Company name: BPM-Art Kft.
Company reg. number: 19-09-511783
Registered seat: 8230 Balatonfüred, Balaton utca 42. (Hungary)
Tax number: 14849255-2-19

PRIVACY POLICY

1. INTRODUCTION

BPM-Art Kft. (otherwise referred to herein as “controller” or “we”) throughout its operation is committed to protect any personal data that is processed by us, to comply with the legal provisions and handle the data in a safe and respectable way.

NAME AND CONTACT DATA OF THE DATA CONTROLLER:

Company name: BPM-Art Kft.
Company reg. number: 19-09-511783
Registered seat: 8230 Balatonfüred, Balaton utca 42. (Hungary)
Tax number: 14849255-2-19

In the course of its operation the controller pays special attention to protect personal data, to comply with the mandatory legal regulation and to ensure fair and safe data management.

When compiling this privacy notice, the controller relied mainly on the following legislation:

- Act CXIX of 1995 on The Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (Hungarian Direct Marketing Act)

- Act CVIII of 2001 on Certain Issues of Electronic Commerce Activities and Information Society Services

- Act XLVIII of 2008 on Advertising (Advertising Act)

- Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information (Info Act)

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)

2. DEFINITIONS

- **data subject** means a natural person identified or identifiable based on any information; 1a. identifiable natural person means 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** means any data relating to the data subject;
- **sensitive data** means all data falling in the special categories of personal data that are personal data revealing racial or ethnic origin, political opinion, religious belief or

worldview, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

- **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his health status;

- **criminal personal data** means personal data related to the data subject and to a criminal record, generated by organs authorised to conduct criminal proceedings or to detect criminal offences, or by the prison service during or prior to criminal proceedings, in connection with a criminal offence or criminal proceedings;

- **data of public interest** means information or data other than personal data, registered through any method or in any form, pertaining to the activities of and processed by the organ or person performing state or local government duties and other public duties defined by law, or generated in the course of performing their public duties, irrespective of the method or form in which it is recorded and regardless of its singular or collective nature; in particular, data concerning material competence, territorial competence, organisational structure, professional activities and the evaluation of their performance, the type of data held and the laws governing its operation, as well as data concerning financial management and concluded contracts;

- **data accessible on public interest grounds** means any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public;

- **consent** means any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which he, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him;

- **controller** means the natural or legal person, or organisation having no legal personality, which, within the framework laid down in an Act or in a binding legal act of the European Union, alone or jointly with others, determines the purposes of data

processing, makes decisions concerning data processing (including the means used) and implements such decisions or has them implemented by a processor;

- **joint controller** means the controller which, within the framework laid down in an Act or in a binding legal act of the European Union, jointly with one or more other controllers, determines the purposes and means of data processing, and, jointly with one or more other controllers, makes decisions concerning data processing (including the means used) and implements such decisions or has them implemented by a processor;

- **processing** means any operation or set of operations that is performed on data, regardless of the procedure applied; in particular collecting, recording, registering, organising, storing, modifying, using, retrieving, transferring, disclosing, synchronising or connecting, blocking, erasing and destroying the data, as well as preventing their further use; taking photos and making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples and iris scans);

- **processing for law enforcement purposes** means processing by an organ or person (hereinafter jointly “organ carrying out processing for law enforcement purposes”) which is, within its or his functions and powers laid down by law, engaged in an activity aimed at preventing or eliminating threats to public order or public safety, preventing and detecting criminal offences, carrying out, or contributing to, criminal proceedings and preventing and detecting infractions, as well as carrying out, or contributing to, infraction proceedings, and implementing the legal consequences imposed in criminal proceedings or infraction proceedings, within the limits and for the purpose of this activity, including the processing of personal data connected to this activity for archival, scientific, statistical or historical purposes (hereinafter jointly “law enforcement purpose”);

- **processing for national security purposes** means processing by the national security services, within their functions and powers laid down by law, as well as processing under the Act on national security services by the counter-terrorism organ of the police, within its functions and powers laid down by law;

- **processing for national defence purposes** means processing under the Act on data processing by the defence forces and the Act on national defence and the Hungarian Defence Forces, as well as the measures that can be introduced during a special legal order, and the Act on the registration of foreign armed forces staying in the territory of the Republic of Hungary for service purposes and of the international headquarters and their staff established in the territory of the Republic of Hungary, as well as on certain provisions concerning their status;

- **data transfer** means providing access to the data for a designated third party;

- **onward data transfer** means the transfer of personal data, by way of transfer to a controller or processor engaged in data processing in any third country or in the

framework of an international organisation, to a controller or processor engaged in data processing in any other third country or in the framework of an international organisation;

- **international organisation** means an organisation, and its subordinate bodies, governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two or more states;

- **disclosure** means making the data accessible to anyone;

- **data erasure** means making the data unrecognisable in such a way that its restoration is no longer possible;

- **restriction of processing** means the blocking of stored data by marking them with the aim of limiting their processing in the future;

- **data destruction** means the complete physical destruction of the data medium that contains the data;

- **technical processing** means the totality of data processing operations performed by the processor acting on behalf of, or instructed by, the controller;

- **processor** means a natural or legal person, or an organisation not having legal personality which, within the framework and under the conditions laid down in an Act or in a binding legal act of the European Union, acting according to a mandate or instructions given by the controller, processes personal data;

- **data source** means the organ performing public duties, which generated the data of public interest that is to be published through electronic means, or during the operations of which such data was generated;

- **data publisher** means the organ performing public duties which, if the data source itself does not publish the data, uploads the data sent to it by the data source to a website;

- **dataset** means all data processed in a single registry;

- **third party** means a natural or legal person, or an organisation having no legal personality, other than the data subject, controller, processor and the persons who, under the direct authority of the controller or processor, carry out operations aimed at processing personal data;

- **EEA State** means any Member State of the European Union and any State Party to the Agreement on the European Economic Area, as well as any state the nationals of which enjoy the same legal status as nationals of State Parties to the Agreement on

the European Economic Area on the basis of an international agreement concluded between the European Union and its member states and the state which is not party to the Agreement on the European Economic Area;

- **third country** means any state that is not an EEA State;

- **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transfer or disclosure of, or unauthorised access to, personal data transferred, stored or otherwise processed;

- **profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- **recipient** means a natural or legal person, or an organisation having no legal personality, for which the controller or the processor provides access to the personal data;

- **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

3. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Personal data shall be processed only for clearly specified and legitimate purposes, in order to exercise certain rights and fulfil obligations. The purpose of processing shall be met in all stages of processing, data shall be collected and processed fairly and lawfully.

Only personal data that is essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose.

In the course of processing, data shall retain their personal character as long as their connection with the data subject can be restored. The connection with the data subject shall, in particular, be considered restorable if the controller is in possession of the technical means necessary for the restoration.

The accuracy and completeness, and, if deemed necessary with respect to the purpose of the processing, the up-to-date status of the data shall be ensured throughout the processing; the identification of the data subject shall be possible for no longer than necessary for the purpose of the processing.

During processing, appropriate technical or organisational measures shall be applied to ensure the appropriate security of personal data, including, in particular, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. The processing of personal data shall be deemed fair and lawful if, for the purpose of ensuring the data subject's right to the freedom of expression, the person wishing to find out the opinion of the data subject visits him at his domicile or place of residence, provided that the data subject's personal data are processed in compliance with this Act and contacting him is not intended for business purposes. Personal visits are not permitted on public holidays under the Labour Code.

Personal data may be processed if the data subject has given explicit consent to the processing of personal data or it is prescribed in an Act or, based on the authorisation of an Act, within the limits set forth therein and for data other than sensitive and criminal personal data, in a local government decree for purposes in the public interest.

The controller or the processor acting on behalf of, or instructed by, the controller falling under the scope of this Act may transfer, including by way of onward data transfer, personal data to a controller or processor engaged in processing in a third country or in the framework of an international organisation (hereinafter jointly "international data transfer") if the data subject has given explicit consent to the international data transfer, or it is allowed by law and the adequate level of protection of the personal data transferred is provided by the controller or processor engaged in processing in the third country or in the framework of an international organisation.

For mandatory processing, the type of data, the purpose and conditions of processing, the access to such data, the controller and the duration of the processing or the regular examination of its necessity shall be specified by the Act or local government decree ordering mandatory processing.

The company shall not make personal data public. However, the law may prescribe – with the explicit description of the personal data – the publication of personal data of public interest. In any other case the publication is subject to the consent of the data subject. In the case of any doubt, it shall be presumed that the data subject has refused to grant his or her consent.

The consent of the person concerned shall be considered given in respect of the data disclosed by him in the course of his public appearance, or delivered by him for the purpose of publication.

In the proceedings instituted at the request of the person concerned, his consent to the handling of his necessary data shall be presumed. The attention of the person concerned shall be drawn to this fact.

The person concerned may give his consent in a written contract. The contract shall set out the subject matter, the duration, the nature and the purpose of the processing, the type of

personal data concerned and the categories of data subjects, as well as the rights and obligations of the processor and the controller.

Unless an Act provides exemption, any other interests attached to data handling, also including the publicity of the data of public interest may not violate the right attached to the protection of personal data and the right to privacy of the person concerned.

3. PROCESSING

The legal basis for processing is your freely given, specific, informed and unambiguous consent, which extends to the processing carried out for the purposes specified in this privacy policy.

Concerning the visitors of the website

The controller, in the course of its operation, does **not** record IP addresses and any personal data.

The use of *cookies* can be banned within the settings of your browser.

Further information on Google's and Facebook's privacy policy can be checked on the links below:

http://www.google.com/privacy.html and https://www.facebook.com/about/privacy

4. DATA SECURITY

Website operator

Name: BPM-Art Kft.

Registered seat: 8230 Balatonfüred, Balaton utca 42. (Hungary)

Electronic mailing address: *info@picturecars.eu*

We take appropriate technical and organisational measures to ensure the protection of your personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular but not limited to where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

5. REQUESTING INFORMATION, YOUR RIGHTS AND OPTIONS FOR LEGAL REMEDY

You may request information about the processing of your personal data anytime. Upon your request Controller shall provide detailed information concerning the data relating to you (Subject), including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and – in case of data transfer – the legal basis and the recipients.

The controller shall maintain a record of its processing operations related to the personal data that it processes, personal data breaches and the measures taken concerning the data subject's right of access (hereinafter jointly „controller's record"). The controller shall record in the controller's record

- the scope of data subjects and of the data processed
- the circumstances of personal data breaches that occurred in the context of the data that it processes, as well as their effects and the measures taken to address them
- other data specifically defined in the Info Act

For the purpose of facilitating the enforcement of the data subject's rights, the controller shall implement appropriate technical and organisational measures, in particular, assessing, within the shortest possible time from its submission, but not later than within twenty-five days, the request submitted by the data subject for the purpose of the enforcement of his rights, and it shall notify the data subject of the decision in writing. The controller shall perform its duties free of charge. If more than one request was submitted fees may be charged, which can be included in the contract between the parties. Fees already paid, should be refunded in the event of unlawful processing. Unreal personal data must be corrected by the controller.

For the purpose of the enforcement of the right to erasure, the controller shall erase the data subject's personal data without delay if the processing is unlawful, the processing is contrary to the principles laid down in section 4 of the Info Act, the purpose of processing has terminated, or further processing is not necessary for the realisation of the purpose of processing, the period laid down has elapsed or the erasure of the data is required by the law.

If, the controller rectifies the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller, it shall notify the controller to whom it has transferred the personal data affected by the rectification on the existence of rectification, as well as on the rectified personal data.

You may object to such processing of your personal data in accordance with the provisions of the applicable law. Controller shall review your objection – concurrently with suspending the processing – as soon as possible, but not later than within fifteen days of the objection and shall notify the client in writing at the contact address (postal address) listed by client, provided that such contact address had been listed in client's request. Failing that, the

fifteen-day time limit prescribed for the Controller shall only be considered expired, after the client has provided his address to the Controller in a verifiable manner.

In case the objection is justified, Controller shall cease data processing, including all further data recordings and transfers, and shall block the data, and notify all parties about the objection and the measures taken on that basis to whom such objected data had been transferred and who are obliged to act to enforce the right to object. If the client finds the decision made by the Controller in response to the objection questionable, the Client may bring action at a court within thirty days of having learned of the decision.

The controller shall be exempted from the obligation of informing the data subject according to paragraph 9 and 19 of the Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information (Info Act).

If a request for data is refused, the requesting party shall be notified thereof within 15 days in writing or, if the requesting party has given his electronic mailing address, by electronic means, and he shall be informed of the reasons for refusal, and the legal remedies that are available for him.

The controller shall keep records on the requests dismissed, including the reasons for them, and shall inform the Authority of them each year, by 31 January.

Requests for legal remedy and complaints may be submitted to the Hungarian National Authority for Data Protection and Freedom of Information:

Name: Hungarian National Authority for Data Protection and Freedom of Information
(Nemzeti Adatvédelmi és Információszabadság Hatóság)
Address: 1125 Budapest Szilágyi Erzsébet fasor 22/c.
Website: www.naih.hu
Electronic mailing address: ugyfelszolgalat@naih.hu
Telephone: 06 1 39 11 400
Fax: 06 1 39 11 410

Balatonfüred,

30 December, 2020