



EASYPROMOS DATA PROCESSING AGREEMENT

PARTIES

This Data Processing Agreement is entered into between:

The Customer, identified in its Easypromos account, sign-up form, order form or applicable commercial agreement, hereinafter referred to as the **CONTROLLER**.

And

EASYPROMOS, S.L., a company with registered address at C/ Bonastruc de Porta 20, 17001 Girona, Spain, and Spanish tax identification number B-65576878, hereinafter referred to as the **PROCESSOR**.

The CONTROLLER and the PROCESSOR are collectively referred to as the **Parties**.

This Agreement will enter into force on the date on which the CONTROLLER accepts the [Easypromos Terms and Conditions of Use](#), which incorporate this Agreement by reference. When executed by separate signature, it will enter into force on the date of the last signature.

BACKGROUND

I. The PROCESSOR provides a platform for creating and managing digital campaigns and promotions, including social media campaigns.

II. The use of the services may involve the PROCESSOR accessing and processing, on behalf of the CONTROLLER, certain personal data for which the CONTROLLER acts as data controller, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation.

III. When the CONTROLLER uses the services on behalf of a third party and itself acts as a processor, EASYPROMOS will act as a subprocessor. In this case, references to the CONTROLLER in this Agreement will refer to the entity that engages and instructs EASYPROMOS, which represents that it has obtained the necessary authorization from the relevant data controller to appoint EASYPROMOS as a subprocessor.

Accordingly, the Parties agree that the processing of personal data will be governed by the following clauses.



CLAUSES

1. Purpose of the Agreement

1.1 The purpose of this Agreement is to govern the processing of personal data carried out by the PROCESSOR on behalf of the CONTROLLER in order to provide the contracted services for the creation and management of digital promotions.

The processing of data by the PROCESSOR does not constitute a transfer or disclosure of personal data. The CONTROLLER determines the purposes of the processing and is responsible for its lawfulness.

2. Term

2.1 This Agreement will remain in force for as long as the CONTROLLER's Easypromos account remains active or a services agreement between the Parties remains in effect.

3. Processing of Personal Data

3.1 The PROCESSOR is authorized to process, on behalf of the CONTROLLER, the personal data required to provide the contracted services.

3.2 Categories of personal data

The PROCESSOR may process the following categories of personal data:

- (i) Identification and contact data, such as first and last name, identity document, postal address, email address, telephone number or image.
- (ii) Personal characteristics, such as date of birth, age, sex, nationality or family information.
- (iii) Data relating to participation, browsing and use of the promotions.
- (iv) Other data that the CONTROLLER chooses to request or include through the configuration of the promotions, provided that such data is necessary for the purposes of the contracted features or services.

The CONTROLLER will not include special categories of personal data as defined in Article 9 of the GDPR, or personal data relating to criminal convictions and offences under Article 10, unless expressly agreed in advance in writing with the PROCESSOR.

3.3 Nature and purpose of the processing

The processing will include the collection, storage, consultation, use, disclosure to authorized subprocessors, export and deletion of personal data, to the extent necessary to provide the services and follow the CONTROLLER's documented instructions.



3.4 Categories of data subjects

The personal data processed may relate to:

- (i) Participants, consumers or users of the CONTROLLER.
- (ii) Employees of the CONTROLLER when they participate in promotions organized or managed by the CONTROLLER.

4. Data Retention

4.1 Retention period by licence type

As a general rule, the retention period applicable to the personal data governed by this Clause is five years. Customers with a Corporate licence may select a retention period of two, three, four or five years.

4.2 Applicable retention periods by category

Category of personal data	Retention period and automatic deletion
Promotion participants and entries	Five years from the end or cancellation of the promotion. For accounts with a Corporate licence, the retention period of two, three, four or five years selected by the CONTROLLER will apply.
Users imported into draws	For completed draws, 90 days from execution. For draws that have not been completed, 90 days from creation.
Draw winners and alternates	Five years from the execution of the draw. For accounts with a Corporate licence, the retention period of two, three, four or five years selected by the CONTROLLER will apply.
Users of Instagram automations	Five years from the date the automation is paused. For accounts with a Corporate licence, the retention period of two, three, four or five years selected by the CONTROLLER will apply.

4.3 Deletion before expiry of the retention period

The CONTROLLER may delete personal data before the retention periods set out in this Clause expire by using the deletion options available for each service on the platform.



5. Processor Obligations

The PROCESSOR and all its personnel agree to:

5.1 Comply with the obligations set out in 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, repealing Directive 95/46/EC, the General Data Protection Regulation, in accordance with this Agreement.

5.2 Process personal data solely to provide the contracted services and in accordance with the CONTROLLER's documented instructions.

5.3 Not use personal data for purposes other than those set out in this Agreement.

5.4 Inform the CONTROLLER if it considers that an instruction infringes applicable data protection law. The PROCESSOR may suspend the instruction until the CONTROLLER modifies or withdraws it.

5.5 Ensure that persons authorized to process personal data are bound by confidentiality obligations and access the data only where required to perform their duties.

5.6 Not disclose personal data to third parties except on the CONTROLLER's instructions, where required by law, or through authorized subprocessors in accordance with Clause 12.

5.7 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, where applicable:

(i) The pseudonymization and encryption of personal data.

(ii) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

(iii) The ability to restore the availability of and access to personal data following a physical or technical incident.

(iv) Regular testing and assessment of the effectiveness of the technical and organizational measures implemented.

5.8 Assist the CONTROLLER in responding to requests from data subjects exercising their rights. If the PROCESSOR receives a request directly, it will forward it to the CONTROLLER by email without undue delay, together with any relevant information available, and will not respond unless instructed to do so.

5.9 Provide reasonable assistance to the CONTROLLER with its obligations relating to processing security, data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the processing and the information available.

5.10 Notify personal data breaches in accordance with Clause 7.

5.11 Provide the information required to demonstrate compliance with its obligations and allow



audits under the terms set out in Clause 10.

5.12 Appoint subprocessors in accordance with Clause 12.

5.13 Inform the CONTROLLER in advance where the PROCESSOR is required under European Union or Member State law to transfer personal data to a third country or international organization, unless that law prohibits such information on important grounds of public interest.

5.14 Assistance provided through the platform's standard features and available documentation is included in the contracted services. The PROCESSOR may charge for additional assistance requiring significant additional resources, subject to prior notice to the CONTROLLER, unless that assistance is required as a result of a breach attributable to the PROCESSOR.

5.15 The PROCESSOR adheres to the applicable privacy principles established in ISO/IEC 29100, in accordance with the personal data protection framework established in ISO/IEC 27018.

6. Controller Obligations

The CONTROLLER is responsible for:

6.1 Complying with its obligations under the GDPR and ensuring the lawfulness of the processing, including having a valid legal basis and providing the required information to data subjects.

6.2 Ensuring that the personal data and instructions provided to the PROCESSOR are adequate, relevant, accurate and compliant with applicable law.

6.3 Implementing the necessary security measures within its own systems and protecting the accounts, credentials and access of its authorized platform users.

6.4 Responding to requests from data subjects exercising their rights and informing the PROCESSOR of any rectification, deletion or restriction that must be applied to the processed data.

7. Personal Data Breach Notification and Impact Assessments

7.1 Personal data breach notification

The PROCESSOR will notify the CONTROLLER by email and without undue delay of any personal data breach affecting personal data processed on the CONTROLLER's behalf once the PROCESSOR becomes aware of it.

Functional errors, technical incidents, unexploited vulnerabilities, blocked access attempts and other events that have not resulted in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data will not be considered personal data



breaches.

Where available, the notification will include:

- (i) A description of the nature of the breach, including, where possible, the categories and approximate number of affected data subjects and personal data records.
- (ii) Contact details for the point of contact from whom further information may be obtained.
- (iii) A description of the likely consequences of the breach.
- (iv) A description of the measures taken or proposed to address the breach and mitigate its possible adverse effects.

Where it is not possible to provide all the information at the same time, the information will be provided in phases without undue delay.

The CONTROLLER is responsible for assessing the risk and determining whether the breach must be reported to the supervisory authority or communicated to the data subjects. Notification to the supervisory authority is not required where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

7.2 Data protection impact assessments

Where applicable, the PROCESSOR will provide reasonable assistance to the CONTROLLER with data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the processing and the information available.

8. Return and Deletion of Data Following Termination

8.1 Before permanently closing its account, the CONTROLLER may export the personal data using the tools provided by the PROCESSOR or request its export. Permanent closure of the account will result in the deletion of the personal data stored in the PROCESSOR's active systems.

8.2 When personal data is deleted by the CONTROLLER, following permanent closure of the account or upon expiry of the retention periods set out in Clause 4, it will be deleted from the PROCESSOR's active systems. Residual copies held in backup systems will be deleted through the ordinary backup rotation cycle within a maximum of 60 days from deletion from the active systems. During this period, the data will not be available for ordinary processing and may only be restored where necessary to recover the systems.

9. Liability

9.1 Each party is responsible for complying with its respective obligations under this Agreement and applicable data protection law.

9.2 The PROCESSOR's total aggregate liability arising from this Agreement, including



damages, indemnities and any reimbursement of fines imposed on the CONTROLLER, will not exceed the fees paid by the CONTROLLER for the contracted service during the twelve months preceding the event giving rise to the claim.

9.3 The PROCESSOR will not be liable for indirect damages, loss of profits, revenue, business, opportunities or reputation, or for claims arising from the CONTROLLER's instructions, data, configurations, actions or omissions.

9.4 The limit set out in Clause 9.2 and the exclusion of indirect damages in Clause 9.3 will not apply where the damage was caused by the PROCESSOR's willful misconduct. Willful misconduct means conduct undertaken deliberately and with knowledge that it breaches the obligations applicable to the PROCESSOR.

9.5 If either party becomes involved in an investigation, administrative proceeding or claim relating to the processing covered by this Agreement, it will inform the other party where the matter may affect that party's rights or obligations.

9.6 The limitations in this Clause govern contractual liability only as between the CONTROLLER and the PROCESSOR. They do not bind supervisory authorities or limit the rights granted to data subjects under the GDPR.

10. Compliance and Audits

10.1 The PROCESSOR will make available to the CONTROLLER the information reasonably necessary to demonstrate compliance with the obligations set out in this Agreement. Where certifications, audit reports or other documentation provided sufficiently demonstrate compliance, they will be considered appropriate evidence.

Where an additional audit is required, the CONTROLLER may conduct it no more than once per year, with at least 30 days' prior notice, during business hours and at its own expense. The audit must be carried out by qualified personnel subject to confidentiality obligations and must not disrupt the services or allow access to other customers' data, trade secrets or information that could compromise system security.

The frequency and notice limitations do not apply where the audit is required by a competent supervisory authority or where there are reasonable grounds to suspect a material breach of this Agreement by the PROCESSOR.

11. Confidentiality

11.1 The parties will keep confidential the information received in connection with this Agreement and may use it only to provide or receive the contracted services.

Confidential information may be disclosed to personnel, advisers and subprocessors who need to know it to perform this Agreement, provided they are bound by confidentiality obligations.

11.2 The PROCESSOR will implement the measures necessary to preserve the confidentiality



of the personal data processed and will ensure that persons authorized to access it respect that confidentiality.

The confidentiality obligations will continue after termination of the Agreement for as long as the information remains confidential. The confidentiality obligation relating to personal data will continue indefinitely.

11.3 The obligations above do not apply to information that:

- (i) Is in the public domain other than as a result of a breach of this Agreement.
- (ii) Was lawfully obtained from a third party not subject to a confidentiality obligation.
- (iii) Was already known to the receiving party.
- (iv) Was independently developed by the receiving party.
- (v) Must be disclosed by law or at the request of a competent authority.

12. Subprocessors

12.1 The CONTROLLER authorizes the PROCESSOR to appoint the subprocessors necessary to provide the services. The subprocessors in place on the effective date of this Agreement are identified in the Annex, EasyPromos List of Subprocessors.

12.2 The PROCESSOR will notify the CONTROLLER of the appointment or replacement of subprocessors at least ten calendar days in advance. The CONTROLLER may object within that period on legitimate grounds relating to the protection of personal data. In the event of an objection, the Parties will cooperate in good faith to seek a commercially and technically reasonable solution. If no solution is possible and the subprocessor is necessary, either Party may terminate the affected services or, where they cannot be separated from the remaining services, all services.

12.3 The PROCESSOR will contractually require its subprocessors to comply with data protection obligations equivalent to those set out in this Agreement and will remain responsible for their compliance to the extent required by applicable law. Where the processing involves an international transfer of personal data, the PROCESSOR will apply a valid mechanism under applicable law.

13. Breach and Termination

13.1 If the CONTROLLER breaches any obligation set out above, the PROCESSOR may terminate this Agreement by notifying the CONTROLLER of its decision. If the PROCESSOR breaches any of its obligations, the CONTROLLER may likewise terminate the Agreement by notifying the PROCESSOR of its decision.



14. Governing Law, Jurisdiction and Severability

14.1 This Agreement will be governed by Spanish law. Any dispute relating to its validity, interpretation, performance or enforcement will be submitted to the courts of Girona, Spain, unless mandatory law provides for another jurisdiction.

14.2 If any provision of this Agreement is held to be invalid, unlawful or unenforceable, the validity, lawfulness and enforceability of the remaining provisions will not be affected. This Agreement will be interpreted in good faith and according to the ordinary meaning of its wording.



EXECUTION BY SEPARATE SIGNATURE

This section will be used only when the Parties decide to execute this Agreement by separate signature. The Agreement may be signed electronically and in counterparts, each of which will be deemed an original and all of which together will constitute one agreement.

THE CONTROLLER	THE PROCESSOR
Legal name:	Legal name: Easypromos, S.L.
Tax identification number:	Spanish tax identification number: B-65576878
Represented by: Name:	Represented by: Name:
Title:	Title:
Date of signature:	Date of signature:
Signature:	Signature:



Annex: List of Subprocessors

To provide the EasyPromos service, we work with a number of service providers. Depending on the services they provide, some may have access to promotion participants' personal data.

The organizer of the promotion is the controller of participants' personal data. When the organizer uses the EasyPromos platform, EasyPromos acts as processor. As a processor, we are committed to complying with the obligations set out in 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 the free movement of such data, repealing Directive 95/46/EC, the General Data Protection Regulation.

Our providers that have access to participants' personal data therefore act as subprocessors. This Annex identifies these providers and describes the services they provide, the participant data they may access, where the data is hosted, and the safeguards and security standards they apply.

1. Google Ireland Limited (Google)

- **Company location:** Dublin, Ireland
- **Service:** Hosting of the EasyPromos infrastructure through Google Cloud Platform.
- **Is the service optional?** No. It is required for the platform to operate.
- **Data location:** Google data center in Belgium, Europe.
- **Data accessed:** All promotion participant data is hosted in this data center.
- **Security:** Compliance with multiple security standards. Further information: <https://cloud.google.com/security/compliance/>
- **Contractual safeguards:** Yes. Google may use the data only to provide the relevant services as a subprocessor, as set out in the Google Cloud Platform terms.

2. Ackstorm SL

- **Company location:** Barcelona, Spain
- **Service:** Maintenance, monitoring and security audits of the EasyPromos infrastructure hosted on Google Cloud Platform.
- **Is the service optional?** No. It is required for the platform to operate and for its proper maintenance and monitoring.
- **Data location:** The Ackstorm team operates from its offices in Barcelona, Spain. Due to the nature of the contracted services, it may have access to any data hosted on the platform.
- **Data accessed:** All promotion participant data.
- **Security:** ISO 27001 certification.
- **Contractual safeguards:** Yes. Ackstorm may use the data only to provide the relevant services as a subprocessor, as set out in the data processing agreement between the parties.

3. The Rocket Science Group, LLC (Mailchimp)

- **Company location:** Nevada, United States



- **Parent company:** Mailchimp is part of the Intuit group of companies (<https://www.intuit.com/>)
- **Service:** Transactional email delivery. EasyPromos provides an email platform that allows promotion organizers to configure automated emails to participants, such as participation confirmations, prize information and participation validation messages.
- **Is the service optional?** Yes. It is an optional feature, and customers can run a promotion without using the email platform.
- **Data location:** United States
- **Data accessed:** Promotion participants' email addresses.
- **Security:** SOC 2 report and ISO 27001 certification.
- **Contractual safeguards:** Mailchimp may process the data only to provide the relevant services as a subprocessor, in accordance with the applicable data processing terms entered into by the parties.
- **International data transfers from the EU:** The United States is recognized as providing an adequate level of protection for organizations participating in the EU-U.S. Data Privacy Framework. The subprocessor participates in the Framework: <https://www.dataprivacyframework.gov/list>
 - Search for Intuit or The Rocket Science Group, LLC

4. Vimeo, Inc. (Vimeo)

- **Company location:** New York, United States
- **Service:** Video hosting for video contests through the Video Hosting extension. EasyPromos allows organizers to create video contests in which participants upload their own video files. This provider hosts and streams those videos.
- **Is the service optional?** Yes. It is an optional feature for video contests.
- **Data location:** United States
- **Data accessed:** Videos uploaded by participants in video contests.
- **Security:** SOC 2 Type 2 report.
- **Contractual safeguards:** Vimeo may process the data only to provide the relevant services as a subprocessor, in accordance with the applicable data processing terms entered into by the parties.
- **International data transfers from the EU:** The United States is recognized as providing an adequate level of protection for organizations participating in the EU-U.S. Data Privacy Framework. The subprocessor participates in the Framework: <https://www.dataprivacyframework.gov/list>
 - Search for Vimeo

5. OpenAI Ireland Limited

- **Company location:** Dublin, Ireland
- **Service:** Artificial intelligence services for optional platform features, including purchase receipt validation and the generation or translation of promotion content.
- **Is the service optional?** Yes. It is an optional feature. The promotion organizer may choose whether to enable automated receipt validation using artificial intelligence.
- **Data location:** United States, with possible processing in other regions depending on the provider's infrastructure.



- **Data accessed:** Data contained in purchase receipts and information that the customer includes in fields, instructions or content submitted to artificial intelligence features.
- **Security:** OpenAI applies appropriate technical and organizational security measures, including encryption in transit and at rest, access controls and compliance with industry standards. Further information is available at <https://openai.com/security>. OpenAI does not use data submitted through the API to train its models and does not retain it longer than necessary to provide the service, in accordance with its enterprise policies.
- **Contractual safeguards:** Yes. OpenAI acts as a subprocessor and may process the data only to provide the contracted service, in accordance with the Data Processing Addendum entered into by the parties.
- **International data transfers from the EU:** Processing may involve international transfers outside the European Economic Area. OpenAI uses appropriate legal transfer mechanisms, including Standard Contractual Clauses. Further information is available at <https://openai.com/policies/privacy-policy>

6. Aruba S.p.A. (Aruba)

- **Company location:** Bergamo, Italy
- **Service:** Data hosting and mirroring in Italy for promotions subject to Italian data localization requirements.
- **Is the service optional?** Yes. It is an optional feature required only for promotions subject to Italian data localization requirements.
- **Data location:** Aruba data center in Milan, Italy.
- **Data accessed:** Any participant data relating to promotions in Italy.
- **Security:** Compliance with multiple security standards. Further information: <https://www.arubacloud.com/infrastructures/italy-global-cloud-data-center-it3.aspx>
- **Contractual safeguards:** Yes. Aruba may use the data only to provide the relevant services as a subprocessor, as set out in Aruba's terms and conditions.

7. Zendesk, Inc. (Zendesk)

- **Company location:** California, United States.
- **Service:** Platform used to manage enquiries, communications and tickets for the EasyPromos support service.
- **Is the service optional?** Yes. It is used when the user contacts the support service.
- **Data location:** United States.
- **Data accessed:** Contact details, communications, attachments and technical information provided during support. Zendesk may incidentally access participant data when a customer includes such data in a support enquiry.
- **Security:** ISO 27001 and ISO 27018 certifications and SOC 2 Type II report, with encryption of data in transit and at rest.
- **Contractual safeguards:** Yes. Zendesk may process the data only to provide the contracted service, in accordance with its DPA.
- **International data transfers from the EU:** Zendesk applies recognized mechanisms, including its Binding Corporate Rules, the EU-U.S. Data Privacy Framework and the Standard Contractual Clauses. Where Zendesk acts as a subprocessor, Module 3 of the Standard Contractual Clauses applies.



8. eesel, Inc. (eesel AI)

- **Company location:** Delaware, United States.
- **Service:** Artificial intelligence platform used for the chatbot and automated assistance within the Easypromos support service.
- Is the service optional? Yes. It is used when the user interacts with the chatbot.
- **Data location:** United States.
- **Data accessed:** Support communications, technical information and content provided by the user. eesel may incidentally access participant data when a customer includes such data in a support enquiry.
- **Security:** Encryption of data in transit and at rest and access controls. SOC 2 Type II audit in progress.
- **Contractual safeguards:** Yes. eesel may process the data only to provide the contracted service and may not use it to train or improve general or shared artificial intelligence models. Data is deleted within a maximum of 30 days following termination of the service.
- **International data transfers from the EU:** Transfers to the United States are based on the Standard Contractual Clauses approved by the European Commission.