

BigArena Data Processing Agreement (DPA)

Version 1.0 of 27 October 2026. Article 28 of Regulation (EU) 2016/679 (“GDPR”).

Parties and acceptance

This Data Processing Agreement (“DPA”) is concluded between:

(1) the client who uses the BigArena services under the BigArena Terms of Service (<https://bigarena.net/en/terms-and-conditions>) or under a fulfilment contract with BigArena (the “**Controller**”); and

(2) the BigArena company that provides the services to the Controller (the “**Processor**”):

- for clients of Бигарена ООД (BIGARENA LTD), UIC 204072747, registered office Golyamokonarsko Shose 29B, 4204 Plovdiv, Bulgaria: Бигарена ООД;
- for clients of Bigarena Fulfillment Europe s.r.o., IČO 54 736 374, registered office Seredská 4084/30, 917 05 Trnava, Slovakia: Bigarena Fulfillment Europe s.r.o.;
- for clients that have a contract with a BigArena company in Romania, Greece or Serbia: that company.

The Terms of Service, the fulfilment contract and the related offers and policies are together the “**Services Agreement**”. This DPA forms part of the Services Agreement (Terms of Service, clause 3.4).

The Controller accepts this DPA in electronic form under Article 28(9) GDPR by accepting the Terms of Service or by signing a contract or addendum that refers to it. For Controllers with a fulfilment contract, this DPA sets out in detail the processing under that contract and supplements its data protection provisions, under which the Controller has confirmed that it is the controller of the personal data and has informed its customers that their data is provided to the Processor and its subcontractors for delivery. On request the Processor provides a dated PDF of this DPA signed on its behalf. If the parties have signed a separate data processing agreement, that agreement prevails.

1. Subject, duration, nature and purpose

1.1 The Processor processes personal data on behalf of the Controller only to provide the services under the Services Agreement: receiving, storing, packing and shipping the Controller’s goods, handling returns and cash on delivery, providing the my.bigarena.net panel with its apps and integrations, and the functions the Controller activates in the panel, including the customer blacklist (clause 3).

1.2 This DPA applies for as long as the Processor processes personal data for the Controller.

1.3 Details of the processing are in Annex 1.

2. Instructions and obligations of the parties

2.1 The Processor processes the personal data only on the Controller’s documented instructions, including with regard to transfers to third countries. The Services Agreement, this DPA, the Controller’s orders and imports and the settings the Controller makes in the panel are the Controller’s instructions. If Union or Member State law to which the Processor is subject requires other processing, the Processor informs the Controller of that requirement beforehand, unless that law prohibits this.

2.2 The Processor informs the Controller if, in its opinion, an instruction infringes the GDPR or other data protection law.

2.3 The Processor does not use the Controller's personal data for its own purposes. Aggregated statistics that do not identify any person are not personal data.

2.4 The Controller is responsible for the lawfulness of the processing it instructs: it has a legal basis for the data it gives to the Processor, keeps the data accurate, and informs its customers in its privacy notice, including that their data is shared with fulfilment providers and couriers.

3. Customer blacklist

3.1 The panel lets the Controller keep a list of end customers (telephone number or e-mail address, a reason and an optional note) whose orders are flagged for the Controller's own review (the "**customer blacklist**"). The list is created, kept and used only for the Controller's account and stores. The Processor does not share it with other clients, does not compare it with other clients' lists and does not use it for its own purposes.

3.2 The Controller decides whom to add to the list and why. The Controller is responsible for:

(a) having a lawful basis for each entry, normally its legitimate interest under Article 6(1)(f) GDPR, and for respecting objections under Article 21;

(b) informing its customers about this processing in its privacy notice (Article 13) and, where it imports data obtained from another source, under Article 14;

(c) entering only factual reasons relating to orders, without insults, without special categories of data (Article 9) and without any reason based on a protected characteristic;

(d) reviewing flagged orders itself; the panel does not refuse orders automatically, and the Controller does not use the list to make decisions without human review (Article 22);

(e) the accuracy of the entries.

3.3 Each entry is kept for 24 months from the date it is added or last extended. Before an entry expires, the panel notifies the Controller, who may extend one or more entries by a further 24 months each time, only where the reason for the entry still exists. If the Controller does not extend an entry, it is deleted on its expiry date. The Controller may delete any entry at any time.

3.4 Files uploaded to import entries into the list are used only for that import.

4. Confidentiality

4.1 The Processor ensures that persons authorised to process the personal data are bound by confidentiality. Its staff access the Controller's data only as needed to provide the services or support.

5. Security

5.1 The Processor implements the technical and organisational measures in Annex 2 (Article 32 GDPR) and may update them, provided the overall level of security is not reduced.

6. Sub-processors

6.1 The Controller gives general authorisation for the sub-processors listed in Annex 3. The Processor informs the Controller of any intended addition or replacement at least 30 days in advance, by e-mail to the account e-mail address; where a replacement is urgently needed for security reasons, it informs the Controller as soon as possible. The Controller may object on reasonable grounds within that period. The Processor will first try to offer a reasonable alternative; if none is agreed, the Controller may terminate the affected services, subject to the end-of-service terms of the Services Agreement.

6.2 The Processor imposes on each sub-processor, by contract, data protection obligations that provide the same level of protection as this DPA, and remains liable to the Controller for the sub-processor's performance.

6.3 Couriers and postal operators receive the delivery data needed for delivery and, to the extent they determine the purposes and means of their processing under postal law, act as independent controllers. The Processor transmits that data on the Controller's instruction, including to the couriers the Controller or its customers choose. The current list of couriers is available in the panel.

7. Assistance

7.1 Taking into account the nature of the processing, the Processor assists the Controller:

(a) in responding to requests from data subjects under Articles 15 to 22 GDPR, mainly through the panel functions and on request to support@bigarena.net. Requests received by the Processor are forwarded to the Controller without undue delay and are not answered by the Processor on its own;

(b) with security, the notification of personal data breaches, data protection impact assessments and prior consultation (Articles 32 to 36 GDPR). Assistance beyond the panel functions and the information in this DPA may be charged at reasonable cost.

8. Personal data breaches

8.1 The Processor notifies the Controller without undue delay, and where feasible within 48 hours, after becoming aware of a personal data breach affecting the Controller's data, with the information available under Article 33(3) GDPR, and then provides further information as it becomes available. The Processor does not notify supervisory authorities or data subjects on the Controller's behalf without the Controller's instruction, unless the law requires it.

9. Audits and information

9.1 The Processor makes available the information necessary to demonstrate compliance with Article 28 GDPR, first by answering the Controller's written questions within 30 days.

9.2 Where that information is not sufficient, the Processor allows audits, including inspections, by the Controller or an auditor it mandates who is bound by confidentiality, on at least 30 days' notice, during business hours, no more than once a year unless a personal data breach or a supervisory authority requires otherwise. Audits must not give access to other clients' data or goods. The Controller bears its own costs and reasonable costs of the Processor's time.

10. End of the services

10.1 At the end of the services, the Processor, at the Controller's choice made within 30 days, returns the personal data through the panel export or deletes it. The Processor deletes the personal data from its live systems within 90 days; backup copies are overwritten in the ordinary backup cycle. Data contained in invoices, cash-on-delivery settlements and other accounting records is kept for as long as the law requires. On request the Processor confirms the deletion in writing.

11. Transfers outside the EEA

11.1 The Processor transfers personal data outside the European Economic Area only to the recipients listed in Annex 3 and to couriers under clause 6.3, and only on the basis of an adequacy decision of the European Commission, including the EU-US Data Privacy Framework, or the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 with the necessary supplementary measures. A copy of the relevant clauses is provided on request.

12. Liability, precedence, changes and law

12.1 Liability under this DPA follows the Services Agreement, except for intent and gross negligence, and without prejudice to Article 82 GDPR, under which each party is liable for its own part of any damage. The Controller indemnifies the Processor against claims and fines arising from the Controller's unlawful instructions or from entries the Controller makes in the customer blacklist.

12.2 If this DPA conflicts with the Services Agreement on data protection, this DPA prevails.

12.3 The Processor may update this DPA to reflect changes in the law, the services or the sub-processors by publishing a new version at <https://bigarena.net/dpa> and informing the Controller by e-mail at least 30 days before it takes effect. Changes may not reduce the protection of the personal data. A Controller who objects in writing within that period may terminate the affected services; until then the previous version applies to it.

12.4 This DPA is governed by the law of the country in which the Processor is registered, and the courts competent for the Processor's registered office have jurisdiction, as under the Terms of Service.

12.5 This DPA is published in Bulgarian and English. If the versions differ, the Bulgarian version prevails for Бигарена ООД and the English version for the other BigArena companies.

12.6 Contact for data protection questions: support@bigarena.net.

Annex 1: Details of the processing

Item	Details
Data subjects	End customers (buyers) of the Controller; persons receiving or returning parcels; the Controller's contact persons and panel users
Categories of data	name, delivery address, telephone, e-mail, order contents and value, cash-on-delivery amount, return reason, IBAN and account holder for refunds where the Controller uses this function, entries in the customer blacklist (telephone or e-mail, reason, note); video recordings of packing and of the opening of returns, where they show personal data (shipping labels)
Special categories	none intended; the Controller must not enter them
Operations	collection from the Controller's shops and imports, storage, labelling, packing, shipping, returns handling, cash-on-delivery reconciliation, matching orders against the customer blacklist, reporting
Duration	for the term of the Services Agreement and until return or deletion under clause 10; customer blacklist entries as in clause 3.3; packing and returns videos up to 90 days
Not covered	general video surveillance of warehouses for security, which the Processor carries out as controller under its own notice

Annex 2: Technical and organisational measures

- Panel and databases hosted in a data centre in the European Union (Germany).
- Access to the panel per account and user, with personal login and password; each client sees only its own data.

- Encrypted connections (HTTPS/TLS) to the panel and the APIs; network protection of the websites and the panel against attacks.
- BigArena staff access client data only as needed to provide the services or support, and are bound by confidentiality; access is removed when a person leaves.
- Packing and returns videos are accessible only to authorised staff and to the client concerned, and are kept for up to 90 days.
- Personal data breaches are handled and notified as set out in clause 8.

Annex 3: Sub-processors

Sub-processor	Service	Location and transfer basis
OVHcloud (OVH)	servers and databases of the panel	Germany (EU)
Cloudflare, Inc.	network security and content delivery for bigarena.net and my.bigarena.net	USA / EU; EU-US Data Privacy Framework, standard contractual clauses as fallback
BigArena companies in Bulgaria, Slovakia, Romania, Greece and Serbia	warehousing and fulfilment, only in the warehouses where the Controller stores goods	EU; Serbia: standard contractual clauses 2021/914
Partner warehouses that use the BigArena system	warehousing and fulfilment, only where the Controller chooses to store goods there	EU; outside the EEA: standard contractual clauses 2021/914