

## **REGULATION**

### **on the ways of processing and using personal data of REVIEW BOOSTER PRO Ltd**

#### **Article 1**

This Regulation, with the task of protecting it, regulates categories of personal data, purposes, processing and protection of personal data.

This Regulation, in terms of the obligation of its content, applies to clients, employees, and to third parties in the contractual relationship (Data subjects) with REVIEW BOOSTER PRO Ltd (hereinafter referred to as RBP), and other persons whose personal data are processed by RBP (Data subjects) in the part of the processing of personal data and in the part in which the provisions of individual contracts are not otherwise contracted.

This Regulation does not apply to the processing of data concerning legal entities, including their form and contact details.

An integral part of this Regulation are annexes related to the processing of personal data of certain categories of Data Subjects.

For all relations not regulated by this Regulation, the provisions of the General Data Protection Regulation (GDPR) and the Law on the Implementation of the General Data Protection Regulation will apply directly.

#### **Article 2**

As the data controller, RBP undertakes to process personal data lawfully, fairly and transparently.

About the Controller:

REVIEW BOOSTER PRO Ltd, Zagreb, Stenjevečka ul. 28, VAT ID: HR25407983967

#### **Article 3**

For the purposes of this Regulation, the following terms have these meanings:

- (1) 'personal data' means all data relating to an individual whose identity has been established or identifiable ("data subject"); an identifiable individual is a person who can be identified directly or indirectly, in particular by means of identifiers such as name, identification number, location data, online identifier or by means of one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;
- (2) 'processing' means any procedure or set of procedures performed on personal data or on sets of personal data, whether automated or by non-automated means such as collection,

recording, organisation, structuring, storage, adaptation or modification, finding, inspecting, using, detecting by transfer, dissemination or making available otherwise, harmonising or combining, restricting, deleting or destroying;

- (3) 'restricting processing' means the labelling of stored personal data with a view to limiting their processing in the future;
- (4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to assess certain personal aspects related to an individual, in particular to analyse or anticipate aspects relating to the performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement of that individual;
- (5) 'controller' means RBP;
- (6) 'data subject' means customers, employees, business partners, third parties in a contractual relationship, and persons whose personal data are processed by RBP;
- (7) 'the recipient' means a natural or legal person, a public authority, an agency or another body to which personal data is disclosed, regardless of whether it is a third party;
- (8) 'a third party' means a natural or legal person, a public authority, an agency or other body other than the data subject, the controller, the processor or persons authorised to process personal data under the direct jurisdiction of the controller or processor;
- (9) 'consent' of the data subject means any voluntary, specific, informed and unambiguous expression of the data subject's wishes by which he or she gives consent to the processing of the personal data relating to him or her by means of a statement or a clear affirmative action;
- (10) 'personal data breach' means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transferred, stored or otherwise processed;
- (11) 'biometric data' means personal data obtained by specific technical processing relating to the physical characteristics, physiological or behavioural characteristics of an individual that enable or confirm the unique identification of that individual, such as facial photographs or dactyloscopic data;
- (12) 'health-related data' means personal data relating to an individual's physical or mental health, including the provision of health services, providing information on his or her health status;
- (13) 'the main establishment' of RBP stands for the Republic of Croatia;
- (14) 'processor' means a natural or legal person, a public authority, an agency or other body that processes personal data on behalf of the controller;
- (15) 'enterprise' means a natural or legal person engaged in economic activity, irrespective of the legal form of that activity, including partnerships or associations that regularly engage in economic activity;
- (16) 'group of undertakings' means an undertaking in a dominant position and its subordinate undertakings;
- (17) 'supervisory authority' means the Personal Data Protection Agency;
- (18) 'regulation' means the General Data Protection Regulation.
- (19) 'the relevant and reasoned objection' means an objection to the draft decision as well as whether there has been a breach of this Regulation, or whether the action is provided for in relation to the controller or processor in accordance with this Regulation, which clearly demonstrates the importance of the risks posed by the draft decision regarding the fundamental rights and freedoms of the data subject and, where applicable, the free flow of personal data within the Union.

- (20) 'Employee' – a person in employment in the company (including on the basis of employment contracts, employment contracts and copyright agreements, student contracts, and other legal forms).

## **PRINCIPLES OF PROCESSING PERSONAL DATA**

### **Article 4**

1. Personal data must be:
  - (a) lawfully, fairly and transparently processed with regard to the data subject ('legality, fairness, transparency');
  - (b) collected for specific, explicit and lawful purposes and may not be further processed in a manner inconsistent with those purposes; further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, shall not be considered incompatible with the original purposes ('purpose limitation');
  - (c) appropriate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data volume reduction');
  - (d) accurate and up-to-date if necessary; any reasonable measure must be taken to ensure that personal data that are not accurate, taking into account the purposes for which they are processed, are deleted or corrected without delay ("accuracy");
  - (e) kept in a form that allows the identification of the data subject only for as long as necessary for the purposes for which the personal data are processed; except in the case of processing for scientific, statistical or research purposes;
  - (f) processed in a way that ensures the proper security of personal data, including protection against unauthorised or illegal processing and against accidental loss, destruction or damage by applying appropriate technical or organisational measures ('integrity and confidentiality');

### **Article 5**

The lawfulness of processing is ensured in such a way that at least one of the following processing grounds must be met when processing the Data Subject's personal data:

- (a) the data subject has given his consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of the contract in which the data subject is a party or to take action at the request of the data subject before the conclusion of the contract;
- (c) processing is necessary in order to comply with the legal and legal obligations of the controller;
- (d) processing is necessary to protect the key interests of the data subject or other natural person;
- (e) processing is necessary for the performance of a task in the public interest or for the exercise of the official authority of the controller;
- (f) processing is necessary for the legitimate interests of the controller or a third party, except where the interests or fundamental rights and freedoms of data subjects

requiring the protection of personal data, in particular where the data subject is a child, would be stronger than those interests.

### **Article 6**

When the controller carries out the processing for purposes other than the purpose for which the data were originally collected, and if the same processing is in line with the original purpose, the controller will be deemed to be sufficient for the subsequent processing of the data.

If the processing for a purpose other than the purpose for which the data was collected is not based on the consent of the data subject, the controller, with a view to determining whether the processing for another purpose is in accordance with the purpose for which the personal data were originally collected, shall be taken into account, inter alia:

- (a) any link between the purposes of the collection of personal data and the purposes of the intended continuation of processing;
- (b) the context in which the personal data were collected, in particular as regards the relationship between the data subject and the controller;
- (c) the nature of personal data, in particular the fact that specific categories of personal data are being processed
- (d) possible consequences of the intended continuation of processing for data subjects;
- (e) the existence of appropriate safeguards.

## **APPROVAL**

### **Article 7**

When the processing of the Data Subject's personal data is based on consent, the controller must prove the existence of consent.

The data subject may also give consent as part of a document relating to other issues, but the request relating to consent must be as clearly distinguished as possible from the rest of the text, and understandable to the Data Subject.

The data subject has the right to withdraw his/her consent at any time in the same form as consent and given.

The withdrawal of consent shall not affect the lawfulness of processing on the basis of consent prior to its withdrawal. Before giving consent, the data subject shall be informed. If the consent of the Data Subject represents only one of the basics of the processing of personal data, the RBP is authorized to continue the processing of personal data from another lawful basis.

## PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

### Article 8

1. It shall be prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data relating to health or data on an individual's sex life or sexual orientation.
2. Paragraph 1 of this Article does not apply if one of the following is met:
  - (a) the data subject has given explicit consent to the processing of these personal data for one or more specific purposes, unless the law of the Republic of Croatia stipulates that the data subject cannot lift the prohibition referred to in paragraph 1;
  - (b) processing is necessary for the purpose of fulfilling obligations and exercising the special rights of the controller or data subject in the field of labour law and social security and social protection law to the extent that it is granted under the law of the Republic of Croatia or the collective agreement in accordance with the law of the prescribes appropriate safeguards for the fundamental rights and interests of the data subject;
  - (c) processing is necessary to protect the vital interests of the data subject or other individual if the data subject physically or is legally unable to give consent;
  - (d) processing shall be carried out as part of legitimate activities with appropriate safeguards by a foundation, association or other non-profit body with a political, philosophical, religious or trade union objective, and provided that the processing concerns only members or former members of the body or persons who have regular contact with it in relation to its purposes and that personal data have not been communicated to anyone outside that body without that body consent of the data subjects;
  - (e) processing refers to personal data that is clearly published by the data subject;
  - (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts act in an judiciary capacity;
  - (g) processing is necessary for the purposes of significant public interest based on the law of the Republic of Croatia, which is proportionate to the desired goal and which respects the essence of the right to data protection and provides appropriate and special measures to protect the fundamental rights and interests of the data subject;
  - (h) processing is necessary for public interest purposes in the field of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicines and medical devices, under Union law or Member State law, which lays down appropriate and specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy;
  - (i) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, and is proportionate to the objective pursued, which respects the essence of the right to data protection and provides adequate and specific measures to protect the fundamental rights and interests of the data subject.

## **PROCESSING BIOMETRIC DATA**

### **Article 9**

The processing of biometric data may be carried out for the purpose of the necessity of the protection of persons, property, classified data, trade secrets or for the individual and secure identification of service users, taking into account that the interests of data subjects contrary to the processing of biometric data referred to in this Article do not prevail.

The legal basis for the processing of biometric data of data subjects in order to safely identify the users of the services is the explicit consent of the Data subject.

The processing of employee biometric data for the purpose of recording working hours and for the purpose of entering and leaving official premises is permitted, if required by law or if such processing is carried out alternatively to another solution for recording working hours or entry and exit from official premises provided that the employee has given explicit consent for such processing of biometric data in accordance with the provisions of the General Data Protection Regulation.

## **VIDEO SURVEILLANCE**

### **Article 10**

1. Video surveillance within the meaning of the provisions of this Regulation concerns the collection and further processing of personal data involving the creation of a recording that constitutes or is intended to form part of a storage system.
2. The processing of personal data through video surveillance may be carried out only for the purpose necessary and justified for the protection of persons and property, taking into account that the interests of the data subjects that are contrary to the processing of data through video surveillance do not prevail.
3. Video surveillance may only cover premises or parts of premises whose supervision is necessary to achieve the purpose referred to in paragraph 2 of this Article.
4. The controller or processor is obliged to mark that the object or individual room in it is under video surveillance, and the marking should be visible no later than when entering the recording perimeter.
5. The notification referred to in paragraph 4 of this Article shall contain all relevant information, in particular a simple and easy-to-understand picture accompanied by the text providing the following information to respondents:
  - that the space is under video surveillance,
  - data about the controller,
  - contact details through which the data subject can exercise his or her rights.
6. The right of access to personal data collected through video surveillance is granted to the responsible person of the controller or processor or the processor and/or the person authorized by him.

7. Persons referred to in paragraph 6 of this Article may not use footage from the video surveillance system contrary to the purpose laid down in paragraph 2 of this Article of the Regulations.
8. The video surveillance system must be protected from access by unauthorized persons.

### **Article 11**

Recordings obtained through video surveillance may be kept for a maximum of 6 months unless the other law provides for a longer retention period or if the evidence is in judicial, administrative, arbitration or other equivalent proceedings.

### Video surveillance of workspaces

### **Article 12**

1. The processing of personal data of employees through a video surveillance system may be carried out only if, in addition to the conditions laid down in this law, the conditions laid down in the regulations governing occupational safety are also met and if the employees were informed individually in advance of such a measure and if the employer informed the employees before deciding on the installation of the video surveillance system.
2. Video surveillance of the working areas shall not include rest rooms, personal hygiene and changing rooms.

## **INFORMATION AND ACCESS TO PERSONAL DATA**

### **Article 13**

1. If the personal data relating to the data subject are collected from the data subject, the controller will provide the data subject with all the following information at the time of collecting the personal data:
  - (a) the identity and contact details of the controller and, where applicable, the representatives of the controller;
  - (b) contact details of the data protection officer, if applicable;
  - (c) processing purposes for which personal data are used as well as the legal basis for processing;
  - (d) where the processing is based on Article 5(1)(f) of the legitimate interests of the controller or a third party;

- (e) recipients or categories of recipients of personal data, if any; and
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation;
- (g) the period in which the personal data will be stored or, if this is not possible, the criteria establishing that period;
- (h) the existence of the right to require the controller to access personal data and to correct or delete personal data or to restrict the processing relating to the data subject or the right to object to the processing of such and the right to data portability;
- (i) where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time without affecting the lawfulness of the processing based on consent before it was withdrawn;
- (j) the right to lodge a complaint with the supervisory authority;
- (k) information on whether the provision of personal data is a legal or contractual obligation or condition necessary for the conclusion of the contract and whether the data subject has an obligation to provide personal data and what are the possible consequences if such data are not provided;
- (l) the existence of automated decision-making, including profiling and, in those cases, meaningful information on the logic involved, as well as the importance and anticipated consequences of such processing for the data subject.

If the controller intends to further process personal data for a purpose other than that for which the personal data were collected, the controller shall, before that additional processing, provide the data subject with information about that other purpose and any other relevant information referred to in the previous paragraph.

The obligation of the controller referred to in this Article shall not apply if and to the extent that the data subject already has the information provided.

The information referred to in Article 13 and Article 14 of this Regulation shall be provided in a concise and comprehensible manner, and in writing or other means, inter alia, where appropriate, electronically. If requested by the data subject, the information may be provided orally, provided that the identity of the data subject is established by other means.

## **Article 14**

1. If the personal data are not obtained from the data subject, the controller shall provide the data subject with the following information:

- (a) the identity and contact details of the controller and the representatives of the controller, if applicable;
- (b) contact details of the data protection officer, if applicable;
- (c) the purposes of processing to which personal data are intended as well as the legal basis for processing;
- (d) categories of personal data in question;
- (e) recipients or categories of recipients of personal data, as appropriate;
- (f) the intention of the controller to transfer personal data to the recipient in a third country or international organisation where applicable



- (g) the period in which the personal data will be stored or, if this is not possible, the criteria establishing that period;
- (h) if the processing is based on Article 5(1). Point (f) legitimate interests of the controller or third party;
- (i) the existence of the right to require the controller to access personal data and to correct or delete personal data or to restrict the processing relating to the data subject and the right to object to processing and the right to data portability;
- (j) where the processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before it was withdrawn;
- (k) the right to lodge a complaint with the supervisory authority;
- (l) the source of personal data and, where appropriate, whether they come from publicly available sources;
- (m) the existence of automated decision-making, including profiling and, in those cases, meaningful information on the logic involved, as well as the importance and anticipated consequences of such processing for the data subject.

The controller provides the information from the previous entry:

- (a) within a reasonable period after obtaining personal data, and no later than one month, taking into account the specific circumstances of the processing of personal data;
- (b) if personal data are to be used to communicate with the data subject, at the latest at the time of the first communication made with that data subject; or
- (c) where the disclosure of the data to the other recipient is foreseen, at the latest at the moment when the personal data was first disclosed.

If the controller intends to further process personal data for a purpose other than that for which the personal data were collected, the controller shall, before that additional processing, provide the data subject with information about that other purpose and any other relevant information referred to in the previous paragraph.

The obligations of the controller referred to in this Article do not apply if and to the extent that:

- (a) the data subject already has information;
- (b) providing such information is impossible or would require disproportionate efforts; in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes,
- (c) obtaining or disclosing data is explicitly prescribed by the law of the Republic of Croatia, which provides for appropriate measures to protect the legitimate interests of the data subject; or
- (d) where personal data must remain confidential in accordance with the obligation to keep professional secrecy governed by the law of the State, including the obligation to keep a secret referred to in the statute.

## **THE RIGHT OF THE DATA SUBJECT TO ACCESS**

### **Article 15**

1. The data subject has the right to obtain confirmation from the controller whether the personal data relating to him or her are being processed and if such personal data are processed, access to personal data and the following information:
  - (a) purpose of processing;
  - (b) categories of personal data in question;
  - (c) recipients or categories of recipients to whom personal data has been disclosed or will be disclosed, in particular recipients in third countries or international organisations;
  - (d) where possible, the foreseen period in which the personal data will be stored or, where this is not possible, the criteria used to determine that period;
  - (e) the existence of the right to require the controller to correct or delete personal data or to restrict the processing of personal data relating to the data subject or the right to object to such processing;
  - (f) the right to lodge a complaint with the supervisory authority;
  - (g) if personal data are not collected from the data subject, any available information about their source;
  - (h) the existence of automated decision-making, including the profiling referred to in Article 23(1) and (4) and, at least in those cases, meaningful information on what logic it is, as well as the importance and anticipated consequences of such processing for the data subject.
2. If personal data are transferred to a third country or international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.
3. The controller shall provide a copy of the personal data to be processed. For any additional copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the data subject submits an application electronically and unless the data subject requests otherwise, the information shall be provided in the usual electronic form.

## **RIGHT TO CORRECTION**

### **Article 16**

The data subject has the right to obtain without undue delay from the controller the correction of inaccurate personal data relating to him. Taking into account the purposes of the processing, the data subject has the right to supplement incomplete personal data, including by making an additional statement.

## **RIGHT TO DELETE**

### **Article 17**

1. The data subject has the right to obtain from the controller the deletion of the personal data relating to him or her and the controller has the obligation to delete the personal data without undue delay if one is fulfilled of the following conditions:
  - (a) personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - (b) the data subject withdraws the consent on which the processing is based and if there is no other legal basis for processing;
  - (c) the data subject objects to the processing in accordance with Article 21. regulations, and there are no stronger legitimate grounds for processing, or the data subject objects to the processing in accordance with Article 21. Item 2;
  - (d) personal data are unlawfully processed;
  - (e) personal data must be deleted in order to comply with the legal obligation under the law of the Republic of Croatia;
2. If the controller has made public personal data and is obliged to delete that personal data in accordance with paragraph 1 of this Article, taking into account the available technology and the cost of implementation, the controller shall take reasonable measures, including technical measures, to inform the controllers processing the personal data that the data subject has asked those controllers to delete all links to them or the copy or reconstruction of that personal data.
3. Paragraphs 1 and 2 of this Article shall not apply to the extent that processing is necessary:
  - (a) in order to exercise the right to freedom of expression and information;
  - (b) in order to comply with a legal obligation requiring processing or to perform a public interest task or to exercise the official authority of the controller;
  - (c) due to the public interest in the field of public health in accordance with the provisions of the Regulation;
  - (d) for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes;
  - (e) to set up, exercise or defend legal claims.

## **RIGHT TO RESTRICT PROCESSING**

### **Article 18**

1. The data subject has the right to obtain a restriction of processing from the controller if one of the following is fulfilled:
  - (a) the data subject disputes the accuracy of the personal data, for a period allowing the controller to verify the accuracy of the personal data;
  - (b) processing is illegal and the data subject opposes the deletion of personal data and instead asks for a restriction on their use;
  - (c) the controller no longer needs personal data for processing purposes, but the data subject requests them for the purpose of setting up, exercising or defending legal claims;
  - (d) the data subject objected to the processing under Article 21. Item 1. The Regulations, expecting confirmation of whether the legitimate reasons of the controller go beyond the reasons of the data subject.
2. If the processing is restricted by paragraph 1 of this Article, such personal data may only be processed with the consent of the data subject, with the exception of storage, or for the establishment, exercise or defence of legal claims or the protection of the rights of another natural or legal person or due to the important public interest of the Republic of Croatia.
3. Data subject who obtained a processing restriction based on paragraph 1 of this Article, the controller report before the processing restriction is lifted.

### **Article 19**

The controller shall communicate any correction or deletion of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 of this Regulation to each recipient to whom personal data has been disclosed, unless this proves impossible or requires disproportionate effort. The controller shall inform the data subject of those recipients if the data subject so requests.

## **RIGHT TO DATA PORTABILITY**

### **Article 20**

1. The data subject has the right to receive personal data relating to him or her, which he has provided to the controller in a structured, commonly used and machine-readable format, and has the right to transfer that data to another controller without interference from the controller to whom the personal data have been provided, if:

- (a) processing is based on consent or contract;
  - (b) processing is carried out by automated means.
2. When exercising its data portability rights under paragraph 1, the data subject shall be entitled to a direct transfer from one controller to another where technically feasible. The law referred to in paragraph 1 of this Article shall not adversely affect the rights and freedoms of others.

## **RIGHT TO OBJECT**

### **Article 21**

1. The data subject has the right, on the basis of his particular situation, to object at all times to the processing of personal data if it is based on a task of public interest, on the exercise of the official powers of the controller or on the legitimate interests of the controller.

The controller may no longer process personal data unless the controller proves that there are compelling legitimate reasons for processing that go beyond the interests, rights and freedoms of the data subject or to make, exercise or defend legal claims.

2. If personal data are processed for direct marketing purposes, the data subject has the right at any time to object to the processing of personal data relating to him for the purposes of such marketing, which includes profiling to the extent related to such direct marketing.
3. If the data subject opposes processing for direct marketing purposes, personal data may no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the data subject must expressly draw attention to the right of objection referred to in paragraphs 1 and 2 of this Article and this must be done in a clear manner and separately from any other information.
5. If personal data are processed for scientific or historical research purposes or for statistical purposes in accordance with the provisions of the Regulation, the data subject has the right to object to the processing of personal data relating to him on the basis of his specific situation, unless the processing is necessary for the performance of the task performed for the reasons of the public interest.

## **FILING OF REQUESTS AND COMPLAINTS OF THE DATA SUBJECT**

### **Article 22**

All requests and objections provided for in the provisions of Articles 15-22 of this Regulation are submitted by the data subject to RBP, as the controller, in writing (recommended document confirming service) to the address:

**REVIEW BOOSTER PRO Ltd**, Dubrovnik, Liechtensteinov put 3, VAT ID: HR25407983967

or

e-mail to the e-mail address:

**info@reviewbooster.pro**

The RBP will act on the data subject's requests within 30 days from the date of the orderly receipt of the request.

The time limit referred to in the preceding paragraph may be extended by a further two months taking into account the complexity of the application.

If it is not able to act on the request, the RBP will inform the data subject.

If the Data Subject's requests are manifestly unfounded or excessive, and an overly frequent controller may refuse to act on such a request from the data subject or request prior payment of the conduct fee.

The compensation will be determined by the decision of the responsible person of the company.

If the controller has reasonable doubts as to the identity of the applicant, he or she may request additional information from the applicant in order to confirm the identity of the data subject.

In the event of a change in the RBPA contact details, the new information will be published on the official website ([www.reviewbooster.pro](http://www.reviewbooster.pro)) and/or the RBP bulletin board.

## **AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING**

### **Article 23**

1. The data subject has the right not to be affected by a decision based solely on automated processing, including profiling, which produces legal effects relating to him or her in a similarly significant manner.

2. Paragraph 1 shall not apply if the decision is:
  - (a) necessary for the conclusion or performance of the contract between the data subject and the data controller;
  - (b) permitted by the law of the Republic of Croatia to which the controller is subject and which also prescribes appropriate measures to protect rights and freedoms and legitimate interests of the data subject; or
  - (c) based on the explicit consent of the data subject.
3. In the cases referred to in paragraphs 2(a) and (c), the controller shall implement appropriate measures to protect the rights and freedoms and legitimate interests of the data subject, at least the right to human intervention of the controller, the right to express his or her own position and the right to challenge the decision.
4. The decisions referred to in paragraph 2 shall not be based on the specific categories of personal data referred to in Article 8(1), unless Article 8(2)(2) (a) or (g) applies and appropriate measures are in place to protect the rights and freedoms and legitimate interests of the data subject

## **CONTROLLER OBLIGATIONS**

### **Article 24**

1. Taking into account the nature, scope, context and purposes of the processing, as well as the risks of different levels of probability and severity for the rights and freedoms of individuals, the controller shall carry out appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is carried out in accordance with this Regulation and regulation. Those measures shall be reviewed and updated where appropriate.
2. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different levels of probability and severity for the rights and freedoms of individuals arising from the data processing, the controller, both at the time of determining the means of processing and at the time of the processing itself, shall carry out appropriate technical and organisational measures, to enable the effective application of the principles of data protection, such as reducing the amount of data, and the inclusion of safeguards in the processing in order to meet the requirements of the Regulations, the Regulation, the implementing law and to protect the rights of the data subject.
3. The controller, in accordance with the possibilities, implements appropriate technical and organizational measures to ensure that only the personal data necessary for each specific purpose of processing are processed in an integrated way. This obligation applies to the

amount of personal data collected, the extent of their processing, the storage period and their availability.

4. The controller may specify by a special general act the protocols, technical, physical and organizational security measures he takes in the application of this Article of the Regulations.

## **PROCESSOR**

### **Article 25**

In order to process the data subject's personal data, the controller may hire the Processor.

If the processing is carried out on behalf of the controller, the controller shall use only processors who sufficiently guarantee the implementation of appropriate technical and organizational measures in such a way that the processing complies with the requirements of this Regulation and ensures the protection of the data subject's rights.

## **RECORDS OF PROCESSING ACTIVITIES**

### **Article 26**

1. Each controller and the representative of the controller, if applicable, shall keep a record of the processing activities for which he is responsible.  
This record shall contain all of the following information:
  - (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representatives and the data protection officer;
  - (b) processing purposes;
  - (c) description of categories of respondents and categories of personal data;
  - (d) categories of recipients to whom personal data have been disclosed or will be disclosed, including recipients in third countries or international organisations;
  - (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 35(1) of the second subparagraph, documentation of appropriate safeguards;
  - (f) where possible, the foreseen deadlines for deleting different categories of data;
  - (g) where possible, the general description of the technical and organisational security measures referred to in Article 28(1) of the rulebook.



2. Each processor and the representative of the processor, where applicable, shall keep a record of all categories of processing activities carried out for the controller, which contains:
  - (a) the name and contact details of one or more processors and each controller on whose behalf the processor operates and, where applicable, the representatives of the controller or processor and the data protection officer;
  - (b) categories of processing carried out on behalf of each controller;
  - (c) where applicable, the transfer of personal data to a third country or international organisation, including the identification of that third country or international organisation and, where referred to in the Regulation, documentation on appropriate safeguards;
  - (d) where possible, a general description of the technical and organisational security measures referred to in Article 28(1).
3. The records referred to in paragraphs 1 and 2 must be in writing, including electronic form.
4. The controller or processor and the representative of the controller or processor, if applicable, shall, upon request, give the supervisory authority an insight into the records.
5. The obligations referred to in this Article shall not apply to an undertaking or organisation employing fewer than 250 persons, unless the processing it carries out is likely to cause a high risk to the rights and freedoms of the data subject, if the processing is not intermittent or the processing includes specific categories of data referred to in Article 8(1) or is personal data relating to criminal convictions and offences.

## **Article 27**

The controller and the processor and, where applicable, their representatives, shall cooperate with the supervisory authority upon request in fulfilling its tasks.

## **Article 28**

Taking into account the latest developments, implementation costs and the nature, scope, context and purposes of processing, as well as the risk of varying levels of probability and seriousness for the rights and freedoms of individuals, the controller and the processor shall carry out appropriate technical and organisational measures to ensure an adequate level of security with regard to the risk.

In particular, the assessment of the relevant level of security shall take into account the risks posed by the processing, in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data or unauthorised access to personal data transferred, stored or otherwise processed.

## **REPORTING TO THE SUPERVISORY AUTHORITY**

### **Article 29**

1. In the event of a personal data breach, the controller shall report, without undue delay and, where feasible, no later than 72 hours after learning of that infringement, the controller shall, in accordance with the Regulation, report the supervisory authority responsible for the infringement of personal data, unless it is unlikely that the personal data breach is likely to cause a risk to the rights and freedoms of individuals.
2. Without undue delay, the processor shall report, in accordance with the Regulation, to the controller after learning of the personal data breach.
3. The controller documents all personal data breaches, including the facts relating to the personal data breach, its consequences and the measures taken to repair the damage.

## **INFORMING THE DATA SUBJECT OF THE INFRINGEMENT**

### **Article 30**

1. In the event of a personal data breach that is likely to cause a high risk to the rights and freedoms of individuals, the controller shall inform the data subject of the personal data breach without undue delay.
2. The notification of the data subjects referred to in paragraph 1 of this Article describes the nature of the personal data breach using clear and plain language.
3. The notification of the data subject referred to in paragraph 1 is not mandatory if any of the following conditions are met:
  - (a) the controller has taken appropriate technical and organisational safeguards and these measures have been applied to personal data affected by the personal data breach, in particular those which render personal data incomprehensible to any person who is not authorised to access them;
  - (b) the controller has taken follow-up measures to ensure that there is no longer likely to be a high risk to the rights and freedoms of the data subjects referred to in paragraph 1;
  - (c) this would require a disproportionate effort. In such a case, there shall be public notification or a similar measure informing the data subjects in an equally effective manner.

## **DATA PROTECTION IMPACT ASSESSMENT**

### **Article 31**

1. Where it is likely that some type of processing, in particular through new technologies and taking into account the nature, scope, context and purposes of the processing, will cause a high risk to the rights and freedoms of individuals, the controller shall carry out an assessment before processing the impact of the envisaged processing operations on the protection of personal data, except in cases provided for in Art. 35th paragraph 10. Regulation. One assessment may relate to a number of similar processing operations that pose similarly high risks.
2. When conducting a data protection impact assessment, the controller seeks advice from the data protection officer, if he or she has been appointed.
3. The controller shall consult the supervisory authority before processing if the data protection impact assessment referred to in paragraph 1 of this Article shows that if the controller fails to adopt risk mitigation measures, the treatment would lead to a high risk.

## **DATA PROTECTION OFFICER**

### **Article 32**

The controller and the Processor may appoint a data protection officer in accordance with the provisions of the Data Protection Regulation.

If appointed, Respondents may contact the Data Protection Officer regarding any matters relating to the processing of their personal data and the exercise of their rights under this Regulation.

In the event of the appointment of a Data Protection Officer, RBP will publish the notification of it, as well as the contact details, on its website, and will notify the supervisory authority.

## **RIGHT TO COMPLAIN TO THE SUPERVISORY AUTHORITY**

### **Article 33**

Every data subject has the right to file a complaint with the supervisory authority, if the data subject considers that the processing of personal data relating to him violates some right protected by the

provisions of this Regulation, the Regulation and the Law on the Implementation of the General Regulation.

## **TRANSFER OF DATA TO A THIRD COUNTRY OR INTERNATIONAL ORGANIZATION**

### **Article 34**

The transfer of data to a third country or international organisation shall be permitted after, in accordance with the Regulation, an adequacy decision has established that it is an entity providing an adequate level of protection.

If no decision has been taken on the basis of the preceding paragraph, the controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided for appropriate safeguards and provided that enforceable rights and effective judicial protection are available to the data subjects.

The appropriate safeguards referred to in paragraph 2 may, without the need for any special authorisation from the supervisory authority, provide:

- (a) a legally binding and enforceable instrument between public authorities or public authorities;
- (b) binding corporate rules;
- (c) standard data protection clauses adopted by the Commission in accordance with the Regulation;
- (d) standard data protection clauses adopted by the supervisory authority and approved by the Commission in accordance with the Regulation;
- (e) approved code of conduct
- (f) approved certification mechanism

Provided that this is approved by the competent supervisory authority, the relevant safeguards referred to in paragraph 2 may, in particular, also provide:

- (a) contractual clauses between the controller or processor and the controller, processor or recipient of personal data in a third country or international organisation; or
- (b) provisions to be entered into administrative arrangements between public authorities or public authorities and containing the enforceable and effective rights of the data subject.

### **Article 35**

1. Where there is no adequacy decision in accordance with Article 34(1), or appropriate safeguards in accordance with Article 34.2 and 3, including binding corporate rules, the transfer or set of transfers of personal data to a third country or international organisation shall be achieved only under one of the following conditions:
  - (a) the data subject explicitly agreed to the proposed transfer after being informed of the potential risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
  - (b) the transfer is necessary for the performance of

- the contract between the data subject and the controller or for the implementation of pre-contractual measures at the request of the data subject;
- (b) transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
  - (c) transfer is necessary for important reasons of public interest;
  - (d) the transfer is necessary for the establishment, exercise or defence of legal claims;
  - (e) transfer is necessary to protect the vital interests of the data subject or other persons if the data subject is physically or legally unable to give consent;
  - (f) the transfer shall be made from a register which, under Union or Member State law, serves to provide information to the public and is open to the public or any person who may prove any legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for inspection in that particular case are met.

Where the transfer cannot be based on a provision referred to in Article 34 including the provisions of binding corporate rules, and where no derogation for the specific situations referred to in the first paragraph of this Article is applicable, the transfer to a third country or international organisation may take place only if the transfer is not repeated, if it concerns only a limited number of respondents, it is necessary for the purposes of the persuasive, legitimate interests of controllers who are not subordinate to the interests or rights and freedoms of the data subject, and the controller assessed all the circumstances of the data transfer and, on the basis of that assessment, provided for appropriate safeguards regarding the protection of personal data.

The controller shall inform the supervisory authority of this transfer. In addition to providing the information referred to in Articles 13 and 14, the controller shall inform the data subject of the transfer and of compelling legitimate interests.

## **EMPLOYEE OBLIGATIONS**

### **Article 36**

When processing personal data, employees of RBP Ltd are obliged to be guided by the principles of confidentiality and security in the management of the same data. Employees will process personal data in accordance with the provisions of this Regulation and according to the instructions of the Employer. The data will be used exclusively for the purposes for which the processing is provided, and will not be made available to persons who do not have the power to do so.

## **CONCLUDING PROVISIONS**

### **Article 37**

The rights and obligations under and under this Regulation will be realized, where appropriate, by making special statements/contracts/annexes with clients, employees or third parties concerned by this Regulation.

In the case where specific declarations/contracts have not been concluded, and in cases which are not regulated by the same separate legal documents, the provisions of this Regulation and regulation will apply directly to the provisions of this Regulation and regulation.

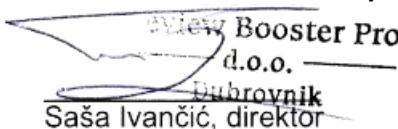
### **Article 38**

This Regulation shall enter into force on the eighth day following the date of its publication on the notice board.

### **Article 39**

This Regulation is amended and supplemented in the manner prescribed for its adoption.

**REVIEW BOOSTER PRO Ltd by company director**

  
Review Booster Pro  
d.o.o.  
Dubrovnik  
Saša Ivancić, direktor

Zagreb, March 1<sup>st</sup> 2022

**Annex 1.** – Refers to the processing of personal data of employees (including on the basis of employment contracts and copyright contracts, student contracts, and the process of recruiting/recruiting candidates)

PERSONAL INFORMATION	PROCESSING PURPOSE	LEGAL BASIS OF PROCESSING	CATECHTORIAS OF DATA RECIPIENTS / THIRD PARTIES	DATA USAGE PERIOD
<ul style="list-style-type: none"> <li>Name and surname</li> <li>Date of birth</li> <li>OIB</li> <li>Address, Place and country of residence</li> <li>Biography</li> <li>Photograph</li> <li>Copy of ID card</li> <li>Information about the parent (father or mother)</li> <li>Data on education and professional training</li> <li>Account number/IBAN</li> <li>Citizenship</li> <li>Birth certificate</li> <li>Birth certificate of children</li> <li>Tax card</li> <li>Seniority data</li> <li>Health data</li> <li>Income data</li> <li>Signature</li> <li>Scholarship data (student contracts only)</li> </ul>	<p>Rights and obligations from the employment relationship, and the legal obligations of the employer to third parties. Establishing an employment relationship (concluding a contract, applying to HZMO and HZZO, etc.), issuing certificates, e.g. (enrollment of children in kindergarten), payment of salary, implementation of occupational safety, and obligations of the employer from other legal regulations. Health data are processed for limited purposes related to legal obligations and the exercise of the rights and obligations provided for in health and social care systems.</p>	<p>Legal (Pension Insurance Act, Labour Act, Occupational Safety and Health Act, etc.)</p>	<p>National Bureau of Statistics - salary reports, etc.</p> <p>Croatian Pension Insurance Institute</p> <p>Croatian Health Insurance Institute</p> <p>Tax Administration-JOPPD forms-reports on payments made, income payments. For the payment of income (salaries, tax-free payments and fees) of employees</p> <p>For the payment of income (fees) of other staff (authors)</p> <p>For the payment of income (scholarships) of students.</p> <p>Banks</p> <p>Credit card companies</p> <p>Other competent authorities</p>	<p>Permanently, for the duration of the employment relationship, and in the case of reasonable grounds and obligations and after the expiry of the data regularly.</p>
<ul style="list-style-type: none"> <li>First and last name</li> <li>Date of birth</li> <li>OIB</li> <li>Contact details</li> <li>Place and country of birth</li> <li>Address, Place and country of residence</li> <li>Biography</li> <li>Photograph</li> <li>Data on education and professional training</li> <li>Home certificate / citizenship</li> <li>Seniority data</li> <li>Health data</li> <li>Signature</li> <li>Email</li> <li>Scholarship data (student contracts only)</li> </ul>	<p>The process of recruiting/recruiting candidates.</p>	<p>Contract-condition for concluding the contract.</p> <p>Legitimate interest-when carrying out the recruitment process, it is necessary to collect the personal data of candidates</p>	<p>Employment agencies</p>	<p>For the duration of the procedure, up to max. 2 years in case of registering candidates in the database of potential employees.</p>
<ul style="list-style-type: none"> <li>First and last name</li> <li>Date of birth</li> <li>OIB</li> <li>Place and country of birth</li> <li>Address, Place and country of residence</li> <li>Biography</li> <li>Photograph</li> <li>Data on education and professional training</li> <li>Account number/IBAN</li> <li>Home certificate/citizenship</li> <li>Birth certificate</li> </ul>	<p>Rights and obligations from the employment relationship. The purpose includes the rights and obligations under employment contracts, additional contracts on the basis of employment, and general acts of the employer. Health data are processed for limited purposes related to legal obligations and the exercise of the rights and obligations provided for in health and social care systems. The processing of this data is necessary for the</p>	<p>Contract</p>	<p>Competent public authorities, judicial authorities, Legal representatives of RBP, Accounting Audit firms</p>	<p>Permanently, for the duration of the employment relationship, and in the case of reasonable grounds and obligations and after the expiry of the data regularly.</p>

<ul style="list-style-type: none"> <li>• Birth certificate of children</li> <li>• Tax card</li> </ul>	establishment of an employment relationship.			
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• Email</li> <li>• Phone number</li> <li>• Mobile number</li> </ul>	Communication within RBP Communication with business partners, clients, etc.	1. Contract - condition for concluding the contract.  2. Legitimate interest of the employer (necessity with the performance of the economic activity of the company)	Business partners, clients, etc.	During the employment relationship, and in the case of reasonable grounds and obligations and after the expiry of the data with regular updating of the data.
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• Email</li> <li>• Phone number</li> <li>• Mobile number</li> </ul>	Using web platforms for business communication	Contract	Business partners, clients, etc. For the duration of the employment relationship	For the duration of the employment relationship
<ul style="list-style-type: none"> <li>• Biometric data</li> </ul>	Insurance of the protection of property, persons, trade secrets.	Legitimate interest of the employer (creating a safe environment, securing business)	If necessary, external companies providing complementary services	For the duration of the employment relationship, if necessary and longer for justified purposes.
<ul style="list-style-type: none"> <li>• Personal data collected through video surveillance</li> </ul>	Protection of property and persons, security of security.	Legitimate interest of the employer If video surveillance of the working premises is carried out, the RBP will inform the employees about it.	If necessary, competent judicial authorities, law firms, etc.	Max. 6 months, except in legally permitted exceptions
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• Email</li> <li>• Phone number</li> <li>• Photograph</li> <li>• Video footage</li> </ul>	Publication on the website, presentation materials of RBP to inform about products, way of doing business, advice to clients, etc.	1. Contract 2. The legitimate interest of the employer (e.g. it is the interest of the employer to allow interested persons to see the data on RBP employees as part of, presentations of the company, etc.)	Website visitors, addressees of materials, etc.	During the duration of the employment relationship, and in the case of reasonable grounds and obligations and after the expiry of the data with regular updating of the data.
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• Photograph</li> <li>• Video footage</li> <li>• Email</li> </ul>	Marketing and promotional activities	1. Contract 2. The legitimate interest of the employer (it is the interest of the employer to enable the publication of certain content for the purpose of promoting RBP)	Event organizers, Publicity Agencies, Media, Social Networks, Brochures, etc.	Occasionally, according to activities
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• OIB</li> <li>• Email</li> <li>• Security info to access the user account</li> <li>• Mobile number</li> <li>• Phone number</li> <li>• Photograph</li> </ul>	Opening, protecting and maintaining an e-mail account, borrowing and deleveraging of equipment	Contract	System operators, where appropriate external companies providing maintenance of ICT systems	During employment
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• OIB</li> <li>• Email</li> </ul>	Preventing unauthorised access to electronic communications networks	Contract	System operators, where appropriate external companies providing	During the employment relationship,



<ul style="list-style-type: none"> <li>Security information to access the user account and other systems</li> <li>Mobile number</li> <li>Phone number</li> </ul>	and the spread of malicious codes, stopping attacks, preventing damage to computer and electronic communication systems, ensuring network capabilities and ICT systems	Legitimate interest of the employer (protection of the ICT system)	maintenance of ICT systems	and in the case of reasonable grounds and obligations and after the expiry of the data with regular updating of the data.
<ul style="list-style-type: none"> <li>First and last name</li> <li>OIB</li> <li>Email</li> <li>Security data to access the user's account, computer and other communication systems</li> </ul>	Supervision of business e-mail and other communication of employees in exceptional case of suspicion of possible unauthorized data transfer, disclosure of trade secrets, violation of obligations from employment relationships, mobbing, etc.	Legitimate interest of the employer (consists in preventing damage, protecting the business)	Judicial authorities, lawyers, etc.	During the employment relationship, and in the case of legal proceedings and after the expiry of the
<ul style="list-style-type: none"> <li>First and last name</li> <li>Date of birth</li> <li>OIB</li> <li>Place and country of birth</li> <li>Place and country of residence/residence</li> <li>Information about the parent (name and surname of the father or mother)</li> <li>Signature</li> </ul>	Disciplinary and other legal proceedings in accordance with the general acts of RBP	Contract	Judicial authorities, lawyers, etc.	For the duration of the procedures, archiving if necessary
<ul style="list-style-type: none"> <li>First and last name</li> <li>Address</li> <li>OIB</li> <li>Security data to access the user's account, computer and other communication systems</li> <li>Email</li> <li>Phone number</li> <li>Mobile number</li> </ul>	Performance of the contract from the company's business	Contract Legitimate interest of the employer (it is necessary to process personal data in the execution of business from the economic activity of the company, and to provide it to business partners, customers, etc.	Customers, Business Partners, third parties related to the business process.	Limited depending on the nature of the contract

**Annex 2.** – Refers to the processing of personal data of customers, suppliers and business partners of RBP

<b>PERSONAL INFORMATION</b> (The personal data provided herein will be processed in accordance with the intended purposes)	<b>PROCESSING PURPOSES</b>	<b>LEGAL BASIS OF PROCESSING</b>	<b>TRANSFER OF DATA TO THIRD PARTIES</b>	<b>DATA USAGE PERIOD</b>
<ul style="list-style-type: none"> <li>First and last name</li> <li>Email</li> <li>Address</li> <li>Phone number</li> <li>IBAN</li> </ul>	Conclusion and execution of contracts for the sale of goods and other business contracts, and the subsequent exercise of the right to warranty and complaint, or for the return of funds to the account	Contract	1.Bank 2.Delivery services 3. Equipment manufacturers (related to the use of the warranty) 4.Credit card companies 5.Bookkeeping 6.Audit firms	PERMANENTLY, in accordance with the legal framework
<ul style="list-style-type: none"> <li>Email</li> </ul>	Resolving requests from complaints, communication with customers	Contract	Equipment manufacturers (related to the use of the warranty)	PERMANENTLY

<ul style="list-style-type: none"> <li>• Adress</li> <li>• Broj Mobitela</li> <li>• Broj Telefona</li> </ul>	Delivery of goods of it is contracted	Contract - a condition for the fulfilment of the contract if service is requested	Delivery services	Until the service is performed
<ul style="list-style-type: none"> <li>• Personal data collected through video surveillance</li> </ul>	Protection of property and persons	Legitimate interest (asset protection, ensuring safety for buyers and employees)	If necessary, competent judicial authorities, law firms, etc.	Max. 6 months, except in legally permitted exceptions
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• OIB</li> <li>• IBAN</li> <li>• Date of birth</li> <li>• Place and country of birth</li> <li>• Place and country of residence</li> <li>• Payment information and other terms of the contract</li> </ul>	Processing of data for the purposes of judicial, administrative and other judicial proceedings	Legitimate interest in non-compliance with the contract	Courts, administrative bodies, legal representatives and other related judicial bodies	Where appropriate, in the case of initiation of judicial, administrative proceedings
<ul style="list-style-type: none"> <li>• First and last name</li> <li>• Email</li> <li>• Address</li> <li>• Phone number</li> </ul>	Delivery of notices to customers about new products and benefits (newsletter, telephone notification, etc.)	Legitimate interest- since customers have done business with the company, it is the business interest to inform them about new products and benefits		Permanently, unless the customer informs the company that he no longer wishes to receive notifications
<ul style="list-style-type: none"> <li>• First and last name / Name</li> <li>• OIB</li> <li>• Registration number</li> <li>• IBAN</li> <li>• Address, Location and Country</li> <li>• Email</li> <li>• Phone number</li> <li>• Mobile number</li> </ul>	Communication with business partners and clients of the company Issuance and receipt of inquiries, quotes, outbound and inbound documents	1.Contract 2.Legitimate business interest	Banks Tax administration, other competent authorities	For the duration of the business relationships, and in the case of reasonable grounds and obligations and after the expiry of the data with regular updating of the data.