GOODTOGO Data Processing Agreement (GDPR Art. 28)

Standard template, version November 2026. GOODTOGO d.o.o., Zagreb.

1. Parties

This Data Processing Agreement ("DPA") is concluded between:

Controller: [Client company name], [address], [registration / VAT no.], represented by [name, title] (the "Controller" or "Organiser")

and

Processor: GOODTOGO d.o.o., Zavrtnica 17, HR-10000 Zagreb, Croatia, OIB 21447846241, MBS 081359397, represented by [name, title] (the "Processor" or "GOODTOGO")

This DPA forms part of the services agreement or order for [event name / services] dated [date] (the "Main Agreement"). It sets out the parties' obligations under Article 28 of Regulation (EU) 2016/679 ("GDPR") for personal data GOODTOGO processes on the Controller's behalf. If this DPA and the Main Agreement conflict on data protection, this DPA prevails.

The Controller owns all personal data processed under this DPA and determines the purposes and means of processing. GOODTOGO processes it only on the Controller's behalf.

2. Subject matter and duration

2.1 GOODTOGO processes personal data of the Controller's event attendees and related persons in order to provide event technology services: registration, ticketing, badge printing, QR access control and check-in, session scanning, and event apps (the "Services").

2.2 Annex 1 describes the nature and purpose of the processing, the categories of personal data and the categories of data subjects.

2.3 This DPA applies for as long as GOODTOGO processes personal data on the Controller's behalf, including after the Main Agreement ends, until the data is deleted or returned under Section 6.

3. Obligations of the Processor

3.1 **Instructions.** GOODTOGO processes personal data only on the Controller's documented instructions, including on transfers to third countries. The Main Agreement, this DPA, and the Controller's configuration and use of the Services are the Controller's instructions. If the law requires other processing, GOODTOGO informs the Controller first, unless that law prohibits it. GOODTOGO informs the Controller without delay if it believes an instruction infringes the GDPR or other data protection law.

3.2 **No own use.** GOODTOGO does not sell personal data, does not use it for its own purposes or marketing, and does not share it with other clients or other events.

3.3 **Confidentiality.** GOODTOGO grants access to personal data only to staff who need it to provide the Services. All such staff are bound by confidentiality, including after their employment ends.

3.4 **Security.** GOODTOGO implements the technical and organisational measures in Annex 2, as required by Article 32 GDPR. GOODTOGO may update these measures, provided the level of protection does not decrease.

3.5 **Data subject requests.** If a data subject contacts GOODTOGO directly, GOODTOGO forwards the request to the Controller without undue delay and does not answer it unless the Controller instructs it to. GOODTOGO helps the Controller fulfil requests to exercise the rights under Chapter III GDPR (access, rectification, erasure, restriction, portability, objection).

3.6 **Assistance.** Taking into account the nature of the processing and the information available to it, GOODTOGO assists the Controller with its obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments and prior consultation).

3.7 **Personal data breaches.** GOODTOGO notifies the Controller without undue delay, and no later than 48 hours after becoming aware of a personal data breach affecting the Controller's data. The notice includes, as far as known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. GOODTOGO does not notify supervisory authorities or data subjects on the Controller's behalf unless the Controller instructs it to.

3.8 **Audits.** GOODTOGO makes available all information needed to demonstrate compliance with Article 28 GDPR. It allows and contributes to audits and inspections by the Controller, or an auditor the Controller mandates, on at least 30 days' written notice, during business hours, no more than once a year unless a breach has occurred or a supervisory authority requires it. The auditor must be bound by confidentiality. Each party bears its own audit costs.

3.9 **Records.** GOODTOGO keeps a record of processing activities carried out on behalf of the Controller, as required by Article 30(2) GDPR.

4. Obligations of the Controller

4.1 The Controller is responsible for the lawfulness of the processing, including having a valid legal basis, informing data subjects (Articles 13 and 14 GDPR) and obtaining any consent required.

4.2 The Controller gives its instructions in writing (e-mail is sufficient) and informs GOODTOGO without delay if it finds errors or irregularities in the processing.

5. Sub-processors and transfers

5.1 The Controller gives general written authorisation for GOODTOGO to use the sub-processors listed in Annex 3.

5.2 GOODTOGO informs the Controller at least 30 days in advance of any intended addition or replacement of a sub-processor. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected Services without penalty.

5.3 GOODTOGO imposes on each sub-processor, by written contract, data protection obligations that offer at least the same level of protection as this DPA. GOODTOGO remains fully liable to the Controller for its sub-processors' performance.

5.4 Personal data is stored in the European Union (Frankfurt am Main, Germany). GOODTOGO does not transfer personal data outside the EEA except as set out in Annex 3, and then only under a valid transfer mechanism under Chapter V GDPR: an adequacy decision (including the EU-U.S. Data Privacy Framework) or the EU Standard Contractual Clauses.

6. Retention, return and deletion

6.1 The Controller decides how long personal data is kept. After an event the Controller may keep the data in its GOODTOGO account, for example to reuse it for future events, or instruct GOODTOGO to delete it.

6.2 On the Controller's written instruction, and in any case when the Services end, GOODTOGO will, at the Controller's choice, return the personal data in a common machine-readable format (e.g. CSV or Excel) and/or delete it. Deletion from live systems is completed within 30 days of the instruction. Backup copies are overwritten in their normal rotation and are not restored except to recover from an incident.

6.3 GOODTOGO confirms the deletion to the Controller in writing on request.

6.4 GOODTOGO may keep personal data longer only where EU or Croatian law requires it, and then only for that purpose.

7. Liability

Each party is liable as set out in Article 82 GDPR. Any limitation of liability in the Main Agreement applies to this DPA, to the extent the law allows.

8. Term and final provisions

8.1 This DPA enters into force when both parties sign it and remains in force as long as GOODTOGO processes personal data on the Controller's behalf.

8.2 Changes to this DPA must be in writing. If any provision is invalid, the rest of the DPA remains in force.

8.3 This DPA is governed by the law of the Republic of Croatia. The competent court in Zagreb has jurisdiction.

8.4 Contact for data protection matters: GOODTOGO d.o.o., info@goodtogo.hr, +385 1 6678082.

Signatures

	Controller	Processor
Company	[Client company name]	GOODTOGO d.o.o.
Name and title		
Place and date		Zagreb,
Signature		

Annex 1: Details of processing

Item	Description
Nature of processing	Collection, storage, organisation, retrieval, use, export and deletion of data through the GOODTOGO platform

Item	Description
Purpose	Registration, ticketing, badge printing, QR access control and check-in, session scanning, event apps and event reporting for the Controller's events
Data subjects	Event attendees and registrants, speakers, exhibitors, staff and guests of the Controller
Personal data	Only the fields the Controller configures, typically: name, e-mail, phone number, company, job title, ticket or registration category, badge and QR code, check-in and session-scan times, and app account data
Special categories (Art. 9)	None, unless the Controller requests it in writing for a specific event (e.g. dietary or accessibility needs)
Duration	For the term of the Main Agreement, then as set out in Section 6

Annex 2: Technical and organisational measures

- **Location:** all personal data is stored in EU data centres in Frankfurt am Main, Germany.
- **Encryption in transit:** all traffic to and from the platform uses HTTPS/TLS.
- **Access control:** access to production systems and the database is limited to authorised GOODTOGO staff, with individual credentials and strong passwords. Administrative access uses SSH keys.
- **Network protection:** applications are reachable only through a reverse proxy behind Cloudflare, which provides TLS and DDoS protection; internal services are not exposed to the internet.
- **Separation:** each Controller's data is logically separated; Controller users see only their own events.
- **Availability:** managed database with automated backups; documented restore procedure.
- **Staff:** confidentiality obligations and need-to-know access; data protection training at least once a year.
- **Deletion:** deletion on instruction, as set out in Section 6.

Annex 3: Authorised sub-processors

Sub-processor	Service	Data location	Transfer safeguard
Vultr (The Constant Company, LLC), USA	Cloud servers and managed PostgreSQL database	Frankfurt, Germany (EU)	Data stored in the EU; SCCs / EU-U.S. DPF for any remote access
Amazon Web Services EMEA SARL, Luxembourg	File storage (Amazon S3, region eu-central-1)	Frankfurt, Germany (EU)	Data stored in the EU; SCCs / EU-U.S. DPF
Cloudflare, Inc., USA	DNS, TLS encryption, DDoS protection and content delivery. Traffic passes through its network; the attendee database is not stored there	Global network, nearest EU location for EU visitors	SCCs / EU-U.S. DPF

GOODTOGO uses no other sub-processors for the Controller's personal data.