

PRIVACY NOTICE

on the processing of personal data relating to the business partners, suppliers,
subcontractors and visitors of Hungary Musashi Kft.

1.) Name, identification data and contact details of the Data Controller

Name: **Hungary Musashi Kft.**

Registered seat: **2840 Oroszlány, Bokodi út 11.**

E-mail address: **hu.gr.info@musashipaint.com**

Telephone number: **06-34-586-264**

Executive officer: **Baricza Péter**

Tax number: **13702393-2-11**

Hereinafter: **Data Controller**

2.) Basic terms used in this Notice

Data subject: any natural person identified or identifiable on the basis of any information.

Identifiable natural person: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data: any information relating to the data subject.

Special category data: any data belonging to the special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation.

Data concerning health: personal data relating to the physical or mental health of a natural person, including data relating to the provision of health care services to that natural person which reveal information about his or her health status.

Criminal personal data: personal data relating to the data subject which are generated during or prior to criminal proceedings in connection with a criminal offence or criminal proceedings, by bodies authorised to conduct criminal proceedings or to investigate criminal offences, as well as by the penitentiary organisation, and personal data relating to criminal records.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Controller: a natural or legal person or an organisation without legal personality which, within the framework defined by law or by a binding legal act of the European Union, alone or jointly with others determines the purposes of the processing of data, makes and implements decisions concerning data processing, including the means used, or has such decisions implemented by a data processor.

Joint Controller: a controller which, within the framework defined by law or by a binding legal act of the European Union, jointly with one or more other controllers determines the purposes and means of processing, makes and implements decisions concerning the processing, including the means used, jointly with one or more other controllers, or has such decisions implemented by a data processor.

Processing: any operation or set of operations performed on data, irrespective of the procedure applied. This includes in particular collection, recording, registration, organisation, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, blocking, erasure and destruction of data, as well as preventing the further use of data, taking photographs, audio or video recordings, and recording physical characteristics suitable for identifying a person, such as fingerprints or palm prints, DNA samples or iris images.

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

Indirect data transfer: the transfer of personal data to a controller or processor carrying out processing in a third country or within the framework of an international organisation by way of transfer to another controller or processor carrying out processing in another third country or within the framework of an international organisation.

Disclosure: making data accessible to anyone.

Erasure: rendering data unrecognisable in such a way that their restoration is no longer possible.

Restriction of processing: marking stored data with the aim of restricting their further processing.

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

Data processing: the set of processing operations carried out by a processor acting on behalf of or on the instructions of the Data Controller.

Processor: a natural or legal person or an organisation without legal personality which, within the framework and under the conditions defined by law or by a binding legal act of the European Union, processes personal data on behalf of or on the instructions of the Data Controller.

Data file: the totality of data processed in one register.

Third party: a natural or legal person or an organisation without legal personality which is not identical to the data subject, the Data Controller, the processor or those persons who, under the direct authority of the Data Controller or processor, perform operations aimed at processing personal data.

EEA State: a Member State of the European Union and any other state party to the Agreement on the European Economic Area, as well as any state whose citizen enjoys the same legal status as a citizen of a state party to the Agreement on the European Economic Area under an international treaty concluded between the European Union and its Member States and a state not party to the Agreement on the European Economic Area.

Third country: any state which is not an EEA State.

Personal data breach: a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transmission or disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed.

Profiling: any form of automated processing of personal data aimed at evaluating, analysing or predicting personal aspects relating to the data subject, in particular aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability, behaviour, location or movements.

Recipient: a natural or legal person or an organisation without legal personality to whom or to which personal data are made available by the Data Controller or processor.

Pseudonymisation: the processing of personal data in such a manner that, without the use of additional information stored separately from the personal data, it can no longer be determined to which data subject the personal data relate, and where technical and organisational measures ensure that the personal data cannot be attributed to an identified or identifiable natural person.

3.) Laws and other provisions serving as the basis for processing

The Data Controller has established and operates its data processing processes on the basis of the General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter: **GDPR**, and Act CXII of 2011 on Informational Self-Determination and Freedom of Information, hereinafter: **Information Act**.

The Data Controller applies the provisions of the GDPR in organic unity with the sectoral legislation of the European Union and Hungary applicable to its activities. Considering the complexity of the legal environment determining data processing, as well as the frequent amendments of statutory references and provisions, the Data Controller, instead of listing specific statutory references, identifies the areas of law which it takes into particular account when designing, operating and regularly reviewing its data processing processes:

- **Sector-specific legislation:** laws applicable to the scope of activities, for example labour, commercial or service-related legislation;
- **Financial and tax law rules:** provisions relating to tax, contribution and accounting obligations;
- **Property protection, occupational safety and other security legislation and standards:** rules determining the conditions and circumstances for the use of technical systems, such as electronic surveillance or access control systems, and measures serving the safety of data subjects and assets;
- **Other civil law and public law rules:** any additional European Union or Hungarian legislation, especially the provisions of the Civil Code relating to limitation periods and liability, which contains mandatory provisions for the Data Controller or regulates the enforcement of legal claims related to data processing.

4.) Data protection principles of the Data Controller

The Data Controller has designed and carries out its internal processes involving the processing of personal data of natural persons by taking appropriate technical and organisational measures, in such a way that they fully comply with the provisions of the GDPR and the Information Act. The Data Controller pays particular attention to ensuring that, within the framework of its economic activity and in its daily practice, while complying with other sectoral legislation applicable to it, the provisions of data protection legislation and the internal data protection policy are also implemented.

The Data Controller organises and carries out its data protection activities in such a way that they are lawful, fair, transparent and accurate, that processing is purpose-bound, and that only the data strictly necessary for the purpose of processing are processed and only for the period actually justified. The processing activities carried out within these processes are properly documented, and the Data Controller is at all times accountable in relation to such activities.

5.) Access to data and data security measures

Access to data and data transfer: The data processed by the Data Controller may be accessed exclusively by the Data Controller and those employees of the Data Controller for whom such access is indispensable for the performance of their duties.

The Data Controller transfers the personal data processed by it only to those contractual partners whose duty it is to process or handle the transferred data on the basis of a contract concluded with the Data Controller for this purpose. Prior to transferring personal data, the Data Controller has made sure that such contractual partners, and the data processing and data handling practices carried out by such contractual partners, comply with the applicable data protection legislation and internal regulations. The circumstances of the data transfer and of the processing or data handling carried out by the contractual partner are recorded in the contract concluded between the two parties. The fact and circumstances of such data transfers are recorded in the detailed description of the individual processing activities. Section 7 of this Notice.

Beyond the above, the Data Controller transfers the personal data processed by it only in exceptional cases, exclusively to authorities legally authorised to receive such data, where required by law or where such authorities request the data. The Data Controller keeps a separate register of such data transfers.

Data security measures: The Data Controller treats the electronic data recorded by it confidentially and stores them on the computers located at its registered seat indicated above, as well as on the server operated there. The method of data storage complies with the applicable data protection legislation. The data are protected by appropriate security measures.

The personal data processed in paper-based databases are stored by the Data Controller at its registered seat indicated above. Databases not currently in use are locked away. The place of storage is protected by appropriate security measures, equipment and devices.

6.) Rights of the data subject

Right to information: The data subject has the right to concise, transparent and intelligible information concerning the processing of his or her personal data. Such information must be provided in an easily accessible form, in a clear and plain manner and in a language fully understandable to the data subject, and must include all essential circumstances of the processing.

Where the Data Controller obtains the personal data from the data subject, it provides the data subject with the appropriate information before obtaining the data.

Where the personal data have not been obtained by the Data Controller from the data subject, the Data Controller provides the appropriate information to the data subject within a reasonable period after obtaining the data, but no later than within one month.

Where the personal data are used for the purpose of communicating with the data subject, the appropriate information must be provided no later than at the time of the first communication with the data subject. Where the personal data are expected to be disclosed to another recipient, the appropriate information must be provided no later than when the personal data are first disclosed.

Where the data subject requests information from the Data Controller concerning the exercise of his or her rights related to the processing of his or her data or concerning the circumstances of the processing, the Data Controller provides the appropriate information without undue delay, but no later than within one month from receipt of the relevant request. In the case of a

complex request, this deadline may be extended by a further two months. The data subject must be informed of the extension of the deadline.

Where the Data Controller does not take action in relation to the request, it informs the applicant thereof, indicating the reasons for the failure to act and the possibility for the data subject to lodge a complaint.

The Data Controller must provide the information and the measures related thereto free of charge. However, where the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive character, the Data Controller may, taking into account the administrative costs of providing the requested information or taking the requested measures, charge a reasonable fee or refuse to act on the request.

Right of access: The data subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning him or her are being processed, and, where such processing is taking place, to access the personal data and the following information: the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients, the envisaged period of storage of the data, the rights of the data subject concerning the processing listed below in this chapter, and the data subject's right to lodge a complaint. Furthermore, where the data were not collected from the data subject, the data subject has the right to information regarding their source, whether automated decision-making or profiling took place during the processing, and whether the personal data were transferred to a third country.

The Data Controller provides the data subject with the data subject to processing. For any further copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs.

Request for rectification of data: The data subject has the right to request that the Data Controller rectify or supplement inaccurate personal data concerning him or her without undue delay.

Right to erasure and right to be forgotten: The data subject has the right to request that the Data Controller erase personal data concerning him or her without undue delay, and the Data Controller is obliged to erase personal data concerning the data subject without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
the personal data must be erased for compliance with a legal obligation under European Union or Member State law applicable to the Data Controller;
- the personal data were collected in relation to the offer of information society services to children under the age of 16.

Where the Data Controller is required to erase personal data which it has previously made public, it must take all steps reasonably expected of it to ensure that every other controller which received the data from it after the disclosure also erases such data.

The Data Controller is not able to erase the data despite the request of the data subject where further processing of the data is necessary for one of the following reasons: for exercising the right of freedom of expression and information; for compliance with a legal obligation applicable to the Data Controller; for reasons of public interest in the area of public health; for

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims.

Right to restriction of processing: The data subject has the right to request that the Data Controller restrict processing where one of the following circumstances applies: the data subject contests the accuracy of the personal data; the processing is unlawful; the Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of a legal claim; or the data subject has objected to the processing.

Where processing is restricted, the personal data may, with the exception of storage, be processed only with the consent of the data subject or for the establishment or exercise of legal claims, or for reasons of important public interest.

Right to data portability: The data subject has the right to receive the personal data concerning him or her which he or she has provided to a controller in a structured, commonly used and machine-readable format. The data subject also has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on the voluntary consent of the data subject or on a contract concluded by the data subject, and where the processing is carried out by automated means. Where technically feasible, the data subject may request that the data be transmitted directly between controllers.

Right to object: The data subject has the right to object, on grounds relating to his or her particular situation, at any time to the processing of his or her personal data which is necessary for the performance of a task carried out in the public interest or for the enforcement of a legitimate interest, including profiling related to such processing. In such a case, the Data Controller may no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or which are related to the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, including profiling, the data subject has the right to object at any time to the processing of personal data concerning him or her for such purposes. Where the data subject objects to such processing, the personal data may no longer be processed for such purposes.

The Data Controller makes the relevant privacy notice available to data subjects in electronic form at the following web address: <https://musashipaint.hu/adatkezeles>

7.) Personal data processing relating to the Data Controller's business partners, suppliers and subcontractors

I. Personal data processing carried out in relation to the representatives, natural persons, of business partners as legal persons

Description of the processing process and its main circumstances: During its operation and in order to perform its tasks, HUNGARY MUSASHI Kft. processes the data detailed below of the natural person representatives of its business partners, as legal persons, with whom it has an economic relationship, in accordance with this Notice, which is available in electronic form at <https://musashipaint.hu/adatkezeles>. During this processing process, only those personal data of natural persons are recorded and used which are indispensable for the effective and efficient performance of the underlying economic activity, for maintaining contact and for fulfilling legal obligations.

Prior to concluding contracts and agreements in the course of business relations, the Data Controller draws the attention of the contracting parties to the privacy notice available in

electronic format. The Data Controller takes the measures expected of it to ensure that the data subjects receive the information. In this context, the Data Controller includes data protection clauses in the contracts concluded with business partners, in which the business partner, as a legal person, undertakes to make the privacy notice of HUNGARY MUSASHI Kft. known to its own affected representatives and contact persons. The Data Controller stores the data necessary for contact and representation in the register of representatives of business partners, as well as in materials related to the given economic activity, such as contracts and correspondence, both electronically and on paper.

The Data Controller, as well as its employees and subcontractors, may process the personal data of data subjects only in accordance with the contract concluded between the Data Controller and the represented legal person, and in accordance with this Notice. In addition, they are subject to a confidentiality obligation with regard to the personal data that come to their knowledge in connection with this activity. The persons performing data processing pay particular attention to ensuring that the personal data processed do not become known to unauthorised persons.

Legal basis of processing: The legitimate interest of the Data Controller.

Purpose of processing: Maintaining contact with the Data Controller's business partners having legal personality and performing the contracts concluded with them.

Scope of processed data: Name, company name, position, telephone number, e-mail address and other data related to the economic transaction.

Method of data storage: In electronic and paper-based databases.

Retention period of the data: Until the duration of the contractual relationship or agreement between the Data Controller and its business partners, subcontractors and suppliers having legal personality, or until the deadline defined by the relevant legislation, for example tax legislation, and further until the rights of the Data Controller arising in relation to such relationships can be enforced and its obligations can be fulfilled. Where there is a change in the persons acting as natural person representatives of business partners, the Data Controller keeps the data of the former representatives until the rights arising in relation to the contractual relationship can be enforced and the related obligations can be fulfilled.

Whether data transfer takes place during the processing and, if so, to which recipient: As a general rule, no data transfer takes place. Where, during the economic transaction, it becomes necessary to transfer such data, the Data Controller informs the data subject thereof.

Whether automated decision-making or profiling takes place during the processing: No.

II. Processing of the personal data of sole entrepreneur subcontractors

Description of the processing process and its main circumstances: During its operation and in order to perform its tasks, the Data Controller processes the personal data listed below of sole entrepreneurs with whom it has an economic relationship, in accordance with this Notice, which is available in electronic form at <https://musashipaint.hu/adatkezeles>. During this processing process, only those personal data of sole entrepreneurs are recorded and used which are indispensable for the effective and efficient performance of the underlying economic activity.

Prior to concluding contracts and agreements in the course of business relations, the Data Controller draws the attention of the contracting parties to the privacy notice available in electronic format. The Data Controller takes the measures expected of it to ensure that the data subjects receive the necessary information. In this context, the Data Controller includes data protection clauses in contracts concluded with sole entrepreneur business partners, in which the business partner declares that he or she has become familiar with the relevant privacy notice and undertakes to make the privacy notice of HUNGARY MUSASHI Kft. known to his or her

own affected representatives and contact persons. The Data Controller stores the data necessary for contact and representation in the register of representatives of business partners, as well as in materials related to the given economic activity, such as contracts and correspondence, both electronically and on paper.

The Data Controller, as well as its employees and subcontractors, may process the personal data of data subjects only in accordance with the contract concluded between the Data Controller and the sole entrepreneur business partner, and in accordance with this Notice. In addition, they are subject to a confidentiality obligation with regard to the personal data that come to their knowledge in connection with this activity. The persons performing data processing pay particular attention to ensuring that the personal data processed do not become known to unauthorised persons.

Legal basis of processing: Performance of contractual and legal obligations, and the consent of the data subject.

Purpose of processing: Maintaining contact with the Data Controller's sole entrepreneur business partners in order to perform the tasks set out in the contracts and agreements concluded with them.

Scope of processed data: Name, registered seat address, tax number, registration number, telephone number, e-mail address, type and registration number of vehicles used by the sole entrepreneur.

Method of data storage: In electronic and paper-based databases.

Retention period of the data: Until the duration of the contractual relationship or agreement between the Data Controller and the sole entrepreneurs, or until the deadline defined by the relevant legislation, for example tax legislation. Furthermore, until the rights of the Data Controller arising in relation to such relationships can be enforced and its obligations can be fulfilled.

Whether data transfer takes place during the processing and, if so, to which recipient: As a general rule, no data transfer takes place. Where, during the economic transaction, it becomes necessary to transfer such data, the Data Controller informs the data subject thereof.

Whether data transfer takes place during the processing and, if so, to which recipient: Data are transferred to ASC Adószakértő Kft. — registered seat: 2890 Tata, Országgyűlés tér 3. — a subcontractor providing accounting services to the Data Controller, for the purpose of carrying out accounting and data reporting tasks.

Whether automated decision-making or profiling takes place during the processing: No.

III. Entry and exit control of business clients, subcontractors, contractors carrying out deliveries and dispatches, and other persons and vehicles arriving at the company's site

Description of the processing process and its main circumstances: The Data Controller records the personal data listed below of business clients, subcontractors, contractors carrying out deliveries and dispatches and other persons arriving at its factory, site, for occupational safety and security purposes, and in order to ensure the uninterrupted operation of business and production processes, and processes them in accordance with this Notice. Before entering the site and before the recording of data, data subjects have the opportunity to familiarise themselves with and study the privacy notice relating to them in printed form at the place of entry control. Before the data are recorded, persons entering the site make a written declaration regarding the provision of the information. These declarations are stored in a separate folder.

The security service of the factory may inspect the packages of persons leaving the factory area and the cargo and passenger compartments of vehicles in compliance with the provisions of the Property Protection Act and with respect for the personality rights of the data subjects.

Legal basis of processing: The legitimate interest of the Data Controller arising from occupational safety legislation and related to property protection.

Purpose of processing: Enforcing occupational safety rules at the Data Controller's site in accordance with the applicable legislation, and ensuring the protection of the life and physical integrity of persons staying at the site, the protection of assets and valuables located there, and the uninterrupted operation of production and business processes.

Scope of processed data: Name, company name, time of entry, time of exit, purpose of entry, host person or department, colour, type and registration number of the vehicle driven or used by the person entering, products, goods, tools or parts delivered to or dispatched from the site, and any documentation prepared in connection with the entry.

Method of data storage: In a paper-based database.

Retention period of the data: The Data Controller stores the data related to the entry of representatives of service providers, business partners and other persons arriving at the site generally for one month. Where the Data Controller has an obligation or legitimate interest in relation to a particular entry, the data processed in connection with the entry of the person concerned are stored until such obligation or legitimate interest ceases to exist.

Whether data transfer takes place during the processing and, if so, to which recipient: No.

Processor involved in the process: IK Universal Bt. — registered seat: 2200 Monor Aradi u. 14. — as the property protection service provider of the Data Controller, for the purpose of recording data at the entry point.

Whether automated decision-making or profiling takes place during the processing: No.

IV. Personal data processing related to extraordinary events

Description of the processing process and its main circumstances: In compliance with its obligations set out in the applicable legislation, the Data Controller, upon detecting extraordinary events, takes the necessary measures to protect human life and valuables, to provide first aid and damage prevention, and to investigate the aspects of the event affecting it. Documents generated in connection with extraordinary events are handled confidentially in separate paper-based and electronic folders, in compliance with the appropriate data protection measures. With regard to processing carried out in relation to extraordinary events, the Data Controller acts in accordance with the provisions of this privacy notice. Data subjects may familiarise themselves with the provisions of the notice before the commencement of processing, and the notice is also available at the company's secretariat at its registered seat during official working hours.

Legal basis of processing: Compliance with the legal obligation of the Data Controller, the voluntary consent of the data subject and the legitimate interest of the Data Controller.

Purpose of processing: Handling extraordinary events in the manner prescribed by law.

Scope of processed data: Name of the data subject, maiden name, place and date of birth, telephone number, e-mail address and the circumstances relevant to the extraordinary event.

Method of data storage: In electronic and paper-based databases.

Retention period of the data: Until the obligations and rights of the Data Controller relating to the extraordinary event cease to exist, but at least for two years after the investigation of the extraordinary event.

Whether data transfer takes place during the processing and, if so, to which recipient: Cannot be determined in advance.

Whether automated decision-making or profiling takes place during the processing: No.

8.) Handling of personal data breaches

The Data Controller notifies the supervisory authority of a personal data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Data Controller keeps a register of personal data breaches in accordance with statutory requirements, and retains the data contained therein for five years. The register relating to personal data breaches contains the following data: the categories and number of data subjects affected by the personal data breach, the categories of personal data affected, the date of the personal data breach, the circumstances and effects of the personal data breach, and the measures taken to remedy the personal data breach.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller informs the data subject of the breach without undue delay. The information clearly and plainly describes the nature and main circumstances of the personal data breach, as well as the measures taken by the Data Controller to remedy it.

The supervisory authority may also order that data subjects be informed where, on the basis of its assessment, it considers that the personal data breach entails a high risk.

The Data Controller is not required to inform the data subject of the personal data breach where any of the following conditions is met:

- the Data Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the data affected by the breach, in particular measures such as encryption which render the data unintelligible to persons not authorised to access them;
- the Data Controller has taken further measures following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- providing the information would involve disproportionate effort. In such cases, the Data Controller informs the data subjects by means of publicly disclosed information or takes a similar measure which ensures similarly effective information of the data subjects.

9.) Legal remedies

Where a data subject has a complaint concerning the processing of his or her personal data, it is advisable to address it primarily to the Data Controller in order to clarify the matter as soon as possible and to settle it amicably. In addition, every data subject is entitled, where he or she considers that the Data Controller has infringed the data protection legislation applicable to it during the processing of his or her personal data, to lodge a complaint with the supervisory authority according to his or her habitual residence, place of work or the place of the alleged infringement. Furthermore, every natural and legal person is entitled to an effective judicial remedy against a legally binding decision of the supervisory authority concerning him or her. Every data subject is also entitled to an effective judicial remedy where he or she considers that his or her rights related to the processing of personal data have been infringed as a result of non-compliance with data protection legislation.

Supervisory Authority: Hungarian National Authority for Data Protection and Freedom of Information — NAIH

Registered seat: 1055 Budapest, Falk Miksa utca 9-11

Postal address: 1363 Budapest, Pf.: 9.

Telephone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu

Website: <https://naih.hu/>

Judicial remedy may be initiated before the Tatabánya District Court competent according to the registered seat of the Data Controller.

Oroszlány, 11 May 2026.

.....
Managing Director