data Subject.

Right to information: data subjects may request information about the processing of their data. The primary means of information for the Data Subject is the Privacy Policy, and the Data Subject may request information from the Data Protection Officer.

The Data Controller shall endeavour to ensure that the data subjects are informed of the details of the data processing prior to data processing.

At the request of the data subject, the Data Controller is obliged to provide information about the data processed by the data subject, their source, the purpose, legal basis, duration of data processing, the name and address of the data processor and its activities related to data management, as well as – in the case of the transfer of the data subject's personal data – the legal basis and the recipient of the data transfer.

The Data Controller shall provide the information in writing within the shortest possible time from the submission of the request, but not later than within thirty (30) days, in an easily understandable form, upon the request of the data subject. The information is free of charge if the person requesting the information has not yet submitted a request for information in respect of the same set of data in the current year. In other cases, reimbursement may be imposed. Reimbursement of costs already paid must be reimbursed if the data has been processed unlawfully or if the request for information has led to rectification.

The Data Controller may refuse to provide information to the data subject only if it is permitted by law. The Data Controller is obliged to inform the data subject of the reason for refusing to provide information, and is also obliged to inform the data subject of the legal remedies.

Right to rectification: the data subject may request that the controller rectify his or her personal data that has been entered incorrectly. In the event that regular data is provided on the basis of the data to be corrected, the data controller is obliged to inform the recipient of the data supply about the correction, if necessary, and to draw the attention of the data subject to the fact that the correction must also be initiated by another data controller.

Enforcement of the rights of the Data Subject: if the Data Subject detects a violation of the law in data processing, he/she may turn his/her claim for damages directly to the territorially competent court or may file a complaint with the supervisory authority (National Authority for Data Protection and Freedom of Information, 1125 Budapest, Szilágyi Erzsébet fasor 22/c, tel: 391-14-00, e-mail: ugyfelszolgalat@naih.hu, web: <http://naih.hu> hereinafter: NAIH). If the Data Subject turns to the NAIH, he/she acknowledges that the NAIH has no authority to determine compensation for the violation of the Data Subject's rights. If the Data Subject so requests, we recommend that the Data Subject choose to contact the competent court in connection with the alleged infringement.

X. GENERAL DATA SECURITY MEASURES

This chapter presents the security measures that Noire Consulting Kft., whether acting as a data controller or as a data processor, follows in all its data processing.

Noire Consulting Kft. is obliged to ensure the security of the data. To this end, it must take the necessary technical and organisational measures, both for data files stored by IT tools and for data files stored on traditional paper media.

Noire Consulting Kft. ensures the appropriate preparation of the employees concerned in order to enforce the conditions of data security.

The measures described in this section all apply to the data processing described in the Policy. Employees and Contributors have been informed of the safety regulations that have been introduced, such as:

- Password protection for company smartphones
- Protect your desktops and notebooks with Bios and HDD password
- Username/password protection for operating systems
- Password/username protection of applications
- Clear Desk Policy
- Lockers & Offices
- Providing antivirus and firewall solutions
- operation of data backup
- Restrict network access
- Restricting file share access with a username and password
- Block the installation and use of apps outside of your company app profile
- Block non-corporate apps that request access to your device's contact lists.
- The use of cloud services is only possible in the case of a company subscription, subject to a manager's instruction.

Violation of the above safety regulations by employees and contributors may result in consequences appropriate to the given legal relationship, such as written warning, disciplinary and immediate termination of the legal relationship, enforcement of liability for damages.

XI. WHAT TO DO WHEN AN INCIDENT IS DETECTED

If a Contributor or Data Subject has detected an incident in any of the data processing operations, or suspects that it will occur, please report it immediately, but no later than the next working day, at the info@smartmaster.hu e-mail address, to the Data Protection Officer.

The Data Controller shall immediately investigate the report and take the necessary steps prescribed by law.

Personal data is considered a data breach:

- Unauthorized Access/View
- to an unauthorised person
- their disappearance/unauthorized, unplanned deletion
- unauthorized modification/copying/use of data other than the purpose and method of data processing.

XII. REDRESS, DATA PROTECTION OFFICER AND OFFICER

The data subject may submit his/her request for information, correction, deletion or objection to the data protection officer.

Internal colleague of the Data Protection Officer: Zoltán Fekete, Data Protection Officer
info@smartmaster.hu and +36-70-319-7843

The Data Controller is obliged to provide the information in writing in a comprehensible form within the shortest possible time from the submission of the request, but not later than within thirty i.e. 30 days.

The Data Controller may not delete the data of the data subject if the data processing is ordered by law. The processing of the data may be suspended until the given procedure is carried out. The data processing of the personal data relating to the Data Subject will be terminated if the data controller has agreed with the objection or the court has established the legitimacy of the objection.

The data controller shall be obliged to compensate for any damage caused to others by the unlawful processing of the data subject's data or the violation of the requirements of data security. The data controller is exempt from liability if the damage was caused by an unavoidable reason beyond the scope of data processing.

The Data Controller is not obliged to compensate for the damage if it was caused by the intentional or grossly negligent conduct of the injured party.

Personal data that the Data Subject has disclosed on the basis of his or her own decision will lose personal data.

If the data subject does not agree with the decision of the data controller, he or she may turn to the Authority with a complaint or for legal remedy.

National Authority for Data Protection and Freedom of Information: 1024 Budapest, Szilágyi Erzsébet fasor 22/c. <http://www.naih.hu>

XIII. AUDIT

The managers of the organisational units performing data processing at the Data Controller are obliged to continuously monitor compliance with the provisions of the data protection regulations, in particular the provisions of the Policy. At the Data Controller, the data protection officer is obliged to carry out an inspection at least once a year.

XIV. CITED LEGISLATION

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR Regulation)
- Act CLV of 1997 on Consumer Protection
- Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Private Archive Material
- Act C of 2000 on Accounting
- Act CL of 2017 on the Rules of Taxation
- Act I of 2012 Labour Code
- Act CXXXIII of 2005 on the Protection of Persons and Property

XV. FINAL PROVISIONS

In matters not regulated in the Prospectus, the provisions of the referred laws and the Civil Code shall be applied.

The Policy shall enter into force on the day of its publication, which shall be indicated on page 3 of the Policy, and at the same time the previous Privacy Policy shall cease to be effective.

All elements of the Privacy Policy are protected by copyright. Partial and full reuse is only possible with the written permission of the owner, Noire Consulting Kft.

Budapest, 30 November 2019



Zoltán Fekete
, Managing Director of
Noire Consulting Kft.

ATTACHMENTS

- No. 1: Records of data processing activities
- No. 2: List of data processors

No. 1: Records of data processing activities

Adatkezelő szervezet megnevezése, ha van közös adatkezelő, akkor annak megnevezése is:	Noire Consulting Kft 1173 Budapest, Gyergyószentmiklós utca 45. Adatkezelés helyszíne: meggyezik a cég székhelyével
--	---

Adatkezelő adatkezeléssel összefüggésben kijelölt személy, vagy adatvédelmi tisztviselő neve és elérhetősége:	Fekete Zoltán info@smartmaster.hu
--	--------------------------------------

Adatkezelés megnevezése	Adatkezelés céljai	Adatkezelés jogalapja	Az érintettek csoportja	A kezelt adatok kategóriája	Azon szervezetek kategóriái, akik az adatkezelésben szereplő adatokat megismerhetik. (Ide értve a 3. ország és nemzetközi szervezeteket is)	3. országbeli, vagy nemzetközi szervezetnek továbbítása esetén a megfelelő garanciák leírása	Az adatkezelésben érintett adatok törlési határideje
Munkavállalói adatkezelés	A munkavállalók járulék fizetésének, a munkaadó adózási és törvényi megfeleltetésének biztosítása	Jogszabályi kötelezettség betartása (GDPR 6. cikk 1.c.)	Munkavállalók, külső Közreműködők	normál, fokozottan védendő, és különleges személyes adat	beírásművelet, könyvelési, informatikai tevékenységet végző adatfeldolgozók. Lásd az adatfeldolgozói listában.	nincs 3. országbeli továbbítás	változó, az adatkezelési szabályzatban meghatározott
Álláspályázatra jelentkezők adatainak kezelése	Az adatkezelés célja a jelentkező által célzott álláspályázat elbírálása, illetve a jelentkezővel való kapcsolattartás.	Az adatkezelés jogalapja az Érintett hozzájárulása. (GDPR 6. cikk 1.a pont) o A megrendelés/szerződéskötés megelőzően gyűjtött adatokra vonatkozóan az adatkezelés jogalapja az Érintett hozzájárulása (GDPR 6. cikk 1.a), mely megrendelés vagy szerződéskötés hiányában bármikor visszavonható. o Megrendelés vagy szerződéskötés esetén a jogalap a szerződésben szereplő minden személyes adata vonatkozóan a jogalap az Érintett által kezdeményezett szerződéskötés, vagy annak teljesítése (GDPR 6. cikk 1.b). o A megrendelés vagy szerződés teljesítését követően a szerződésben, a teljesítési dokumentumokban és számlában szereplő személyes adatok kezelésekor a jogalap a jogi kötelezettség teljesítése (GDPR 6. cikk 1.c. pont, 2017. évi CL. tv. az Adózási rendjéről szóló törvény valamint a 2000. évi C. tv. a számviteli törvény, valamint a PTK vonatkozó részei).	Azon érintettek, akik munkavállalónak jelentkeznek	normál és fokozottan védendő személye adat.	nincs	nincs 3. országbeli továbbítás	A megpályáztatási pozíció lezárásáig
Az üzleti tevékenysége során szerzett potenciális és tényleges megrendelők munkavállalóhoz kapcsolódó személyes adatok kezelése	Az adatkezelő üzleti céljainak megvalósítása		Az érintettek, akik üzleti célból kommunikálnak az Adatkezelővel.	normál személyes adat	nincs	nincs 3. országbeli továbbítás	változó, az adatkezelési szabályzatban meghatározott
Üzleti hírclevelek	Az üzleti tevékenységének támogatása, és kapcsolattfelvételi kezdeményezése.	A személyes adatok jellegét megíró emailcímek esetén az Érintett hozzájárulása. (GDPR 6. cikk 1.a pont)	A hírclevele felrakozó vagy azokat más módon megkapó Érintettek.	normál személyes adat	nincs	nincs 3. országbeli továbbítás	Érintett hozzájárulásnak visszavonásáig
Általános Adatmentés és Archiválás	Az Adatkezelő az adatmentéssel és archiválással a részben, vagy egy teljes informaitikai katasztrófa és adatvesztés elhárítására készül fel.	Az Adatkezelő jogos érdeke, amely az informaitikai katasztrófa elkerülése. (GDPR 6. cikk 1.f pont)	Azon Érintettek, akik adatai az Adatkezelő informaitikai rendszeribe rögzítésre kerültek	normál, fokozottan védendő, és különleges személyes adat	az informaitikai támogatást végző külső közreműködő, mely megtalálható az adatfeldolgozói listában.	nincs 3. országbeli továbbítás	A mentéstől számított maximum 180 napig.
Nem az Adatkezelő munkavállalóként Érintett postai és/vagy email és/vagy weboldali ürlap kommunikációjának, valamint hálózati forgalmának tárolása és ellenőrzése adatkezelés	Az Adatkezelő és az Érintett közötti kommunikáció biztosítása, annak tárolásával és ellenőrzésével, valamint az Érintett által az Adatkezelő hálózaton keresztül zajló forgalom tárolása és ellenőrzése céljából.	- Amennyiben az Érintett, postai levelet, emailt, vagy webes ürlapot küld, vagy bármilyen más adatkezelési eljárásban az Adatkezelő számára megadja az email és postai címet, valamint az Adatkezelő által kialakított informaitikai hálózaton használja az internet, vagy más zárt hálózati elérési céljából, úgy ráutaló magatartásával hozzájárul, hogy az Adatkezelő ezen kommunikációt, valamint a hálózati forgalom naplót, az Érintett további írásos visszavonásáig tárolja. Ez alapján jelen adatkezelés jogalapja az Érintett hozzájárulása (GDPR 6. cikk 1.a. pont). Amennyiben az Érintett hozzájárulása a jogalap, úgy az Érintett bármikor visszavonhatja azt. - Amennyiben az Érintett postai levél és email kommunikációja jelen Tájkéztatóban felsorolt, valamely másik adatkezeléshez kapcsolódik, úgy az adott kommunikációban szereplő személyes adatok kezelésének a jogalapja, az Érintett hozzájárulása helyett, az adott kapcsolódó adatkezeléssel megegyezik. - Amennyiben az Érintett kommunikációja vagy hálózati forgalma az Adatkezelő jogos érdekét sérti (pl: törvénybe utkozó cselekedet, illegális tartalom stb.) úgy az adattárolás jogalapja, az Érintett hozzájárulása helyett, az Adatkezelő jogos érdeke, mely az adatbiztonság (GDPR 6. cikk 1.f. pont).	Azon Érintettek, akik emailen, postai levélben, weboldali ürlapban kapcsolatba kerülnek az Adatkezelővel, vagy hálózati eszközöket használnak	normál, fokozottan védendő adat	a tárhely és email szolgáltatást végző adatfeldolgozó, mely megtalálható az adatfeldolgozói listában	nincs 3. országbeli továbbítás	Az adatokat a keletkezésüktől az Érintett hozzájárulásnak visszavonásáig, vagy az egyéb felsorolt jogalap megszűnéséig tároljuk.
Mindösszebiztosításhoz, Oktatószóhoz, Panaszkezeléshez, Érintettek jogainak érvényesítéséhez kapcsolódó adatkezelés	Az Adatkezelő célja a hozzá beérkező panaszok és jogérvényesítések kezelése, feldolgozása, a szükséges intézkedések megtételéhez és a jogszabályi megfeleltetés bizonyítása céljából, valamint a tárolt kommunikációk utólagos elemzése folyamatainak tökéletesítése vagy oktatási céljából.	A panasz, vagy jogérvényesítés lezárásáig a jogalap az Adatkezelő jogszabályi megfeleltetésének biztosításához szükséges (GDPR 6. cikk 1. c. pont). A lezárt panaszok vagy jogérvényesítések utólagos elemzése oktatási anyag készítése esetén a jogalap az Adatkezelő jogos érdeke (GDPR 6. cikk 1. f. pont).	Azon Érintettek, akik panasszal, vagy jogérvényesítéssel fordulnak az Adatkezelőhöz.	a panasz jellegétől függően, lehet normál, fokozottan védendő, különleges személyes adat	nincs	nincs 3. országbeli továbbítás	A panaszok és jogérvényesítések a Tájkéztatóban megelőlt egyéb adatkezeléshez kapcsolódik, úgy az ott megelőlt törlési időtartalmakat figyelembe véve, a panasz lezárását követően a megelőlt megőrzési idő plusz öt évig tárolja. Ha az adott dokumentációra nincs megőrzési idő, úgy a fogyasztóvédelmi törvény alapján 5 év a megőrzési idő.
Google Adwords és Weboldali egyéb Cookie kezeléséhez kapcsolódó adatkezelés	Az Adatkezelő, a weboldali napi működésének biztosítása, valamint marketingtevékenysége érdekében cookiekat használ. A cookiek segítségével végli: o weboldali technikail működését o a weboldali felhasználói élményének javítása kényelmi cookiekkel o a marketing célú adatgyűjtés 3. féltől származó cookiekkel	o A weboldali működéséhez szükséges cookiek esetén a jogalap az Adatkezelő jogos érdeke (GDPR 6. cikk 1.f. pont) o Minden más típusú cookiek esetén a jogalap az Érintett hozzájárulása (GDPR 6. cikk 1.a pont)	Az adatkezelésben az adatkezelő weboldali látogató Érintettek vesznek részt.	normál és fokozottan védendő személye adat.	tárhelyszolgáltató és marketing tevékenységet támogató adatfeldolgozó, az adatfeldolgozói lista alapján	USA, Google Inc.	A cookiek típusai alapján eltérő a megőrzési idejük, melyet az adatkezelési tájkéztató részletez
Facebook alkalmazásban történő adatkezelés	Az adatkezelés marketingcélból történik, hogy az online térben megérőltetés jelenlétét, ügyfél hűségét erősítsen, marketing célú üzeneteket minél szélesebb körben ismertetni tudja a potenciális ügyfeleivel.	Az Érintett önkéntes hozzájárulása (GDPR 6. cikk 1.a pont). Ezen önkéntes hozzájárulást az Érintett bármikor egyoldalúan visszavonhatja. Az önkéntes hozzájárulást az Érintett az Adatkezelő profiljának követésével/feliratozásával/kezelésével, míg a hozzájárulás visszavonását a követés/feliratozás/kezelés visszavonásával teheti meg.	Azon Érintettek, akik a Facebook alkalmazásban kedveléseket/Adventéseket/felir atkozásai szándékukat, vagyis általánosságban érdeklődési szándékukat jelezték, mellyel önkéntes hozzájárulásukatadták személyes adataik marketing célú kezelésére az Adatkezelő számára.	normál és fokozottan védendő személye adat. (Az adott alkalmazásban, az Érintett saját profiljának beállításában, az engedélyezett adatokat ismeri meg az Adatkezelő.)	Az adatkezelési tájkéztató adatfeldolgozói melléklete alapján.	USA, Facebook	Az önkéntes hozzájárulás visszavonásáig az adott alkalmazásban. (Vagyis a követés/tetszés megszűnéséig.)
Saját célból használt ingatlanok vagyonvédelme - kamerával	A saját, és kezelt ingatlanok vagyonvédelme - a megfigyelésnek és a képfelvételek rögzítésének a célja az ingatlanok területén tartózkodó személyek életének, testi épségének, valamint az ingatlanok területén tartózkodó személyek, továbbá az ingatlanok, és az ingatlanokon található vagyontárgyak védelme. Ennek keretében cél a jogserőtek észlelése, az elkövető tettenérése, a jogserő cselekmények megelőzése, továbbá, hogy ezekkel összefüggésben bizonyítottként kerüljenek hatósági eljárás keretében felhasználásra.	Az adatkezelés jogalapja az Adatkezelő jogos érdeke, amely a személy és vagyonvédelem. (GDPR 6. cikk 1.f. pont)	Az Adatkezelő saját célra használt ingatlanjainál elhelyezett kamerák létezéséről érkező Érintettek.	fokozottan védendő személyes adat	kamerarendszer karbantartását végző adatfeldolgozó, az adatfeldolgozói lista alapján	nincs 3. országbeli továbbítás	3 munkanap, incidens esetén 30 nap, vagy az Adatkezelő jogos érdekeinek megszűnéséig.
Üzleti tevékenysége során - mint Adatfeldolgozó tevékenység személyes adatok kezelése, megrendelésekkel, megbízási és vállalkozási szerződésekkel.	Az Adatkezelő célja az adott Megbízó adatkezelési tájkéztatójában található. A Noire Consulting Kft., mint megrendelővel, vagy a megbízások/vállalkozási szerződéssel rendelkező adatfeldolgozó, tevékenysége során, kizárólag az ott meghatározott célok érdekében biztosítja a SMARTMASTER, TAKMASTER, HOMAMASTER, SMARTRECORD alkalmazást, és az így, mint adatfeldolgozóként, kezelt adatokat más célra nem használja fel.	Az adatkezelő és az adatfeldolgozó között kötött megbízási/vállalkozási jogviszonyban szereplő felhatalmazás.	Ez egy külön adatfeldolgozó nyilvántartás táblázatban kerül meghatározásra	Ez egy külön adatfeldolgozó nyilvántartás táblázatban kerül meghatározásra	Ez egy külön adatfeldolgozó nyilvántartás táblázatban kerül meghatározásra	nincs 3. országbeli továbbítás	3 munkanap az Adatfeldolgozó szerződés megszűnésétől számítva.

No. 2: List of data processors

Name of the data management organisation, if there is a joint data controller, then also its name:

- **Noire Consulting Ltd**
- 1173 Budapest, Gyergyószentmiklós utca 45.

Location of data processing: the same as the company's registered office.

Subcontractor name	Area	Data type	Seat	Availability
E-Accounting	Accounting office	Billing information	1133 Budapest, Kárpát utca 7/B	e-konyveles.com
Tárhely.eu Ltd	Server service	Customer data, databases	1138 Budapest, Váci út 188.	tarhely.eu
Tóth Sándor EV	Programming, web development	Customer data, databases	4026 Debrecen, Csemete utca 1.	-
Facebook	Marketing	Advertising and marketing	-	facebook.com
Google	Marketing	Advertising and marketing	-	google.com

The data correspond to reality in all respects and are constantly updated as needed.

Budapest, 2025. January 12.



Zoltán Fekete
 , Managing Director of
 Noire Consulting Kft.

REGISTER OF CHANGES		
RELEASE NUMBER	DATE	NAME OF THE EDITION
1.	2019.11.30.	Reprint
2.	2025.01.09.	Revised edition
3.	2025.10.12.	Revised edition