Internal guidelines on the processing of personal data under the GDPR

Version of the Internal Directive: **v.1 from 11.8.2023**
Controller: MSM Global s r.o. ID: 19345674 With registered office at U Sluncové 666/12a, 186 00 Prague 8
Internal guidelines: this Internal Directive in the form of a regulation governs the protection and processing of personal 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the "Regulation") and other regulations, effective as of 25 May 2018
Approved: Jevgenij Kolesnik, Managing Director of the company Date: 11.8.2023
Validity and effectiveness: from 11.8.2023 for an indefinite period
Annex: written record of instruction and familiarisation with the content of this Internal Regulation

Article 1 General provisions

1.1 Subject matter and objectives of the Internal Rules

This internal regulation regulates the rules and procedure of the administrator in the protection and processing of personal data of natural persons processed by the administrator in the performance of its work activities.

1.2 Scope of the internal regulation

This internal regulation is binding on the controller as an employer, all its employees and persons who process personal data for the controller on the basis of a contract.

1.3 Update of the Internal Rules

The content of the internal regulations is reviewed, evaluated and updated periodically, annually, otherwise at any time as required, by an authorised employee of the administrator, who is the head of the company.

1.4 Access to the Internal Rules

The Internal Regulation is publicly accessible to all employees of the controller,

as well as to natural persons whose data the controller processes.

Article 2 Basic concepts

In accordance with this Internal Regulation and the legal provisions:

2.1 "**Personal data**" means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, a network identifier or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2 "**Data subject**" means natural persons - employees of the controller or other natural persons ("clients of the controller") whose personal data is processed by the controller in the course of its business activities;

2.3 '**Processing**' means any operation or set of operations which is performed upon personal data or upon sets of personal data, whether or not automated processes, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction;

2.4 "**Restriction of processing**" means the marking of stored personal data in order restrict its processing in the future;

2.5 "A '**record**' is any structured set of personal data accessible according to specific criteria;

2.6 '**Controller**' means the natural or legal person, authority, agency or 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 such processing are determined by European Union or Member State law, that law may determine the controller concerned or the specific criteria for its determination;

The administrator according to this internal regulation is MSM Global s r.o., company ID No.: 19345674, with registered office at U Sluncové 666/12a, 186 00 Prague 8

2.7 "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data for the controller;

2.8 "**Consent**" of the data subject is any free, specific, informed and unambiguous expression of will by which the data subject gives his or her consent to the processing of his or her personal data by declaration or other manifest acknowledgement;

2.9 "**Supervisory authority**" means an independent public authority established by a Member State pursuant to Article 51 of the Regulation;

the supervisory authority of the controller is the Office for Personal Data

Protection, located at Pplk. Sochor 727, 170 00 Prague 7. The same authority is the supervisory authority in the case of cross-border processing of personal data;

the managing director of MSM Global s.r.o. is appointed to act legally and represent the administrator in negotiations with supervisory authorities;

2.10 **An "authorised person"** is any employee of the controller (or a person who processes personal data for the controller under contract) who, by reason of his or her employment with the controller, comes into contact with or processes personal data. Authorised persons must be instructed, familiarised with the contents of this Internal Regulation; a written record of the instruction and familiarisation shall be made. Authorised persons must be re-educated if there is a change in their job description or any other change resulting a change in the scope or extent of the authorised person's work in relation to the processing of personal data. Access to the personal data of data subjects is strictly limited to the instructed authorised persons only;

2.11 "**Responsible person**" means an authorised employee of the controller (or an authorised person under a contractual relationship) who is authorised by the controller to fulfil the controller's rights and obligations under this Internal Regulation towards data subjects and to be the controller's point of contact with data subjects.

The responsible person is not appointed to act legally and represent the administrator with supervisory authorities.

Article 3 Principles of personal data processing

The processing of personal data by the controller under this Internal Regulation is subject to the following principles in accordance with the law:

3.1. Personal data must be:

a. processed fairly and in a lawful and transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
b. collected for specific, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes;
c. proportionate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimisation');
d. accurate and, where necessary, up-to-date; all reasonable measures shall be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. stored in a form which permits identification of data subjects for no than is necessary for the purposes for which they are processed ("storage limitation");
f. processed in a manner that ensures appropriate security of personal data, including protection by appropriate technical or organisational measures

against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality").

3.2 The Administrator shall be responsible for compliance with paragraph 1 and shall be able to demonstrate such compliance.

Article 4 Purposes and lawfulness of processing and categories of personal data

4.1 Purposes of processing

The purposes of the processing for which the personal data are intended are the performance of the contract with clients ("data subjects") of the controller, in particular the creation of a client database, contacting clients regarding the agreed services; and the performance of legal obligations.

4.2 Legal basis for processing

The legal basis for the processing of the personal data of the data subject is that the processing is necessary for compliance with the legal obligations imposed on the controller by applicable law pursuant to Article 6(1)(a), (b), (c) and (e) of the Regulation.

4.3 Identification of personal data

a. client agenda;
b. employees and associates;
c. operation of the company administrator, taxes, accounting;
d. sales and marketing, online communication;
e. the others.

4.4 Categories of personal data

a. client agenda - name, surname, date of birth, nationality phone, email, photo, address;
b. employees and associates - name, surname, date of birth, address, telephone, email, account number;
c. company operations, taxes, accounting - name, surname, date of birth, address, phone, email, account number;
d. sales and marketing, online communication - name, surname, email;
e. other - name, surname, phone, email.

Article 5 Sources of personal data

The controller obtains personal data from the following data subjects:

a. clients of the administrator;
b. employees and associates;

c. third parties (suppliers, etc.).

Article 6 Transfer and disclosure of personal data of the data subject to a third party

6.1 The controller may only transfer or disclose the personal data of the data subject to a third party in accordance with the instructions under this Internal Regulation. In case of doubts or questions in the transfer or disclosure, the correct procedure should be asked in advance to the person in charge and await his decision.

6.2 The controller makes personal data available to the following recipients:

a. financial institutions;
b. State i. authorities within the framework of the fulfilment of legal obligations set out in the relevant legislation;
c. third parties (insurance companies, suppliers, etc.);

6.3 The controller is entitled to transfer or disclose the personal data of the data subject to a third party in the context of compliance with the purpose of processing in order to comply with the legal obligations of the controller, subject to the instructions of the person responsible.

6.4 If personal data of the data subject are to be transferred or disclosed to a third party for a purpose other than that for which they were collected, they may only be transferred or disclosed with the prior written consent of the responsible person.

Article 7 Retention period of personal data of the data subject

7.1 In accordance with the principle of storage limitation pursuant to Article 5(1)(e) of the Regulation, personal data of the data subject may only be retained for as long as necessary for the purpose of processing. After that period, personal data may be retained solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to Article 89(2) of the Regulation, provided that the appropriate technical and organisational measures required by the Regulation are implemented in order to safeguard the rights and freedoms of the data subject. When used for these purposes, the right to protection against unlawful interference with the private and personal life of the data subject shall be respected, the principle of data minimisation shall be observed and personal data shall be anonymised as soon as possible.

7.2 Specific retention periods for personal data:

Origin of personal data	Required/maximum storage time
From the contract	10 years from the end of the business

	relationship
From marketing activities	3 years after the acquisition of the personal data

If not determined by the Administrator, then law.

Article 8 Security of personal data

8.1 Processing security
The controller shall implement personal data security and processing security in with the instructions under this Internal Regulation and in accordance with the instructions of the person in charge. In case of doubts or questions about the security of personal data and the security of processing, it is necessary to ask the responsible person in advance for the correct procedure and await his decision.

8.2 Taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, as well as the differently likely and differently serious risks to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk concerned, including, where applicable:

a. encryption of files containing personal data;
b. the introduction of technical and organisational measures to ensure the security of processing;
c. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
d. the ability to restore the availability of and access to personal data in a timely manner in the event of physical or technical incidents.

8.3 In assessing the appropriate level of security, account shall be taken in particular of the risks posed by the processing, in particular accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed.

Article 9 Method of processing personal data

9.1 The processing of personal data is carried out by the controller. The processing is carried out at the controller's registered office by individual authorised employees of the controller. The processing is carried out by means of computer technology and also manually for personal data in paper form, in compliance with the security principles for the management and processing of personal data.

9.2 To this end, the controller has adopted the following technical and organisational measures to ensure the protection of personal data, in particular measures to exclude the possibility of unauthorised or accidental access to, alteration, destruction or loss of personal data, as well as other misuse of personal data:

a. electronic storage of personal data:
for the storage and transmission of personal data, the company uses internal

registers developed on the basis of xls tables. Access to personal data files is secured by a password. Personal data is only handled by a responsible person on a dedicated computer with an antivirus program. Access to the computer is password protected.

b. documentary storage of personal data:
in locked cupboards, keys stored in a locked box

Article 10 Information and rights of data subjects

10.1 In accordance with Article 12 of the Regulation, the controller shall inform the data subject of the right of access to personal data and to the following information upon request:

a. the purpose of processing;
b. the category of personal data concerned;
c. the recipients or categories of recipients to whom the personal data are disclosed;
d. the planned period for which the personal data will be stored;
e. all available information about the source of the personal data.

10.2 Any data subject who becomes aware of, or believes that the controller is carrying out, processing of his or her personal data which is contrary to the protection of his or her private and personal life or contrary to law shall be entitled to:

a. ask the administrator for an explanation;
b. require the controller to remedy the situation, in particular to block, supplement, correct or delete the personal data, or the data subject is entitled to contact the supervisory authority, i.e. the Office for Personal Data Protection;
c. if the data subject's request under (b) is justified, the controller shall immediately rectify the defective condition;
d. if the controller does not remedy the defective situation pursuant to point c), the data subject has the right to apply to the supervisory authority, i.e. the Office for Personal Data Protection.

Annex

to the internal directive on the processing of personal data according to GDPR v.1 from 11.8.2023

List of authorised persons instructed and familiarised with the contents of this internal regulation:

Responsible person	Date	Signature
1. Yevgeny Kolesnik	11.9.2023	

Authorised person	Date	Signature
1. Alyona Tsurkan Knysh	11.9.2023	
2. Ulloa Wood Tamara Ailin	11.9.2023	

Internal guidelines for dealing with personal data breaches

Version of the Internal Directive: **v.1 from 11.8.2023**
Controller: MSM Global s r.o. ID: 19345674 With registered office at U Sluncové 666/12a, 186 00 Prague 8
Internal guidelines: This Internal Directive in the form of a regulation regulates the main obligations of the data controller in the event of a personal data breach as defined in Article 4(12) GDPR Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the "Regulation").
Approved: Jevgenij Kolesnik, Managing Director of the company Date: 11.8.2023
Validity and effectiveness: from 11.8.2023 for an indefinite period
Attachments: Annex 1 Diagram showing the requirements for reporting security breaches Annex 2 Examples of security breaches and procedures Annex 3 Sample Documentation of records of all reported security breaches A written record of instruction and familiarisation with the contents of this internal directive

Article 1 Introductory Provisions

1.1 This Internal Directive in the form of a regulation (hereinafter also referred to as the "Regulation") regulates certain rights and obligations of the authorized person of MSM Global s.r.o. (hereinafter referred to as the "Administrator") arising from or related to the employment relationship with the Administrator or a contractual relationship. This Code also governs the rights and obligations of the person who has operational responsibility for dealing with breaches (the "Responsible Person").

1.2 For the purposes of these Regulations, an authorised person means employees working for the Controller under an employment relationship, or other persons performing activities for the Controller under other legal titles, in particular under a work performance agreement or a work activity agreement or under a contractual relationship.

1.3 The regulation is binding on the authorised persons and each authorised person is obliged to comply with it.

Article 2 Definition of terms

2.1 For the purposes of this Regulation, personal data shall mean any information about an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, a network identifier or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2 For the purposes this Regulation, a personal data breach (also referred to as a "Security Breach") means a breach of security that results in the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

2.3 A security breach is a security incident that results in the Controller being unable to ensure compliance with the Personal Data Processing Policy. These are cases of:

a) breach of confidentiality - a breach of security of personal data in the event of unauthorised or accidental disclosure or access to personal data.
b) availability breach - a breach of security of personal data in the event of accidental or unauthorised loss of access to or destruction of personal data. An availability breach is always an incident in which personal data is permanently lost or destroyed, by accidental intentional deletion, encryption of data, loss of decryption , etc.
c) integrity breach - a breach of security of personal data in the event of unauthorised or accidental alteration of personal data.

2.4 Security breaches can be detected in particular:

a) directly by the Responsible Person
b) on the basis of a notification by an authorised person
c) following notifications from data subjects
d) on the basis of notifications from other third parties
e) on the basis of other information (including information published in the media).

Article 3 Obligations of the Authorised Person

3.1 This Regulation defines the obligations of the authorised person in the event of a personal data breach, in accordance with the requirements imposed on the Controller by Regulation (EU) No 2016/679 (GDPR).

3.2 Any authorised person who causes or becomes aware of a security breach or has reason to believe that a security breach has occurred or is imminent is obliged to report it to the responsible person. In reporting a breach of security, authorised persons shall comply with Article 5.

contact the responsible, he/she is obliged to report the above to his/her supervisor.

3.3 Each Authorized Person shall be obligated to cooperate with the Responsible Person in the investigation of the Security Breach and in the remediation of the Security Breach.

Article 4 Responsibilities of the Responsible Person in the event of a Security Breach

4.1 The responsible person has the following duties:

a) the obligation to receive notices from employees and others about Security Breaches,

b) obligation to act on the first notice and investigate the Security Breach,

c) if the conditions under Article VII are met, report the Security Breach to the supervisory authority - the Office for Personal Data Protection (hereinafter also referred to as the "OSC") and cooperate with the OSC's office in the investigation of the Security Breach,

d) if the conditions of Article VIII are met, notify the Data Subject of the Security Breach,

e) the obligation to keep records and document all Security Breaches, stating the facts relating to the breach, its effects and the corrective action taken.

4.2 In carrying out the duties referred to in paragraph 1 of this Article, the Responsible Person shall be guided by the following provisions of the Regulations as well as the procedures set out in Annex 1 and Annex 2.

Article 5 Duty of the Responsible Person to Receive Notifications of Security Breaches

5.1 The responsible person has set up an e-mail address msmpraha@seznam.cz to receive notifications. The Responsible Person also receives notifications of Security Breaches at +420 724 923 495.

5.2 All Authorized Persons may report a Security Breach to the email listed in paragraph 1, tel. Responsible Persons and may also contact the Responsible Person directly orally or by written submission. Authorised Persons are obliged to choose a method of notifying the Responsible Person such that the Responsible Person becomes aware of the Security Breach without delay.

Article 6 Responsibilities of the Responsible Person in a Security Breach Investigation

6.1 The Responsible Person shall be required to investigate any notice received pursuant to Article V or other notice of a Security Breach received.

6.2 The Responsible Person shall periodically check for reports of Security Breaches in any of the ways specified in Article 5.

6.3 The Responsible Person may request the relevant department of the Administrator to assist the Responsible Person in the investigation of a Security Breach.

6.4 The Responsible Person shall proceed as follows when investigating a Security Breach:

a) Based on the information received, the Responsible Person will assess whether a Security Breach has actually occurred;
b) The Responsible Person shall assess which type of Security Breach is involved (see Article 2.3);
c) The Responsible Person shall assess the potential consequences and risks of the Breach to the Data Subjects (e.g. material or immaterial damage, identity theft, fraud, etc.), together with the amount of data affected by the Breach;
d) The Responsible Person shall evaluate whether it is necessary to report the Security Breach to the OCCP pursuant to Article VII and to notify the Data Subjects pursuant to Article VIII;
e) The Responsible Person shall propose measures to address the Security Breach, including appropriate measures to mitigate potential adverse impacts (e.g., making a backup copy operational in the event of a data breach).

Article 7 Obligation to Report Security Breaches to and Cooperate with the OSSA

7.1 Based on the investigation conducted pursuant to Article VI, the Responsible Person shall evaluate whether the Security Violation should be reported to the OSSA.

7.2 The Responsible Person shall report a Security Breach to the OSSA in any where a Security Breach has actually occurred, except where:

a) a Security Breach has occurred that does not and cannot have any effect on Data Subjects,
b) the device has been lost, but it is securely encrypted and there is no possibility that it could be misused by a third party,
c) A security breach has occurred, but the person who received the personal data is trustworthy, has sent the data back or has securely destroyed it.

In assessing the need to report a Security Breach to the OSSA, the Responsible Person shall be guided by the examples set out in Annex 2 as appropriate.

7.3 The Responsible Person is obligated to report a Security Breach to the OSSA without undue delay after it is confirmed that a Security Breach has occurred and it has been determined that the Security Breach requires reporting to the OSSA. The Responsible Person shall report the Security Violation to the OSSA no later than 72 hours after discovery.

7.4 In the event that the Responsible Person fails to report a Security Breach within the time limit, the OCCP shall be notified without delay and, in addition to the information set forth in the following paragraph, the Responsible Person shall include in the report the reasons for the delay in reporting and shall supplement such reasons with documentation demonstrating the reasons for the delay.

7.5 When reporting a Security Breach to the Office of the Security Officer, the Responsible Person shall state:

a) a description of the nature of the Security Breach in question, including, where possible, the categories and approximate number of data subjects affected and the

categories and approximate number of personal data records affected;

b) your name and contact details;

c) a description of the likely consequences of a Security Breach;

d) a description of the measures that the Administrator has taken or proposed to address the Security Breach, including any measures to mitigate potential adverse effects.

7.6 If the Responsible Person cannot provide all of the information referred to in paragraph V of this Article at the same time, it shall provide it to the OMA without further undue delay.

Article 8 Obligation to Notify Data Subjects of a Security Breach

8.1 If a particular Security Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Responsible Person shall notify the Data Subject of the Security Breach without undue delay.

8.2 In the notification to the data subject referred to in paragraph 1 of this Article, the Responsible Person shall use clear and plain language, describe the nature of the Security Breach and include, at a minimum, the information and measures referred to in Article VII(5)(b), (c) and (d) and, where possible, the steps that data subjects can take to protect themselves.

8.3 The notification to the data subject referred to in paragraph 1 shall not be required where any of the following conditions are met:

a) the controller has put in place appropriate technical and organisational safeguards and these safeguards have been applied to the Personal Data affected by the Breach. This includes, in particular, measures that render the data incomprehensible to anyone not authorised to have access to it (e.g. encryption);

b) the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 of this Article is no longer likely to occur;

c) notification would require disproportionate effort, in which case the Responsible Person shall ensure that data subjects are informed in an equally effective manner by means of a public notice or similar measure.

Article 9 Obligation to keep records and document security breaches

9.1 The Responsible Person shall document all Security Breaches that have been reported.

9.2 The responsible person shall keep the documentation in such a form that it shows at least:

a) description Security breach (description of what),

b) the date on which the Security Breach was discovered,

c) source of discovery breach,

d) the Personal Data affected by the Security Breach,

e) Identified causes Security breach,

f) Consequences of a Security Breach,

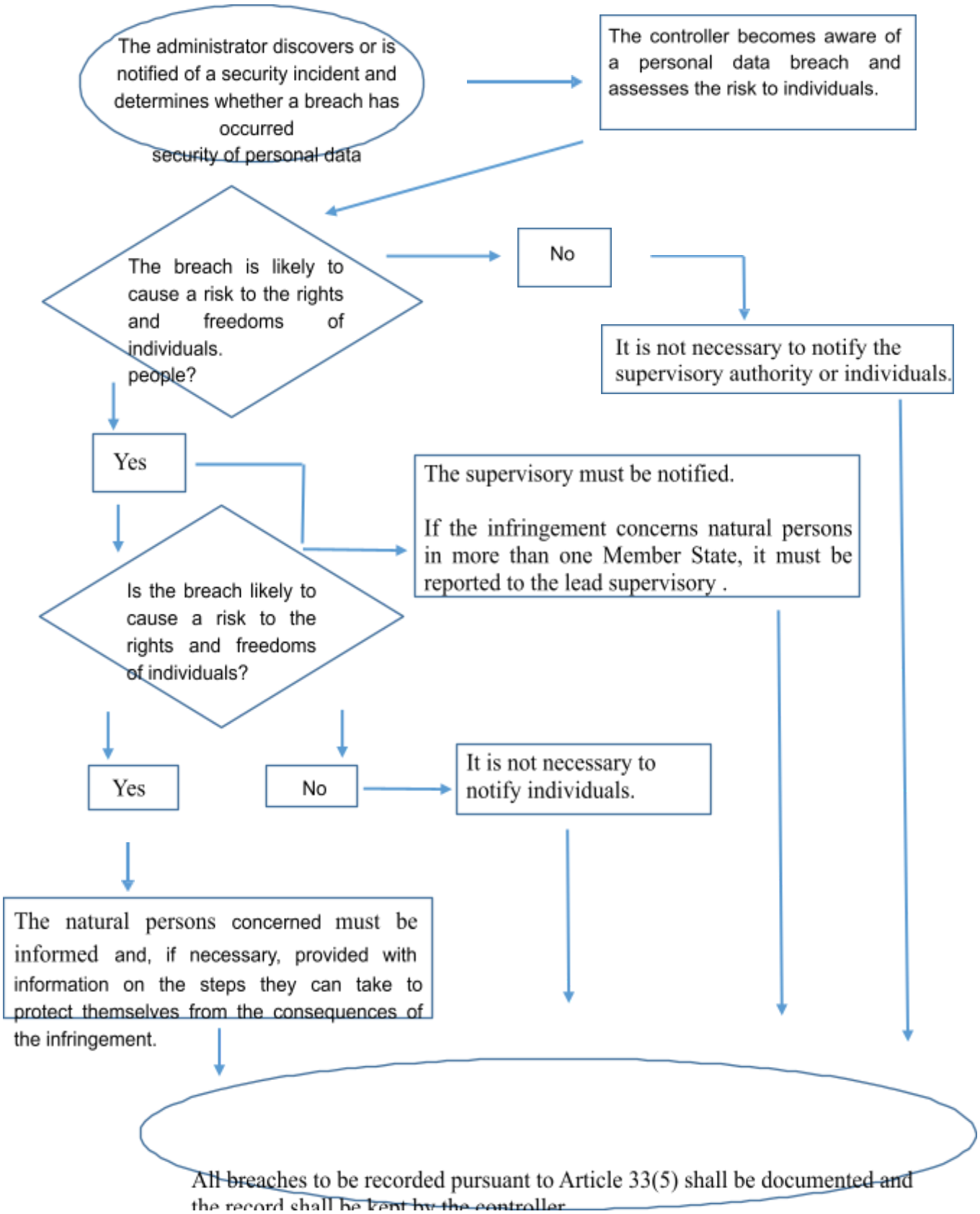
g) corrective actions taken by the Administrator,

h) if the Security Breach has been reported to the OCCP or notified to data subjects, information about the report and notification.

9.3 The Responsible Person shall use Annex 3 for record keeping.

Prague, 11 August 2023

Diagram showing the requirements for reporting a security breach



Source: the Guidance on Reporting Personal Data Breaches under Regulation 2016/679 developed by the Article 29 Data Protection Working Party, adopted on 3 October 2017, revised and adopted on 6 February 2018.

Examples of security breaches and procedures

The Responsible Person shall follow the procedures set out in this Annex as appropriate when reporting a Security Breach.

Example	It is necessary to understand	The subject must be notified	Notes and recommendations
i. The administrator has deposited a deposit archive personal data encrypted on a USB storage device. During a break-in, the storage device is stolen.	No.	No	If are the data is encrypted using a state-of-the-art algorithm, there are backups, the security of the unique key and the data can be recovered quickly enough, it may not be a breach. If However, is later breached, it must be to report the incident.
ii. The administrator operates an online service. As a result of a cyber-attack on this service, personal data of individuals will be leaked. The administrator has customers in one Member State.	Yes, notify the supervisory authority, if any Probability consequences for natural persons.	Yes, notify breach to natural persons, depending on the nature of the personal data concerned, and where the gravity of the Probable consequences for individuals high.	
iii. The administrator's call center experiences a brief power outage that lasts several minutes, preventing customers from calling the administrator and accessing their records.	No.	No	It is not a reportable breach, but it is still an incident that must be recorded under Article 33(5). The administrator should keep appropriate records.
iv. The administrator suffers a ransomware attack that results in the encryption of all data. No backups are available	Yes, notify the supervisory authority, if any Probability consequences for individuals, as it is	Yes, notify individuals depending on the nature of the personal data concerned and the possible impact of non-availability	If a backup is available and the data can be restored quickly enough, it is not necessary to incident to be reported to the supervisory authority or

and the data cannot be recovered. The investigation will show that the only function of ransomware was data encryption and that the system no other malware existed.	of loss of accessibility.	data, as well as on other likely consequences.	notify individuals, as there would be no permanent loss of availability or confidentiality. However, if the supervisory authority becomes aware of an incident by other means, it may consider conducting an investigation to assess compliance with the broader security the requirements of Article 32.
v. An individual calls the bank's call centre to report security breach data breach. The individual received someone else's monthly account statement. The controller will conduct a brief investigation (i.e. one that is completed within 24 hours) and determine with a reasonable degree of certainty whether a personal data breach has actually occurred and whether it is a systemic deficiency that may mean that other persons are or may be affected.	Yes.	If there is a high risk and it is clear that others were not affected by the incident, the breach is only reported to the individuals concerned.	If, after further investigation, it is found that more than one individual is affected, this must be reported to the supervisory authority and, in addition, the administrator shall notify the breach to other individuals if they are at high risk.

vi. The administrator operates an online marketplace and has customers in multiple member Member States. Marketplace will suffer cyber attack and the attacker publishes usernames, passwords and purchase history on the internet.	Yes, inform the lead supervisory authority if the incident is involved cross-border processing.	Yes, because the incident could result in a high risk.	The administrator should take appropriate measures, such as forced password resetting of the affected accounts, as well as other steps to mitigate the risk. The controller should also take into account any other notification obligations, e.g. under the NIS Directiveas a digital service provider.

vii. A web hosting company acting as a data processor detects an error in the code that controls user authorization. As a result of this error, any user can access k account details From other user.	As the processor, the web hosting company must notify its affected clients (administrators) without undue delay. Assuming that this web hosting company has made its own investigation, the affected parties should have administrators a reasonable degree of certainty as to whether each of them suffered a security breach, and therefore it would likely be that once they were (processor) notified, they know about the incident in question. The administrator must then notify the supervisory authority.	If individuals are not likely to be at high risk, it is not necessary to notify them of the incident.	The web hosting company (processor) must take account any other notification obligations (e.g. under the NIS Directive) as a digital service provider). If there is no evidence that this vulnerability has been exploited by one of its administrators, this may mean that it is not a reportable breach, but is likely to be an incident to be recorded or a failure to comply with Article 32.
viii. As a result of the cyber-attack, they are not in the hospital for 30 hours available medical records.	Yes, the hospital is required to report the incident because can pose a high risk to health and patient privacy.	Yes, the incident must be reported to the individuals concerned.	

ix. The personal details of a large number of students are inadvertently sent to an incorrect mailing list with over 1000 recipients.	Yes, the incident must be reported to the supervisory authority.	Yes, notify individuals depending on the scope and type of personal data and the severity of the possible consequences.	
x. E-mail message for the purpose of direct marketing is sent to recipients who are all listed in the recipient or recipients box of a copy of the message, so that each recipient can see the email address of the other recipients.	Yes, reporting the incident to the supervisory authority may be mandatory if it involves a large number of individuals, if sensitive data has been disclosed (e.g. a list of the psychotherapist's patients' addresses) or if other factors pose a high (e.g. if the message contains original passwords).	Yes, notify individuals depending on the scope and type of personal data and the severity of the possible consequences.	Notification may not be necessary if no sensitive data is disclosed and if only a small number of email addresses are disclosed.

Annex 3

Sample Documentation of records of all reported security breaches

a) Description Security Breach:

.....

b) Date of Discovery Violation:

.....

c) Source of discovery breach:

.....

d) Identification of Responsible Person.

Has it been determined that a Security Breach actually occurred?

Yes □ No □

e) Personal Data Affected by the Security Breach:

.....

f) Identified causes Security breach:

.....

g) Consequences Security breach:

.....

h) Corrective taken:

.....

i) Notification of Security Breach to the Office of the Security Officer (date and content)

.....

j) Security Breach Notification to Data Subjects (date and content)

.....

Annex

to the Internal Directive on the handling of personal data breaches v.1 from 11.8.2023

List of employees of the Company who have been instructed and familiarized with the contents of this internal directive:

Responsible person	Date	Signature
1. Yevgeny Kolesnik	11.9.2023	
2. Yuliya Hrebenyk	11.9.2023	

Authorised person	Date	Signature
1. Yuliya Hrebenyk	11.9.2023	
2. Alyona Tsurkan Knysh	11.9.2023	
3. Ulloa Wood Tamara Ailin	11.9.2023	

Internal regulations for the processing of personal data in accordance with the GDPR

Version of the Internal Rules: **v.1 as of 11.8.2023**
Personal Data Controller: MSM Global s r. o. ID: 19345674 Legal : U Sluncové 666/12a, 186 00 Prague 8
Internal regulations: This Internal Regulation governs the protection and processing of personal data pursuant to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as "Regulations") and other regulations effective as of May 25, .
Affirmed: Evgeny Kolesnik, Director Date: 11.08.2023
Term and start of validity: from 11.08.2023 for an unlimited period
Annex: briefing and familiarization sheet on the content of these internal rules

Art. 1 General provisions

1.1 Subject matter and objectives of the internal rules

These Internal Regulations (hereinafter referred to as "the Regulations") regulate the rules and procedures for the Controller to protect and process personal data of natural persons which the Controller processes in the course of his/her professional activities.

1.2 Scope of application of the internal rules

These regulations are binding on the controller, all its employees and persons who process personal data for the controller on the basis of the contract.

1.3 Update of internal regulations

The content of the internal rules shall be systematically reviewed, evaluated and updated annually or as required
by an authorised officer of the controller who is the head of the company.

1.4 Access to internal regulations

The internal regulations are publicly available to all employees of the controller as well as to individuals whose data are processed by the controller.

Art. 2 Basic definitions

In accordance with the regulations and in accordance with the law:

2.1 **"Personal data"** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a first name, surname, identification number, data, online identifier or one or more factors specific to that person, whether physical, physiological, genetic, spiritual, economic, cultural or by reference to social factors

2.2 "**Data Subject**" means a natural person - the controller's employees or other natural persons ("the controller's clients") whose personal data is processed by the controller in the course of the controller's professional activities;

2.3 **"Processing"** means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automatic means. Such as collection, recording, organisation, structuring, storage, adaptation or alteration, consultation, use, disclosure (whether by transmission, dissemination or otherwise making available), alignment or combination, restriction, erasure or destruction;

2.4 **"Restriction of processing"** marking of stored personal data in order to restrict its processing in the future;

2.5 **"File"** means any structured set of personal data that is accessible according to certain criteria.

2.6 **"Controller" means** a natural or juridical person, public institution, agency or other entity that, either individually or together with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by legal acts of the European Union or of an EU Member State, the controller or the private criteria for its appointment may be provided for in those legal acts;
The controller in accordance with these regulations is MSM Global s. r. o., IČO: 19345674, jur. address: U Sluncové 666/12a, 186 00 Prague 8

2.7 **"Processor"** means an individual or entity, government body, agency or other authority that processes personal data on behalf of the controller;

2.8 **"Consent"** of the data subject is any free, specific, intelligent and unambiguous indication of the data subject's wishes by which the data subject, by means of a notice or an explicit confirmatory action, consents to the processing of his or her personal data;

2.9 **"Supervisory Institution"** means an independent public institution established by a Member State subject to Article 51;

The supervisory authority of the controller is the Office for the Protection of Personal Data, which is located at Pplk. Sochora 727, 170 00 Prague 7. The same office is the supervisory authority in case of cross-border processing of personal data;

Managing Director of MSM Global s r. o. is the person authorized to represent the interests of the controller in communication with supervisory authorities;

2.10 **"Authorised person"** means any employee of the controller (or person who processes personal data for the controller under a contract) who, in the course of their work for the controller, handles or processes personal . Authorized persons shall be instructed and familiarized with the content of the Regulations; a written record of the instruction and familiarization shall be made. Authorized persons shall be re-instructed if there is a change in the classification of their positions or any other change that results in a change or scope of the authorized person's work in connection with the processing of personal data. Access to the personal data of data subjects is strictly limited and restricted to instructed authorised persons only;

2.11 **"Responsible person"** means an employee of the controller (or the controller's designee) who is authorized to exercise the controller's rights and duties under the regulations with respect to data subjects and to be the controller's point of contact with data subjects.

The Responsible Person is not authorized to conduct legal negotiations or represent the Controller before oversight bodies.

Art. 3 Principles for the processing of personal data

The processing of personal data shall be carried out by the controller within the framework of the regulations in accordance with the following principles and legal rules:

3.1 Personal data:

a. are processed lawfully, fairly, in the form prescribed for the data subject ("lawfulness, specificity and transparency");
b. are collected for specific, explicit and legitimate purposes and are not further processed in a incompatible with those purposes;
c. are adequate, relevant and limited to the necessary for the purposes of the processing ('data minimisation');
d. are accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that inaccurate data is deleted or rectified immediately, taking into account the purposes which it is processed ("accuracy").

e. shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("retention restriction");
f. shall be processed in such a way as to ensure the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality").

3.2 The Controller is responsible for compliance with paragraph 1 and must prove it if necessary.

Art. 4 Purposes, legitimacy of processing and categories of personal data

4.1 Processing objectives

The purposes of the processing for which the personal data is used are the performance of the contract with the controller's customers ("data subjects"), in particular the creation of a customer database for the purpose of contacting customers regarding the agreed services; and the performance of obligations in accordance with applicable law.

4.2 Legal basis for processing

The legal basis for the processing of the personal data of the data subject is the fact that the processing is necessary for the fulfilment of the legal obligations that arise for the controller pursuant to paragraph 6 Article 1 point a), b), c) and e) of the Regulation.

4.3 Classification of personal data

a. customer base;
b. employees and partners;
c. company's current operations, taxation, ;
d. business, marketing, online communication;
e. and so on.

4.4 Categories of personal data

a. client database - name, surname, date of birth, citizenship, telephone, e-mail, photo, address;
b. Employees and partners - name, surname, date of birth, address, telephone, email, account number;
c. current company activities, taxation, accounting - name, surname, date of birth, address, telephone, e-mail, account number;
d. business, marketing, online communication - first name, last name, email address;
e. other - name, surname, phone, email

Art. 5 Sources of personal data

The Controller receives personal data from the following data subjects:

a. controller clients;
b. employees and partners;
c. Third parties (suppliers, .).

Art. 6 Transfer and disclosure of personal data of the data subject to a third party

6.1 The Controller may only transfer or disclose personal data of the data subject to a third party in accordance with the instructions provided for in the regulations. If in doubt or with questions about the transfer or disclosure, the responsible person should be asked in advance about the correct procedure and await his or her decision.

6.2 The Controller provides personal data to the following recipients:
a. financial authorities;
b. State and other authorities in the framework of the implementation of legislative norms;
c. Third parties (insurance companies, suppliers, .);

6.3 The controller shall have the right to transfer or disclose the personal data of the data subject to a third party in the performance of the purposes of the processing in accordance with the controller's legal obligations, following the instructions of the controller.

6.4 If the personal data of the data subject are to be transferred or provided to a third party for purposes other than those for which they were collected, they may only be transferred or provided with the prior written consent of the data controller.

Art. 7 Retention period of personal data

7.1 In accordance with the principle of limitation referred to in Article 5, paragraph 1 (e) of the EU Regulation, the personal data of the data subject may be retained only for the necessary for the purposes of processing. After that period, personal data may be kept solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes as referred to in Article 89 (2), provided that the rights and freedoms of the data subject are safeguarded subject to the implementation of appropriate technical and organisational measures as provided for in the Regulation. When used for these purposes, the right to protection against unauthorized interference with the privacy and personal life of the data subject, the principle of data minimization and the depersonalization of personal data as soon as possible should be respected.

7.2 Specific retention periods for personal data:

Source of personal data	Required/maximum shelf life
Since the conclusion of the contract	10 yearsc since the end of business relationship
From marketing activities	3 years c since received this personal data

If not specified by the controller, then according to current legislation

Art. 8 Protection of personal data

8.1 Security of processing

The Controller shall ensure the security of personal data and the security of processing in accordance with the instructions and in accordance with the regulations. In case of doubts or questions regarding the security of the processing of personal data, it is necessary to inquire about the correct procedure in advance from the person in charge and wait for his decision.

8.2. Taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of natural persons, the controller shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where necessary:

a. encrypt files containing personal data;
b. Implement technical and organizational measures to ensure the safety of processing;
c. ensure the continued confidentiality, integrity, availability and stability of processing;
d. ensure that the availability and access to personal data can be restored in a timely manner in the event of physical or technical incidents.

8.3 In assessing the appropriate level of security, account should be taken in particular of the risks associated with processing, in particular accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed.

Art. 9 Manner of processing personal data

9.1 The processing of personal data is carried out by the controller at the location of the controller by individual authorized employees.

The processing of personal data is carried out by computer and manually in paper form, in compliance with the principles of personal data processing security.

9.2 To this end, the controller has adopted the following technical and organizational measures to ensure the protection of personal data, in particular measures to prevent unauthorized or accidental access to, alteration, destruction or loss of personal , as well as other misuse of personal :

a. electronic storage of personal data:

   The company uses internal registers based on xls tables to store and transfer personal data. Access to personal data files is secured with a password. Personal data is only handled by a responsible person on a dedicated computer with antivirus software. Access to the computer is secured with a password.

b. documenting the storage of personal data:
   in locked cabinets, keys kept in a locked drawer.

Art. 10 Clarification and rights of data subjects

10.1 In accordance with Article 12 of the EU Regulation, the controller must inform the data subject upon request of the data subject's right of access to personal data and to the following information:

a. purpose of treatment;
b. the category of personal concerned;
c. recipients or categories recipients, to whom disclosed personal data;
d. the planned period for which the personal data will be stored;
e. all available information about the source of the personal data.

10.2 Subject data, who will detect or suspects violation of legal norms concerning personal data, has the right to:

a. seek clarification from the controller;
b. require the controller to rectify the , particular to block, supplement, correct or delete the personal data. The data subject also has the right to apply to the supervisory authority, i.e. to the Office for Personal Data Protection;
c. if the data subject's request pursuant to point (b) is justified, the controller shall immediately remedy the breach;
d. if the controller does not rectify the disputed situation in accordance with point (c), the data subject has the right to apply to the supervisory authority, i.e. to the Office for Personal Data Protection.

Annex

to the internal regulations for the processing of personal data in accordance GDPR v.1 of 11.08.2023

List of authorized persons instructed and familiar with the contents of these Internal Rules:

Responsible person	Date	Signature
1. Yevgeny Kolesnik	11.9.2023	

Authorized person	Date	Signature
1. Alyona Tsurkan Knysh	11.9.2023	
2. Ulloa Wood Tamara Ailin	11.9.2023	