Privacy policy

Name:	Wash Point Kft.
Head office:	Budapest

2018.

I.CHAPTER

GENERAL PROVISIONS

I.1. Introduction

The data controller declares that the data processing activity has been carried out in such a way that it must comply with the applicable laws, regulations and official resolutions in all circumstances, for which purpose appropriate internal rules, technical and organizational possibilities must be put in place.
When issuing these regulations, the Data Controller considers in particular:

- Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 Data Protection Regulation, hereinafter "the Regulation")
- Act CXII of 2011 on the right to information self-determination and freedom of information. (hereinafter: Info Act).

I.2. Purpose of the regulations

1. The purpose of the regulations is to establish the internal rules and to establish measures that ensure that the data management activities of the Data Controller comply with the Decree and the Info tv. and other applicable laws.

2. The purpose of the Regulation is also to ensure that the Data Controller complies with the Regulation and the principles governing the processing of personal data set out therein (Article 5).

3. The purpose of the regulations is also to provide the Data Controller's employees with clear guidelines on their data management processes in the course of their work.

I.3. Scope of the Regulations

1. These Regulations shall apply to all employees of the Data Controller in matters in which they process personal data concerning a natural person or have access to personal data in any way.

2. The rules do not apply to the processing of personal data concerning legal persons, including the name and form of the legal person and the contact details of the legal person.

I. 4. Concept definitions

Definitions for the purposes of these rules are set out in Article 4 of the Regulation. Accordingly, we highlight the main concepts:

1. "**personal data**" shall mean any information relating to an identified or identifiable natural person ("data subject"); identify a natural person who, directly or indirectly, in particular by reference to one or more factors such as name, number, location, online identifier or physical, physiological, genetic, mental, economic, cultural or social identity of the natural person identifiable;

2. "**processing**" means any operation or set of operations on personal data or files, whether automated or not, including the collection, recording, organization, sorting, storage, transformation or alteration, consultation, access, use, communication, dissemination or otherwise made available, coordinated or interconnected, restricted, deleted or destroyed;

3. "**restriction** of data processing" means the marking of stored personal data with the aim of limiting their processing in future;

4. "**profiling**" means any form of automated processing of personal data in which personal data are evaluated for the purpose of assessing certain personal characteristics of a natural person, in particular his performance, economic situation, state of health, personal preferences, interests, reliability, behavior, residence or used to analyze or predict motion-related characteristics;

5. "**pseudonymisation**" means the processing of personal data in such a way that it is no longer possible to determine to which individual the personal data relate without the use of additional information, provided that such additional information is stored separately and technical and organizational measures are taken. ensuring that this personal data cannot be linked to identified or identifiable natural persons;

6. "**registration system**" means a set of personal data which is accessible in any way, whether centralized, decentralized or functional or geographical, on the basis of defined criteria;

7. "**controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of the processing are defined by Union or Member State law, the controller or the specific criteria for the designation of the controller may be determined by Union or Member State law;

8. "**processor**" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

9. "**recipient**" means a natural or legal person, public authority, agency or any other body to whom personal data are disclosed, regardless of whether it is a third party. Public authorities that may have access to personal data in the framework of an individual investigation in accordance with Union or Member State law shall not be considered as recipients; the processing of such data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

10. **"third party"** means any natural or legal person, public authority, agency or any other body which is not the data subject, the controller, the processor or the persons who, under the direct control of the controller or processor, process personal data; have been authorized to handle it;

11. **"consent of the data subject"** means the voluntary, specific and well-informed and unambiguous statement of the will of the data subject to indicate his or her consent to the processing of personal data concerning him or her by means of a statement or unequivocal statement;

12. **"data protection incident"** means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data which are transmitted, stored or otherwise handled.

II. CHAPTER

LEGAL BASIS OF DATA MANAGEMENT

II.1. Data management with the consent of the data subject

1) In the case of data processing based on consent, the data subject's consent to the processing of personal data shall be obtained from the document entitled "Consent Statement" annexed to these Regulations.
2) Consent shall also be deemed to be consent if the data subject checks a box to do so when viewing the Data Controller's website, makes technical adjustments to it when using information society services, as well as any other statement or action in that context. clearly indicates the data subject's consent to the intended processing of his or her personal data. Silence, a pre-ticked box, or inaction is therefore not considered consent.
3) The consent shall cover all data processing activities carried out for the same purpose or purposes. If the data processing serves several purposes at the same time, the consent must be given for all data processing purposes.
4) If the data subject gives his or her consent in the form of a written statement which also covers other matters, e.g. conclusion of a service contract - the request for consent must be made in a way that is clearly distinguishable from these other matters, comprehensible and easily accessible, in clear and simple language. Any part of such a statement containing the data subject's consent which infringes the Regulation shall not be binding. The Data Controller may not enter into the conclusion or performance of a contract to give consent to the processing of personal data that is not necessary for the performance of the contract.
5) Withdrawal of consent should be as simple as giving it.
6) If the personal data have been collected with the consent of the data subject, the Data Controller may process the collected data for the purpose of fulfilling the legal obligation applicable to him or her without further consent and after the withdrawal of the data subject's consent.

II.2. the processing is necessary for the performance of a contract in which the data subject is required by one of the parties or to take steps at the request of the data subject prior to the conclusion of the contract;

The personal data provided at the time of concluding the contract is necessary for the Data Controller to fulfill the contract. This interest is a sufficient legal basis for the processing of personal data. The interest lasts as long as the legitimate interests in the performance of the contract can be asserted - ie until the expiry of the general five-year civil enforcement period following the performance of the contract (except where the law provides for a shorter enforcement period).

II.3. the data processing is necessary to fulfill the legal obligation to the Data Controller

II.3.1 Data management for tax and accounting purposes

The Data Controller manages the data of natural persons who enter into business relations with the customer or supplier for the purpose of fulfilling the statutory tax and accounting obligations (bookkeeping, taxation). The treatment of data is in particular the provisions of Act CXXVII of 2017 on Value Added Tax § 169 and § 202, as well as § 167 of Act C of 2000 on Accounting, respectively.

II.3.2. Payer Data Management

The Data Controller manages the personal data of the data subjects - employees, their family members, employees, recipients of other benefits - required by tax law for the purpose of fulfilling the legal obligation and fulfilling the statutory tax and contribution obligations (tax, tax advance, assessment of contributions, payroll accounting, social security, pension administration). CL of 2017 on the system of taxation. Act (Art.) § 7 31. is related to the payers. The scope of the processed data is defined in Article 50 of the Art. If the tax laws impose a legal consequence on this, the Data Controller may process the data on the members' health (§ 40 of the Personal Income Tax Act) and trade union membership (§ 47 (2) b. Of the Personal Income Tax Act) for the purpose of fulfilling tax and contribution obligations (payroll accounting, social security administration).

II.3.3. Data management for records of permanent value according to the Archives Act

(1) The Data Controller manages the provisions of Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Private Archival Material in order to fulfill a legal obligation. (Archives Act) in order to preserve the permanent value of the archives of the Data Controller in good condition and in a usable condition for future generations. Time of data storage: until handed over to the public archives.

(2) The Recipients Act shall govern the recipients of personal data and other issues of data management.

II.3.4. Data management on the basis of other legal authorization

The data controller processes personal data in the manner and on the legal basis specified in the appendices to these regulations. In view of this, the Data Controller may also process personal data on the basis of separate legal provisions specified in the appendices to these regulations.

II.4 the data processing is necessary to enforce the legitimate interests of the Data Controller or a third party

The legal basis for data processing may also be that it is necessary to enforce the legitimate interests of the Data Controller or a third party. In the case of data processing on the basis of a legitimate interest, it is always necessary to carry out a balancing test as to whether the interest to be enforced outweighs the interest in the protection of personal data. The Data Controller is obliged to present the relevant assessment.

III. CHAPTER

INFORMING THE STAKEHOLDERS

III.1. Irrespective of the legal basis of the data processing, the Data Controller informs the data subjects about the fact of the data processing as follows

The Data Controller shall make the data management information in accordance with the annexes to these Regulations available to the data subjects. The purpose of this prospectus is to inform data subjects clearly and in detail in all publicly available forms before and during the processing of all facts concerning the processing of their data, in particular the purpose and legal basis of the processing, the data subject and the duration of the processing. , and who can access the data. The information shall also cover the data subject's rights and remedies in relation to the processing. This data management information must be made available by marking each of the most important data management steps with a separate link (for example, in the case of a registration before registration, during the registration process, etc.). Stakeholders should be informed of the availability of this information.

IV. CHAPTER

INDIVIDUAL DATA MANAGEMENTS BY THE DATA CONTROLLER

Labor and personnel data

General rules for the processing of labor data

(1) Workers may be required to keep and record only data relating to the establishment, maintenance and termination of employment and the provision of social welfare benefits which do not infringe the worker's personal rights.

(2) Article 6 (1) (b) of the Data Controller's employee data (data processing is necessary for the performance of a contract in which the data subject is required to take steps at the request of one of the parties or before the conclusion of the contract) and c) (data processing is necessary to fulfill the legal obligation to the data controller) for the purpose of establishing an employment relationship, the data specified in the appendix to these regulations.

(3) Article 6 (1) (b) of the Data Controller's employee data (the processing is necessary for the performance of a contract in which the data subject is required to take action at the request of one of the parties or before the conclusion of the contract) and c) (data processing is necessary for the fulfillment of the legal obligation to the data controller) for the purpose of maintaining or terminating the employment relationship.

(4) The employer shall process data on illness and trade union membership only for the purpose of fulfilling a right or obligation specified in the Labor Code.

(5) Recipients of personal data: the head of the employer, the exercise of the employer's authority and his / her superior with the right to instruct, the employees of the Data Controller performing labor duties and the appendix to these regulations.

(6) Data controllers recorded in a register called "register of transfers".

(7) Duration of storage of personal data: As detailed in the appendix to these regulations for each type of data.

(8) The data subject shall be informed before the start of the data processing that the data processing is based on the Labor Code and is necessary for the fulfillment of a contract or the fulfillment of a legal obligation.

(9) Simultaneously with the conclusion of the employment contract, the employer shall inform the employee about the processing of his / her personal data and his / her rights to the person by submitting the Prospectus in accordance with the annex to these regulations.

Data management relating to the control of the use of a business mobile telephone

(1) The employer shall not authorize the private use of a business mobile telephone, the mobile telephone may only be used for work-related purposes and the employer may check the number and details of all outgoing calls and the data stored on the mobile telephone.

(2) The employee is obliged to notify the employer if he has used the company mobile phone for private purposes. In this case, the check can be performed by the employer requesting a call detail from the telephone company and asking the employee to make the dialed numbers unrecognizable on the document for private calls. The employer may require that the cost of private calls be borne by the employee.

(3) In other respects, the provisions of the data management title related to the control of the use of the E-mail account shall govern the control and its legal consequences.

Data management related to camera surveillance at work

(1) The data controller shall use an electronic surveillance system for the protection of property at its headquarters, some premises and premises open to the reception of customers, which enables the recording of images, on the basis of which the data of the data subject shall also be considered personal data.

(2) The legal basis for this processing is the consent of the data subject.

(3) A warning sign and information on the fact of the application of the electronic monitoring system in a given area shall be placed in a clearly visible place in a clearly legible manner in a manner that facilitates the information of third parties wishing to appear in the area. The information must be provided for each camera. This information shall include the fact of the monitoring carried out by the electronic security system and the purpose of making and storing the image and sound recording containing personal data recorded by the system, the legal basis of the data processing, the storage location of the recording, the duration of storage, the system operator (operator) information on the identity of the data subject and the provisions concerning the rights of data subjects and the procedure for enforcing them. A model for the information is given in the Annex to these Regulations.

(4) The recorded recordings may be stored for a maximum of 3 (three) working days if they are not used. Use is considered to be the use of the recorded image and other personal data as evidence in court or other official proceedings.

(5) A person whose right or legitimate interest is affected by the recording of the data of the image recording may, within three working days as of the recording of the image, request that the data controller not destroy or delete the data.

(6) An electronic monitoring system may not be used in a room where monitoring may violate human dignity, in particular in changing rooms, showers, toilets or in rooms designated for the purpose of taking a break from work.

(7) If no one may be legally present in the workplace, in particular outside working hours or on public holidays, the entire area of the workplace (such as changing rooms, toilets, rooms designated for breaks) may be observed.

(8) In addition to those authorized by law, the operating staff, the head and deputy head of the employer, as well as the workplace manager of the monitored area shall have the right to view the data recorded by the electronic monitoring system in order to detect violations and verify the operation of the system.

Contract - related data processing

Management of data of contracting partners - register of customers

(1) For the purpose of concluding, fulfilling, terminating the contract and providing a contractual discount, the Data Controller shall process the data of the natural person contracted with the customer as specified in the appendix to these regulations. Such processing shall also be considered lawful if the processing is necessary to take steps at the request of the data subject before the conclusion of the contract.
Recipients of personal data: employees of the Data Controller performing tasks related to customer service, employees performing accounting and tax tasks, and data processors.
Duration of storage of personal data: 5 years after the termination of the contract.

(2) The data subject shall be informed before the start of the data processing that the data processing is based on the right to perform the contract, this information may also be provided in the contract. The data subject shall be informed of the transfer of his or her personal data to the data controller. The text of the data management information related to the contract concluded with a natural person is contained in this Annex.

Contact details of natural person representatives of customers, customers and suppliers of a legal entity

(1) The scope of personal data that can be processed: the name, address, telephone number, e-mail address and online ID of the natural person.

(2) The purpose of the processing of personal data: fulfillment of the contract concluded with the Company's legal entity partner, business relations,

(3) Legal basis of the data processing: Legitimate interest of the Data Controller (the interest balance examination was placed among the data protection documents of the Data Controller)

(4) Recipients of personal data and categories of recipients: employees of the Company performing customer service-related tasks.

(5) Duration of storage of personal data: 5 years after the existence of the business relationship or the status of the data subject's representative.

Visitor data management on the Data Controller's website - Information on the use of cookies

(1) Cookies are short data files placed on the user's computer by the website you are visiting. The purpose of the cookie is to make the given infocommunication and internet service easier and more convenient. There are many varieties, but they can generally be divided into two major groups. One is the temporary cookie that the website places on the user's device only during a specific session (e.g. during the security authentication of an internet bank), the other is the persistent cookie (e.g. the language setting of a website) that remains until then on the computer until the user deletes it. According to the guidelines of the European Commission, cookies [unless they are absolutely necessary for the use of the given service] may only be placed on the user's device with the user's permission.

(2) In the case of cookies that do not require the user's consent, information shall be provided during the first visit to the website. It is not necessary for the full text of the information on cookies to appear on the website, it is sufficient for the operators of the website to briefly summarize the essence of the information and to indicate the availability of the full information via a link.

(3) In the case of cookies requiring consent, the information may also be related to the first visit to the website in case the data processing related to the use of cookies starts already with the visit to the website. If the cookie is used in connection with the use of a function specifically requested by the user, the information may also be displayed in connection with the use of this function. In this case, it is not necessary for the full text of the information on cookies to appear on the website, a short summary of the essence of the information and a link to the availability of the full information is sufficient.

(4) The visitor shall be informed about the use of cookies on the website in the data management information set out in the annex to these regulations. With this information, the Data Controller ensures that the visitor can find out before and at any time during the use of the information society-related services of the website which data types the Data Controller handles, including the handling of data that cannot be directly contacted by the user.

Data management related to newsletter service

(1) A natural person who registers for the newsletter service on the website may consent to the processing of his or her personal data by ticking the appropriate box. It is forbidden to check the box in advance. During the registration, the Data Management Information according to the appendix to these regulations must be made available with a link. The data subject may unsubscribe from the newsletter at any time by using the "Unsubscribe" application of the newsletter, or by making a written or e-mail statement, which means the withdrawal of consent. In this case, all data of the subscriber must be deleted immediately.

(2) The scope of personal data that can be processed is included in the appendix to these regulations.

(3) The purpose of the processing of personal data is:

1. Sending a newsletter regarding the products and services of the Data Controller

2. Sending promotional material

(4) Legal basis for data processing: consent of the data subject.

(5) Recipients of personal data: employees of the Data Controller performing tasks related to customer service and marketing activities, as employees of the Data Controller's IT service provider for the purpose of performing the hosting service.

(6) Duration of the storage of personal data: until the existence of the newsletter service or the withdrawal of the data subject's consent (request for cancellation).

Data management on the Data Controller's Community page(s)

(1) The Data Controller maintains a Facebook page for the purpose of introducing and promoting its products and services.
(2) The question asked on the Facebook page of the Data Controller does not qualify as an officially submitted complaint.
(3) The Data Controller does not process the personal data published by the visitors on the Facebook page of the Data Controller.
(4) Visitors are governed by the Facebook Privacy and Service Terms.

(5) In the event of the publication of illegal or offensive content, the Data Controller may exclude the data subject from the membership or delete his / her comments without prior notice.
(6) The Data Controller is not responsible for data contents or comments that violate the law published by Facebook users. The Data Controller is not responsible for any errors, malfunctions or changes in the operation of the system resulting from the operation of Facebook.
(7) Facebook acts as a data controller when it displays advertisements to people based on information provided directly by people to Facebook, as well as information that Facebook receives when various websites and applications install the Facebook pixel and SDK . In such cases, the Community side is responsible for complying with data protection regulations.
(8) When using Facebook's "individual target audience based on a data file" product, the Data Controller is responsible for complying with the Data Management Regulations, this is the only case where Facebook acts as a Data Processor. Given that the Data Controller transmits the personal data of the Data Subjects to Facebook. In this case, the Data Controller is responsible for obtaining the consent, and the statement required for obtaining the consent is included in the appendix to these regulations.

(9) The rules of this chapter also apply to the Linkedin, Instagram, Google+, Youtube pages of the Data Controller.

Data management for direct marketing purposes

(1) Unless otherwise provided by a separate law, the method of direct contact of a natural person as the recipient of an advertisement (acquisition of a direct business), in particular by electronic mail or other equivalent means of individual communication - shall be in accordance with Annex XLVIII of 2008. with the exception provided by law - may be communicated only with the prior express and explicit consent of the recipient of the advertisement.

(2) The scope of personal data that may be processed by the Data Controller for the purpose of inquiring about advertising recipients: the name, address, telephone number, e-mail address and online ID of the natural person.

(3) The purpose of the processing of personal data is to carry out direct marketing activities related to the activities of the Data Controller, ie to send advertising publications, newsletters, current offers in printed (postal) or electronic form (e-mail) to the contact details provided during registration.

(4) Legal basis for data processing: consent of the data subject.

(5) Recipients and categories of recipients of personal data: employees of the Data Controller performing tasks related to customer service, employees of the Data Controller's IT service provider providing server services as data processors, employees of the Post Office in the case of postal delivery.

(6) Duration of storage of personal data: until the consent is withdrawn.

(7) These rules apply to consent to data management for direct marketing purposes a "statement of consent" may apply.

Data management related to entry and exit

(1) Data Controller - For its external guests who are not employed by the Data Controller- operates an access control system, the data management information of which is included in the Annex to these Regulations.

(2) The scope of personal data that can be processed is included in the appendix to these regulations.

(3) Legal basis for data processing: Legitimate interest of the data controller.

(4) The purpose of the processing of personal data is the protection of property.

(5) Recipients of personal data: employees of the Management at the Data Controller and the Data Protection Officer of the Data Controller as data processor.

(6) Duration of processing of personal data: 24 hours.

Data management related to camera surveillance

(1) The data controller shall use an electronic surveillance system for the protection of property at its headquarters, certain premises and premises open to the reception of customers, which enables the recording of data, on the basis of which the data of the data subject shall also be considered personal data.

(2) The legal basis for this processing is the consent of the data subject.

(3) A warning sign and information on the fact of the application of the electronic monitoring system in a given area shall be placed in a clearly visible place in a clearly legible manner in a manner that facilitates the information of third parties wishing to appear in the area. The information must be provided for each camera. This information shall include the fact of the monitoring carried out by the electronic security system and the purpose of making and storing the image and sound recording containing personal data recorded by the system, the legal basis of the data processing, the storage location of the recording, the duration of storage, the system operator (operator) information on the identity of the data subject and the provisions concerning the rights of data subjects and the procedure for enforcing them. A model for the information is given in the Annex to these Regulations.

(4) Images and sound recordings of third parties (customers, visitors, guests) entering the monitored area may be taken and managed with their consent. Consent may also be given by implied conduct. Indicative behavior, in particular, if the natural person enters the monitored area despite an indication or description of the use of the electronic monitoring system located there.

(5) The recorded recordings may be stored for a maximum of 3 (three) working days if they are not used. Use is considered to be the use of the recorded image and other personal data as evidence in court or other official proceedings.

(6) A person whose right or legitimate interest is affected by the recording of the data of the image recording may, within three working days from the recording of the image, request that the data controller not destroy or delete the data.

(7) An electronic surveillance system shall not be used in a room where surveillance may violate human dignity.

(8) In addition to those authorized by law, the operating staff, the head and deputy head of the employer, as well as the workplace manager of the monitored area are entitled to view the data recorded by the electronic monitoring system in order to detect violations and check the operation of the system.

V. CHAPTER

OTHER PROVISIONS RELATING TO DATA PROCESSING

V.1. Data security measures

1) The Data Controller is obliged to take the technical and organizational measures and to establish the procedural rules necessary for the enforcement of the Decree and the Information Act in order to ensure the security of personal data in relation to all its purposes and legal basis.

2) The Data Controller shall take appropriate measures to protect the data against accidental or unlawful destruction, loss, alteration, damage, unauthorized disclosure or unauthorized access.

3) The Data Controller classifies and treats personal data as confidential data. It imposes an obligation of confidentiality on the processing of personal data with employees, to which an employee statement in accordance with the annex to these regulations shall apply. The Data Controller restricts access to personal data by specifying authorization levels.

4) The Data Controller protects the IT systems with a firewall and provides virus protection.

5) The Data Controller shall perform the electronic data processing and registration by means of a computer program which complies with the requirements of data security. The program ensures that only those who need it in order to perform their duties have access to the data only in a controlled and targeted manner.

6) During the automated processing of personal data, the Data Controller and the data processors shall ensure by additional measures:
   a. prevention of unauthorized data entry;

b. prevent the use of automatic data - processing systems by unauthorized persons using data communication equipment;

c. the verifiability and traceability of the personal data to which personal data have been or may be transmitted using data communication equipment;

d. the verifiability and traceability of which personal data have been input into automated data-processing systems, when and by whom;

e. the resilience of installed systems in the event of failure;

f. that errors in automated processing be reported.

7) The Data Controller shall ensure the control of incoming and outgoing electronic communications in order to protect personal data.

8) Only the competent clerks shall have access to the documents in progress, which are being processed, and the documents containing personnel, wage and labor and other personal data shall be kept securely locked.

9) Adequate physical protection of data and the devices and documents carrying them shall be ensured.

V.2. Dealing with privacy incidents

V.2.1.1 The concept of a data protection incident

(1) Data protection incident: a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled;

V.1.2. Management and remediation of data protection incidents

(1) The Head of the Data Controller is responsible for the prevention and management of data protection incidents and the observance of the relevant legal regulations.

(2) Accesses and access attempts on IT systems shall be logged and continuously analyzed.

(3) This Regulation provides that an incident which is likely to jeopardize the rights and freedoms of data subjects is to be reported to the supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of it. If the 72-hour time limit cannot be met, the reason for the delay shall be stated.

(4) If the incident concerns personal data, a decision shall be taken on the extent, timing and content of the contact with the data subjects. The Regulation stipulates that contact must take place "without undue delay" if the incident "poses a high risk to the rights and freedoms of natural persons".

(5) The data controller may deviate from the provisions of these regulations, taking into account the specific circumstances of the incident, in order to remedy it as effectively as possible.

V.2.1.3. Privacy Incident Handling Procedure

V.2.1.3.1. Internal report of a privacy incident

(1) In practice, several types of data protection incidents can occur, in particular:

(a) confidentiality incident: this includes cases of unauthorized access to and disclosure of personal data;

(b) data modification incident: this includes cases where personal data is modified unauthorized or accidentally.

(2) If any employee of the Data Controller or any other person accessing the personal data of the Company experiences any data protection incident or real threat thereof, he / she must report it to the Head of the Data Controller in detail and provide all assistance in a timely manner to fully detect and deal with the data protection incident.

(3) Reported incidents need to be evaluated and documented.

(a) the date and place of the incident,

(b) a description of the incident, its circumstances, its effects,

(c) the scope and number of data compromised during the incident,

(d) the persons affected by the compromised data,

(e) a description of the measures taken to deal with the incident,

(f) a description of the measures taken to prevent, remedy and reduce the damage.

(4) A record of data protection incidents shall be kept, including:

a) the scope of the personal data concerned,

b) the number and number of persons involved in the data protection incident,

c) the date of the data protection incident,

d) the circumstances and effects of the data protection incident,

e) the measures taken to remedy the data protection incident,

f) other data specified in the legislation requiring data processing.

(5) Data on registered data protection incidents shall be kept for 5 years.

(6) The incident log for the registration of data protection incidents is attached to this policy.

V.2.1.3.2. External information obligations

Following a finding of a data protection incident, the Regulation requires two parties to be informed. These are the following:

1. Supervisory authority
2. Affected

The incident should be reported subject to an assessment of the risk to the "rights and freedoms of natural persons" and should therefore be subject to such a risk assessment.

V.2.1.3.3. Supervisory authority

With regard to the Data Controller pursuant to the Regulation, the supervisory authority is as follows:

Name:	Nemzeti Adatvédelmi és Információszabadság Hatóság
Adress:	1125 Budapest, Szilágyi Erzsébet fasor 22/C
Phone:	+36 1 391 1400
Fax:	+36 1 391 1410
Email:	ugyfelszolgalat@naih.hu

V.2.1.3.4. Deciding whether to notify the supervisory authority

The Regulation states that a data processing incident must be reported to the supervisory authority "unless the data protection incident is not likely to endanger the rights and freedoms of natural persons".

Based on this, the Data Controller is obliged to assess the level and extent of the risk posed by the data protection incident before deciding whether to make a report.

- The following aspects, among others, should be considered in the risk assessment:
- the nature of the incident (see eg above categories);
- the nature, sensitivity and amount of personal data involved in the incident;
- other factors considered relevant (including, but not limited to, assessment of the impact of the incident).

The Head of the Data Controller shall be responsible for carrying out the above risk assessment, implementing the decision on the notification, preparing the appropriate documentation, and contacting and answering any further questions or concerns from data subjects.

The method, rationale and conclusions of the risk assessment shall be documented and signed by senior management. The outcome of the risk assessment shall be one of the following:

1. A privacy incident does not require reporting
2. The data protection incident shall only be reported to the supervisory authority
3. The data protection incident shall be reported to both the supervisory authority and the data subject

V.2.1.3.5. Method of notification to the supervisory authority

Where the decision requires notification to the supervisory authority, the Regulation requires that this be done "without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident". If, for legal reasons, the notification is not made within the prescribed time limit, the reasons shall be stated in the notification.

The notification shall be made to the competent data protection authority in an appropriate and secure manner.

V.2.1.3.6. Stakeholders

(i) Deciding whether to inform stakeholders

The Regulation states that the data subject must be informed of the data processing incident,

"Where the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons".

The Regulation does not require those concerned to be informed if this would "require a disproportionate effort". In such cases, however, those concerned shall be informed by means of publicly available information.

(ii) How to inform stakeholders

Once a decision has been made that the incident justifies informing the persons concerned, the information must be provided without undue delay under the Regulation.

The information provided to data subjects shall "clearly and intelligibly describe the nature of the data protection incident" and the following:

a. the name and contact details of the Data Protection Officer or other contact person for further information;
b. description of the likely consequences of the data protection incident; and
c. the measures taken or planned to be taken to remedy the data protection incident, including, where appropriate, measures to mitigate any adverse consequences.

V.3. Rights of the person concerned

V.3.1.1. Right to prior information

The data subject shall have the right to be informed of the facts and information relating to the processing prior to the commencement of the processing.

The information shall include in particular:

If personal data concerning the data subject are collected from the data subject, the Data Controller shall provide the data subject with all of the following information at the time of obtaining the personal data:

a) the identity and contact details of the Data Controller and, if any, of the Data Controller's representative;
b) the contact details of the Data Protection Officer, if any;
c) the purpose of the intended processing of the personal data and the legal basis for the processing;
d) in the case of data processing based on the enforcement of a legitimate interest, the legitimate interests of the Data Controller or a third party;
e) the recipients or categories of recipients of the personal data;
f) where applicable, the fact that the controller intends to transfer the personal data to a third country or to an international organization;
g) the period for which the personal data will be stored or, if that is not possible,

the criteria for determining that period;

h) the right of the data subject to request the controller to access, rectify, delete or restrict the processing of personal data concerning him or her and to object to the processing of such personal data and the right of the data subject to data portability;
i) in the case of data processing based on the consent of the data subject, the right to withdraw the consent at any time, without prejudice to the lawfulness of the data processing carried out prior to the withdrawal;
j) the right to lodge a complaint with the supervisory authority;
k) whether the provision of personal data is based on a law or a contractual obligation or a precondition for the conclusion of a contract, whether the data subject is required to provide personal data and the possible consequences of not providing such data;
l) the fact of automated decision-making, including profiling, and at least in such cases, comprehensible information on the logic used and the significance of such data processing for the data subject.

V.3.2. The data subject 's right of access

The data subject has the right to receive feedback from the Data Controller as to whether the processing of his / her personal data is in progress and, if such data processing is in progress, he / she has the right to access the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been or will be communicated, including in particular third country recipients or international organizations;

(d) where applicable, the intended period for which the personal data will be stored or, if that is not possible, the criteria for determining that period;

(e) the right of the data subject to request the controller to rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data;

(f) the right to lodge a complaint with a supervisory authority;

(g) if the data were not collected from the data subject, all available information on their source;

(h) the fact of the automated decision-making referred to in Article 22 (1) and (4) of the Regulation, including profiling, and, at least in those cases, comprehensible information on the logic used and the significance of such processing and on the data subject the expected consequences.

Where personal data are transferred to a third country or to an international organization, the data subject shall be entitled to be informed of the appropriate guarantees regarding the transfer in accordance with Article 46 of the Regulation.

The Data Controller shall make a copy of the personal data subject to data processing available to the data subject. The Data Controller may charge a reasonable fee based on administrative costs for additional copies requested by the data subject.

Where the data subject has submitted the request by electronic means, the information shall be provided in a widely used electronic format, unless the data subject requests otherwise. The right to request a copy shall not adversely affect the rights and freedoms of others.

V.3.3. Right of cancellation ("right to be forgotten")

The data subject shall have the right to delete personal data concerning him or her without undue delay upon request, and the data controller shall be obliged to delete personal data concerning him or her without undue delay if any of the following reasons exist:

(a) personal data are no longer required for the purpose for which they were collected or otherwise processed;

(b) the data subject withdraws his or her consent under Article 6 (1) (a) or Article 9 (2) (a) of the Regulation and there is no other legal basis for the processing;

(c) the data subject objects to the processing pursuant to Article 21 (1) of the Regulation and there is no overriding legitimate reason for the processing, or the data subject Object to the processing pursuant to Article 21 (2);

(d) personal data have been processed unlawfully;

(e) personal data must be deleted in order to fulfill a legal obligation to which the controller is subject under applicable Union or Member State law;

(f) personal data have been collected in connection with the provision of information society services referred to in Article 8 (1) of the Regulation.

If the Data Controller has disclosed personal data and is required to delete it pursuant to paragraph 1 above, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the Data Controllers that the data the data subject has requested them to delete the links to the personal data in question or a copy or duplicate of such personal data.

V.3.4. Right to restrict data processing

The data subject has the right, at the request of the Data Controller, to restrict the data processing if one of the following is met:

(a) the data subject disputes the accuracy of the personal data, in which case the restriction shall apply for a period which allows the Data Controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the data and instead requests that their use be restricted;

c) the Data Controller no longer needs the personal data for the purpose of data processing, but the data subject requests them in order to submit, enforce or protect legal claims; obsession

(d) the data subject has objected to the processing in accordance with Article 21 (1) of the Regulation; in this case, the restriction shall apply for the period until it is determined whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the data subject.

Where processing is restricted, such personal data may be processed, with the exception of storage, only with the consent of the data subject or for the purpose of bringing, enforcing or protecting legal claims or protecting the rights of another natural or legal person or in the important public interest of the Union or a Member State.

The Data Controller shall inform the data subject at whose request the data processing has been restricted in advance of the lifting of the data processing restriction.

V.3.5. The right to data portability

The data subject shall have the right to receive personal data concerning him or her made available to a Data Controller in a structured, widely used machine-readable format and to transfer such data to another Data Controller without being hindered by the Data Controller whose provided personal data if:

(a) the processing is based on consent or contract; and

(b) the processing is carried out in an automated manner.

When exercising the right to data portability, the data subject shall have the right, if technically feasible, to request the direct transfer of personal data between Data Controllers.

V.3.6. Right to protest

The data subject shall have the right at any time to object to the processing of his or her personal data on grounds of legitimate interests, including profiling based on those provisions.

In this case, the Data Controller may not further process the personal data, unless it proves that the processing is justified by compelling legitimate reasons which take precedence over the interests, rights and freedoms of the data subject or which relate to the submission, enforcement or protection of legal claims.

Where personal data are processed for the direct purpose of obtaining a business, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for that purpose.

If the data subject objects to the processing of personal data for the purpose of direct business acquisition, the personal data may no longer be processed for that purpose.

V.3.7. Automated decision making in individual cases, including profiling

The data subject shall have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have a legal effect on him or her or a significant effect on him or her.

The above right may not be exercised if the decision:

a) necessary for the conclusion or performance of a contract between the data

subject and the Data Controller;

b) is governed by Union or Member State law applicable to the controller, which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; obsession

c) is based on the express consent of the data subject.

V.3.8. Deadline for the administration of the customer's application as a data subject

(1) The controller shall, without undue delay and in any event within one month of receipt of the request, inform the data subject of the action taken on his or her request to exercise his or her rights.

(2) If necessary, taking into account the complexity of the application and the number of applications, this time limit may be extended by a further two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month from the receipt of the request.

(3) Where the application has been submitted by electronic means, the information shall, as far as possible, be provided by electronic means, unless the person concerned requests otherwise.

(4) If the Data Controller fails to take action on the data subject's request, it shall inform the data subject without delay, but no later than one month after receipt of the request, of the reasons for the non-action and of the data subject's right to appeal to a supervisory authority. right of appeal.

(5) If the data subject's request is manifestly unfounded or, in particular due to its repetitive nature, excessive, the Data Controller shall, taking into account the administrative costs of providing the requested information or information or taking the requested action:

(a) charge a fee, or
(b) refuse to act on the application.

The burden of proving that the request is manifestly unfounded or excessive is on the Data Controller.

(6) If the Data Controller has reasonable doubts about the identity of the natural person submitting the request, he / she may request the provision of additional information necessary to confirm the identity of the data subject.

V.4. Complaint to the supervisory authority

Without prejudice to other administrative or judicial remedies, any person concerned shall have the right to lodge a complaint with a supervisory authority.

Supervisor of the data controller:

Name:	Nemzeti Adatvédelmi és Információszabadság Hatóság
Adress:	1125 Budapest, Szilágyi Erzsébet fasor 22/C
Phone:	+36 1 391 1400
Fax:	+36 1 391 1410
Email:	ugyfelszolgalat@naih.hu

The provisions of the Decree and the Info Act, as well as those described on the NAIH website, shall govern the submission of complaints and the procedure for their adjudication.

FINAL PROVISIONS

VI.7. Establishment and amendment of regulations

The head of the Data Controller is entitled to establish and amend the regulations.

VI.8. Measures to make the rules known

The provisions of these regulations must be communicated to all employees (employees) of the Data Controller, and employment contracts must stipulate that compliance with and enforcement of them is an essential job obligation for all employees (employees).