Data Processing Agreement

Annex 1 to the Inboxgame Terms of Service

Last updated: 17 November 2026

1. Parties and background

1.1 This Data Processing Agreement (the "DPA") is entered into between the customer that has accepted the Inboxgame Terms of Service (the "Customer"), acting as controller, and Inboxgame ApS, CVR no. 38486071, Løvsangervej 16, Kongsted, 4683 Rønnede, Denmark ("Inboxgame"), acting as processor.

1.2 The DPA is Annex 1 to the Inboxgame Terms of Service (the "Terms"). It sets out the conditions under which Inboxgame processes personal data on behalf of the Customer, as required by Article 28(3) of Regulation (EU) 2016/679 (the "GDPR").

1.3 The structure of the DPA follows the European Commission's standard contractual clauses under Article 28(7) GDPR (Implementing Decision (EU) 2021/915) in a shortened form.

1.4 The Customer runs game campaigns built on the Inboxgame platform. Inboxgame hosts each game on its servers in Amsterdam and publishes it on a subdomain of the Customer's own domain, for example spil.customer.dk, which the Customer points to Inboxgame's servers. Inboxgame collects the participants' sign-ups, delivers them to the Customer's own systems and gives the Customer a private link to the campaign statistics.

2. Definitions

2.1 Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meaning given in the GDPR.

2.2 "Campaign" means a game campaign that the Customer has approved and that runs on the Inboxgame platform. "Participant" means a person who plays a game or signs up in a Campaign. "Sub-processor" means a processor engaged by Inboxgame to process personal data on behalf of the Customer.

3. Description of the processing

The subject matter, nature, purpose and duration of the processing, the categories of data subjects and the types of personal data are described in Appendix A.

4. Instructions

4.1 Inboxgame processes personal data only on documented instructions from the Customer, including with regard to transfers to third countries, unless Union or Member State law requires

otherwise. In that case Inboxgame informs the Customer of that legal requirement before processing, unless the law prohibits it.

4.2 The Customer's documented instructions consist of the Terms, this DPA and the Campaign setup the Customer approves, including the sign-up fields, the consent text the Customer writes and the systems the sign-ups are delivered to. The Customer may give further instructions in writing, including by email.

4.3 Inboxgame immediately informs the Customer if, in Inboxgame's opinion, an instruction infringes the GDPR or other Union or Member State data protection rules.

4.4 If the law requires Inboxgame to disclose personal data to an authority or another third party, Inboxgame informs the Customer before the disclosure, unless the law prohibits it.

4.5 On the Customer's Campaigns, Inboxgame does not:

- send copies of sign-ups to Inboxgame's own lists, brands or email platforms
- place its own tracking, such as advertising pixels, on the Campaign pages
- offer the Campaign or its sign-ups to lead networks or lead buyers
- add sponsors or other recipients to the sign-up form, the consent text or the competition rules
- use the sign-ups for its own purposes, such as its own marketing or enriching its own lists

If the Customer wants its own tracking on the Campaign pages, the Customer instructs Inboxgame in writing and describes the tracking in its own privacy policy. This clause does not affect clause 13.4.

5. Confidentiality

Inboxgame grants access to the personal data only to employees and others who need it to perform the services. Everyone with access is bound by a duty of confidentiality, either by contract or by law. The duty of confidentiality continues after this DPA has ended. Persons who are not employed by Inboxgame, such as an external developer, sign a written confidentiality declaration before they get access. Inboxgame keeps a list of the persons who have access and gives it to the Customer on request.

6. Security of processing

6.1 Inboxgame implements the technical and organisational measures required by Article 32 GDPR to ensure a level of security appropriate to the risk. The measures are described in Appendix C.

6.2 Inboxgame may update the measures as technology develops, provided the overall level of security is not reduced.

7. Sub-processors

7.1 The Customer gives Inboxgame general written authorisation to engage sub-processors. The sub-processors Inboxgame uses on the date of this DPA are listed in Appendix B.

7.2 Inboxgame notifies the Customer in writing at least 30 days before adding or replacing a sub-processor. The notice is sent by email to the Customer's contact person.

7.3 The Customer may object to the change on reasonable data protection grounds within the notice period. If the Customer does not object, or continues to use the services after the change, the Customer has accepted it. If the Customer objects, the parties seek a solution in good faith. If they cannot agree, the Customer may terminate the affected services. Termination is the Customer's only remedy. Inboxgame does not pay compensation, and paid amounts are not refunded, see section 5.4 of the Terms.

7.4 Inboxgame imposes the same data protection obligations as in this DPA on each sub-processor by written contract. Inboxgame remains fully liable to the Customer for the sub-processor's performance of its obligations.

---

8. Transfers to third countries

8.1 Inboxgame transfers personal data to a country outside the EU and EEA only in compliance with Chapter V GDPR, namely on the basis of:

- an adequacy decision from the European Commission, including the EU-US Data Privacy Framework for certified US companies, or
- the Commission's standard contractual clauses, together with supplementary measures where needed.

8.2 By accepting this DPA, the Customer instructs Inboxgame to carry out the transfers listed in Appendix B.

---

9. Assistance to the Customer

9.1 Inboxgame forwards any request concerning the personal data that it receives from a data subject, a supervisory authority or another third party to the Customer without undue delay and no later than 2 working days after receiving it. Inboxgame does not respond to the request itself unless the Customer authorises it or the law requires it.

9.2 Taking into account the nature of the processing, Inboxgame assists the Customer with appropriate technical and organisational measures in responding to requests from data subjects exercising their rights. On the Customer's request, Inboxgame finds, exports, corrects or deletes a named Participant's data within 5 working days. Inboxgame can find a Participant by email address.

9.3 Taking into account the nature of the processing and the information available to Inboxgame, Inboxgame also assists the Customer with:

- the security of processing under Article 32
- notification of personal data breaches under Articles 33 and 34
- data protection impact assessments under Article 35
- prior consultation of the supervisory authority under Article 36

9.4 Inboxgame may charge for assistance that goes beyond what is included in the services, unless the assistance is needed because Inboxgame has breached this DPA. Inboxgame gives the Customer the price before the work starts. Pricing never delays the deadlines in this DPA or in the GDPR: Inboxgame notifies breaches under clause 10 and helps the Customer meet the deadlines for data subjects' requests, whether or not a price for further assistance has been agreed.

---

10. Personal data breaches

10.1 Inboxgame notifies the Customer of a personal data breach without undue delay and no later than 24 hours after becoming aware of it. Inboxgame notifies the Customer's contact person in writing by email, see clause 16.1.

10.2 The notification contains, as far as possible:

- a description of the nature of the breach, including the categories and approximate number of data subjects and records concerned
- the name and contact details of Inboxgame's contact person
- the likely consequences of the breach
- the measures taken or proposed to address the breach and limit its effects

If not all information is available at once, Inboxgame provides it in phases without undue delay.

10.3 The Customer is responsible for notifying the Danish Data Protection Agency (Datatilsynet) and the data subjects where required. Inboxgame assists as described in clause 9.3.

10.4 Inboxgame documents every personal data breach, including the facts, its effects and the measures taken. Inboxgame makes the documentation available to the Customer and to the supervisory authority on request.

---

11. Audits and information

11.1 Inboxgame makes available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and this DPA. On request, this includes:

- who has access to the Customer's personal data, with name and role
- documentation that the Customer's personal data is kept in a separate database
- the results of Inboxgame's automated nightly checks, including of separation, encryption and deletion
- a record of deletions, with the number of records deleted per date

Inboxgame logs every successful login to the platform's administration with account, time and IP address, and every login to the servers with the personal key used. The logs show who has logged in and when. They do not attribute each action within a session to a named person.

11.2 Inboxgame allows and contributes to audits, including inspections, carried out by the Customer or by an independent auditor appointed by the Customer. Inboxgame must approve the auditor in advance and does not refuse without good reason. The auditor must be bound by confidentiality. The

audit only covers the processing of the Customer's personal data and must be carried out without unreasonably disrupting Inboxgame's operations. The Customer gives at least 30 days' written notice. Audits take place no more than once a year, unless a personal data breach or a request from a supervisory authority justifies more.

11.3 Inboxgame may meet an audit request by providing documentation, written answers or reports from independent third parties, where these are sufficient.

11.4 The Customer bears its own costs of an audit and pays for the time Inboxgame spends assisting with it, see clause 9.4. Inboxgame tells the Customer the expected amount before the audit starts. If the audit shows that Inboxgame has materially breached this DPA, Inboxgame bears its own costs.

11.5 Audits and inspections carried out by a supervisory authority are not subject to the conditions in clauses 11.2 to 11.4.

---

12. The Customer's obligations

12.1 The Customer is responsible for having a lawful basis for the processing, normally the Participants' consent. Where sign-ups are used for marketing by email or text message, the Customer is responsible for obtaining consent under section 10 of the Danish Marketing Practices Act (markedsføringsloven) or the equivalent rules in its own country.

12.2 The Customer writes its own consent text and competition rules, approves them before the Campaign goes live and is responsible for their content.

12.3 The Customer informs the Participants under Article 13 GDPR, including through its own privacy policy, which must be linked from the sign-up.

12.4 The Customer draws the winner among the Participants in its own systems and handles the prize.

12.5 Once sign-ups have been delivered to the Customer's own systems, the Customer is solely responsible for the further processing there.

12.6 The Customer does not instruct Inboxgame to collect special categories of personal data under Article 9 GDPR unless the Customer has obtained the Participants' explicit consent and has informed Inboxgame in writing in advance. The Customer never instructs Inboxgame to collect personal data relating to criminal convictions and offences under Article 10 GDPR.

12.7 The Customer sets the minimum age for Participants in its competition rules. Campaigns must not be aimed at children. The minimum age must not be lower than the age at which a child can consent on its own in the country where the Campaign runs. In Denmark that age is 15 (section 6(2) of the Danish Data Protection Act). Campaigns can run in any country, and the Customer is responsible for knowing the age limit and the other rules in each country where its Campaign runs. The Customer tells Inboxgame which countries a Campaign will run in before it goes live.

12.8 The Customer decides which sign-up fields and other personal data each Campaign collects, and only asks for the data needed for the purpose. The Customer bears the risk if a Campaign collects more personal data than needed.

12.9 On request, the Customer gives Inboxgame without undue delay the information and assistance Inboxgame needs to comply with the GDPR when processing personal data for the Customer.

13. Duration, deletion and return

13.1 This DPA applies for as long as Inboxgame processes personal data on behalf of the Customer.

13.2 Inboxgame automatically deletes each Participant's personal data 90 days after the Participant signed up, unless the parties agree on another period in writing. Deletion runs every night. Sign-ups are delivered to the Customer's own systems as they come in, see clause 12.5. Inboxgame ensures that LeadByte deletes the sign-ups within the same period: before a Campaign goes live, Inboxgame sets the retention period in the Customer's own LeadByte campaign to 90 days, so LeadByte deletes the sign-ups automatically. Deletion at Inboxgame does not delete at LeadByte, which is why the period is set in both systems.

13.3 When the services end, Inboxgame, at the Customer's choice, either returns all personal data in a machine-readable format and then deletes it, or deletes it, within 7 days after the services end, unless Union or Member State law requires storage. Inboxgame then deletes the Customer's separate database in its entirety. Until it is deleted, the nightly deletion in clause 13.2 continues, so no Participant's data is kept longer than the period in clause 13.2. On request, Inboxgame confirms the deletion in writing.

Deleted data can remain in backups for up to one month, after which the backups are overwritten. This covers Inboxgame's own backups and DigitalOcean's daily backups of the whole server, which are kept for seven days, see Appendix C. Inboxgame does not delete data inside a backup, because that would make the backup unusable for restoring the platform. The backups are not used for any other purpose than restoring data.

13.4 The Customer instructs Inboxgame to anonymise and aggregate data from Campaigns so that neither the Customer nor any Participant can be identified. Inboxgame may use the anonymised data, also after this DPA has ended, to improve the platform and to show aggregated figures, such as average participation rates, in its marketing.

14. Liability

14.1 Each party's liability under this DPA is subject to the limitations of liability in the Terms, unless mandatory law provides otherwise.

14.2 Nothing in this DPA limits the parties' liability to data subjects under Article 82 GDPR.

15. Precedence, changes and governing law

15.1 In case of conflict between this DPA and the Terms on matters of data protection, this DPA prevails.

15.2 Inboxgame may change this DPA by notifying the Customer's contact person by email at least 30 days before the change takes effect. Changes required by law can take effect with shorter notice.

Changes of sub-processors follow clause 7. If the Customer continues to use the services after the change has taken effect, the Customer has accepted it. If the Customer does not accept the change, the Customer may terminate the services before it takes effect.

15.3 This DPA is governed by Danish law. Disputes are settled by the courts specified in the Terms.

---

16. Contact persons and acceptance

16.1 Inboxgame's contact person for data protection is Camilla Estrup Vetterlain, privacy@inboxgame.ai. The Customer's contact person is the person given when the Customer signed up, unless the Customer informs Inboxgame of another.

16.2 The Customer accepts this DPA electronically by ticking a box when it accepts the Terms and approves its first Campaign. Inboxgame stores the time of acceptance and the version of this DPA that was accepted.

Appendix A. Description of the processing

Subject matter	Running game Campaigns for the Customer on the Inboxgame platform
Nature	Hosting the game, collecting and storing sign-ups, delivering them to the Customer's systems, statistics and support
Purpose	To let the Customer run competitions and collect sign-ups with consent for its own marketing
Duration	For as long as Inboxgame processes data for the Customer, see clause 13
Data subjects	Participants in the Customer's Campaigns, and visitors who open a Campaign without playing or signing up. For visitors, only IP address, device and browser data and the source of the visit are processed
Frequency	Continuously while a Campaign is live
Location	Servers in Amsterdam, the Netherlands (EU). Delivery of sign-ups through LeadByte, received in Ireland (EU). Cloudflare's global network. See Appendix B

Types of personal data

- name, email address and phone number
- other sign-up fields the Customer chooses, and what the Participant writes in them
- game activity: time stamps, number of attempts, whether the Participant won, and clicks
- IP address, browser, operating system, device type and language
- consent record: whether the consent box was ticked, the time stamp, and a fingerprint (SHA-256) of the consent text shown to the Participant. Each version of the text is kept in a log that can only be added to, so it can be shown later what the Participant agreed to
- source of the visit, for example UTM parameters

Special categories of personal data: none, unless clause 12.6 applies. No data relating to criminal convictions and offences.

Retention: 90 days after the Participant signed up, see clause 13.2, and no more than 7 days after the services end, see clause 13.3. Up to one month more in backups, see clause 13.3.

Appendix B. Approved sub-processors

Sub-processor	Purpose	Location	Transfer basis
DigitalOcean, LLC	Server, database and backups for the game platform, including a daily backup of the whole server that DigitalOcean keeps for seven days	Amsterdam, the Netherlands (EU). DigitalOcean is a US company	The data is stored in the EU. Any access from the United States is covered by the EU-US Data Privacy Framework, or by standard contractual clauses if the certification lapses
Cloudflare, Inc.	DNS, access control, protection against attacks and bots, and delivery of the game pages	United States, global network	EU-US Data Privacy Framework
LeadByte Limited	Delivering sign-ups to the Customer's systems	Ireland (EU), where sign-ups are received (Amazon Web Services, Dublin, measured by a DNS lookup on 16 November 2026). LeadByte is a UK company	Received in the EU. Any access from the United Kingdom is covered by the EU adequacy decision for the United Kingdom, valid until 27 December 2031. LeadByte's privacy policy reserves the right to transfer personal data outside the United Kingdom and the EEA under standard contractual clauses when needed to provide its service
External developer	Operating and developing the game platform, with full access to the server	Denmark	Within the EU

Inboxgame uses no other sub-processors for Participants' personal data. The providers Inboxgame uses for inboxgame.ai itself, such as Supabase, Hetzner and Resend, do not receive Participants' personal data. The Customer's statistics page runs on a Hetzner server in Germany and shows only counts, not data about individual Participants. AI providers do not receive Participants' personal data either.

For each Customer, Inboxgame sets up a separate campaign in LeadByte that is used only for that Customer. Sign-ups from the Customer's Campaigns are not shared with or sold to others. Automatic

replies by email or text message from LeadByte are switched off, unless the Customer asks for them in writing.

Appendix C. Technical and organisational security measures

Area	Measure
Hosting	The game platform runs on a DigitalOcean server in Amsterdam. DigitalOcean has a SOC 2 Type II report, and its data centres are certified to ISO 27001. The reports and certificates cover DigitalOcean's own infrastructure, not Inboxgame's processes. Inboxgame itself is not certified
Separation	Each Customer's Participant data is kept in a separate database that is used only for that Customer. If that database cannot be opened, the platform stops with an error instead of writing the data anywhere else
Encryption in transit	All traffic to the game pages uses HTTPS (TLS) through Cloudflare. Sign-ups are delivered to LeadByte over HTTPS
Encryption at rest	All database tables are encrypted with AES-256. Inboxgame's own backups are encrypted separately with AES-256. The keys are stored on the server, readable only by the system accounts that use them, and a copy is kept outside the server. The encryption protects copies that leave the server. It does not protect against anyone with full access to the server or to a complete copy of it, see Backups
Access control	Personal admin accounts with hashed passwords and two-factor authentication for each account. The administration can only be reached through Cloudflare Access. Server access only with personal SSH keys, without passwords. The control panel and the database only accept connections from named addresses
Logging	Every successful login to the administration is logged with account, time and IP address, and every login to the server with the key used
Monitoring	An automated check runs every night, covering among other things separation, encryption, backups, updates, the consent record, passwords in clear text and new server keys. Inboxgame is alerted if a check fails
Protection against abuse	Cloudflare protection and Cloudflare Turnstile against bots and spam. The server only accepts web traffic from Cloudflare
Secrets	API keys and passwords are stored on the server, never in the browser. Passwords for the Customer databases are kept outside the web root and outside the code repository
Backups	Two layers. Inboxgame's own backups run daily on the server: seven daily copies and one monthly copy are kept, encrypted. DigitalOcean also takes a daily backup of the whole server and keeps each for seven days. The server has one disk, so DigitalOcean's backup also contains the encryption keys. The encryption therefore does not protect those copies against DigitalOcean, which is why DigitalOcean is listed in Appendix B for storage

Area	Measure
Updates	The control panel updates the server's packages every night and installs security updates every hour. On the first working day of each month, a person installs waiting updates, including a new kernel, and restarts the server. The nightly check raises an alert if a new kernel has waited more than 7 days without a restart, or a security update has waited more than 30 days
Staff	Access only for the persons who need it. Everyone with access is bound by confidentiality, see clause 5
Breaches	A written plan for handling security incidents and personal data breaches, see clause 10
Deletion	Automatic deletion every night as described in clause 13, logged with the number of records per Customer