

MUTUAL NONDISCLOSURE AND RESTRICTED USE AGREEMENT

PartEnvoy manufacturing sourcing engagements

Effective Date	[INSERT DATE]
PartEnvoy	Dániel Gergő Kis, registered in the Netherlands as a sole proprietor (eenmanszaak), KVK number 42159606, registered office Tongelresestraat 377, Eindhoven, Netherlands, trading as PartEnvoy
Counterparty	[FULL LEGAL NAME], a [LEGAL FORM] organised under the laws of [JURISDICTION], registration number [NUMBER], registered office [ADDRESS]

Each entity identified above is a Party and together they are the Parties. A Party is a Disclosing Party when it provides Confidential Information and a Receiving Party when it receives Confidential Information.

The Parties expect to exchange information to evaluate, negotiate, arrange, quote, source, manufacture, inspect, deliver or support custom-manufactured components and related services, including requests for quotation, technical feasibility, supplier qualification and commercial coordination (the Purpose). The Parties agree as follows.

1 Definitions and interpretation

Affiliate means an entity that directly or indirectly controls, is controlled by or is under common control with a Party, where control means ownership of more than fifty percent of voting rights or the practical power to direct management.

Applicable Law means all laws, regulations, binding regulatory requirements, court orders and sanctions applicable to a Party, the information or the Purpose.

Confidential Information means information disclosed or made accessible by or on behalf of a Disclosing Party, before or after the Effective Date, in any form, that is marked confidential or that a reasonable person would understand to be confidential given its nature or the circumstances of disclosure. It includes: technical drawings, CAD models, specifications, tolerances, samples, prototypes, bills of material, software, source code, manufacturing methods, test and inspection data, quality records, nonconformities, tooling, processes, know-how and inventions; RFQs, quotations, costs, prices, margins, forecasts, volumes, delivery terms and commercial strategies; supplier, customer and prospect identities, contacts, capabilities, capacity, performance and relationship history; contracts, negotiations and the existence or terms of discussions; credentials, security information, system architecture, incident information and access logs; Personal Data; third-party information the Disclosing Party must protect; and analyses, notes, compilations, models or other materials that contain, reflect or permit inference of such information.

Disclosing Party means a Party and its Affiliates or third-party sources whose Confidential Information is disclosed by or through that Party.

Introduced Party means a supplier, manufacturer, customer, prospect, consultant, logistics provider or other commercial contact whose identity or relevant opportunity is first disclosed to the Counterparty by or through PartEnvoy in connection with the Purpose.

Personal Data means personal data as defined by Regulation (EU) 2016/679 and any applicable implementing or successor law.

Representative means a Receiving Party's directors, officers, employees, professional advisers, auditors, insurers, financing sources, Affiliates and approved subcontractors who need the information for the Purpose and are bound by confidentiality and restricted-use obligations at least as protective as this Agreement.

Security Incident means actual or reasonably suspected unauthorised access to, acquisition, use, alteration, loss, destruction or disclosure of Confidential Information, or a material compromise of systems holding it.

Trade Secret means Confidential Information that qualifies for protection as a trade secret or bedrijfsgeheim under Applicable Law, including the Dutch Trade Secrets Protection Act and Directive (EU) 2016/943.

1.1 References to including or includes are non-exhaustive. A reference to writing includes email and a reliable electronic signature process. Headings aid navigation and do not affect interpretation.

1.2 An obligation not to do something includes an obligation not to permit, assist or procure it. A requirement for consent means prior written consent from an authorised representative.

2 Coverage of disclosures

2.1 This Agreement covers Confidential Information disclosed during the term and during the twenty-four months before the Effective Date in connection with the Purpose.

2.2 Information need not be labelled, summarised in writing or disclosed in a particular medium to be protected. Oral, visual and observed information is protected when its nature or context would indicate confidentiality.

2.3 Information remains Confidential Information when combined with public information if the combination, selection, arrangement or resulting insight is not public.

2.4 The Disclosing Party's failure to mark or restrict one disclosure does not waive protection for that or any later disclosure.

3 Exclusions

Confidential Information excludes information that the Receiving Party proves by contemporaneous written evidence:

- (a) was lawfully known to it without restriction before receipt from the Disclosing Party;
- (b) becomes public through no breach of this Agreement or other duty by the Receiving Party or any person for whom it is responsible;
- (c) is lawfully received from a third party that, after reasonable enquiry where circumstances warrant it, is not known to owe a confidentiality duty concerning the information;
- (d) is independently developed without access to or use of the Confidential Information, as demonstrated by dated development records; or
- (e) the Disclosing Party expressly authorises for unrestricted release in writing.

3.1 A disclosure does not fall within an exclusion merely because individual elements are public or because the Receiving Party can reconstruct the information after receiving it.

4 Restricted use and standard of care

4.1 The Receiving Party shall use Confidential Information only for the Purpose and only to the extent reasonably necessary for the Purpose.

4.2 The Receiving Party shall protect Confidential Information using at least the care it uses for its own information of comparable sensitivity and, in all cases, no less than reasonable care.

4.3 The Receiving Party shall not, without consent: exploit Confidential Information for its own or another person's commercial advantage outside the Purpose; copy or translate it except as necessary for the Purpose; remove confidentiality, ownership or traceability markings; publish it; use it to compete with, disintermediate or

disadvantage the Disclosing Party; or combine it with another dataset in a way that exposes or materially increases access to it.

- 4.4 The Receiving Party shall not upload Confidential Information to a public, consumer or unapproved generative-AI, machine-learning or data-analytics service. Use of an approved service is permitted only if the service is contractually prohibited from training on, retaining beyond the authorised task, or disclosing the information, and the Receiving Party remains responsible for the service.
- 4.5 The Receiving Party shall not use Confidential Information for benchmarking, model training, dataset enrichment or product development unrelated to the Purpose.

5 Representatives and controlled disclosure

- 5.1 The Receiving Party may disclose Confidential Information only to Representatives who need it for the Purpose. It shall disclose only the minimum information reasonably required for each Representative's role.
- 5.2 Before disclosure, the Receiving Party shall ensure that each Representative is subject to enforceable confidentiality and restricted-use duties at least as protective as this Agreement. Professional advisers may instead be bound by professional duties.
- 5.3 The Receiving Party is responsible for each Representative's act or omission as if it were the Receiving Party's own, except to the extent Applicable Law does not permit that responsibility.
- 5.4 A competitor of the Disclosing Party, a competing sourcing platform, a proposed substitute supplier or a subcontract manufacturer is not an authorised Representative unless the Disclosing Party expressly approves the disclosure.
- 5.5 On reasonable request, the Receiving Party shall identify the categories of Representatives that received specified Confidential Information and confirm their continuing need for access. It need not disclose legally privileged advice or adviser work product.

6 Information security

- 6.1 The Receiving Party shall maintain proportionate technical and organisational safeguards appropriate to the sensitivity, volume and risk of the Confidential Information. For technical files, credentials, Personal Data and commercially sensitive RFQ material, safeguards shall include, where reasonably applicable: role-based least-privilege access; multi-factor authentication; encryption in transit and at rest; supported and patched systems; malware protection; secure transfer channels; access revocation when no longer required; resilient backups; and secure disposal.
- 6.2 The Receiving Party shall not store Confidential Information in personal email, unmanaged devices, public links, removable media or consumer file-sharing services unless specifically authorised and appropriately secured.
- 6.3 The Receiving Party shall preserve file integrity, version information and material metadata where relevant to engineering, quality, traceability or evidentiary use. It shall not alter technical requirements except through an authorised change process.
- 6.4 If Schedule 1 specifies an approved system, territory, classification or handling rule, the Receiving Party shall comply with it. A stricter project-specific requirement controls for that project.
- 6.5 On a reasonable written request related to a material risk or Security Incident, the Receiving Party shall provide a written description of relevant safeguards and reasonable evidence of compliance. Any independent review shall protect the Receiving Party's own confidential information and avoid unreasonable operational disruption.

7 Security incidents

- 7.1 The Receiving Party shall notify the Disclosing Party without undue delay after becoming aware of a Security Incident and, where reasonably practicable, within twenty-four hours. Initial notice may be preliminary and shall not be delayed because an investigation is incomplete.

- 7.2 The notice shall describe, to the extent known: the affected information and systems; likely timing, cause, scope and consequences; containment and remediation taken or planned; and a contact for coordination. The Receiving Party shall provide material updates as facts develop.
- 7.3 The Receiving Party shall promptly contain, investigate and remediate the Security Incident; preserve relevant evidence and logs; cooperate with reasonable mitigation; and not notify third parties, regulators or affected persons in the Disclosing Party's name without consent, unless Applicable Law requires it.
- 7.4 Each Party bears its own internal response costs. Responsibility for losses, regulatory consequences and third-party claims remains determined by this Agreement and Applicable Law.

8 Required and protected disclosures

- 8.1 If Applicable Law, a regulator, stock-exchange rule or binding court order requires disclosure, the Receiving Party may disclose only the legally required minimum. Unless prohibited, it shall give prompt written notice, provide the proposed disclosure where practicable, and reasonably assist the Disclosing Party in seeking confidential treatment or protective relief. The Disclosing Party bears the external cost of relief it requests.
- 8.2 Nothing in this Agreement prohibits a person from reporting suspected unlawful conduct to a competent authority, cooperating with an investigation, making a protected whistleblowing disclosure, consulting a worker representative or professional adviser, or exercising a non-waivable legal right. A person need not notify a Party where notification is prohibited or would undermine the protected activity.

9 Personal data

- 9.1 Each Party shall process Personal Data lawfully, fairly, transparently and securely, and only as necessary for the Purpose. Each Party acts as an independent controller unless the circumstances and a separate written agreement establish another role.
- 9.2 This Agreement is not a data-processing agreement. Before one Party processes Personal Data as processor for the other, the Parties shall enter into an agreement satisfying Article 28 GDPR and any required international-transfer mechanism.
- 9.3 A Party shall not intentionally disclose special-category data, criminal-offence data, national identification numbers or unnecessary personal data unless the Parties first document a lawful basis, necessity and appropriate safeguards.
- 9.4 A Security Incident involving Personal Data shall also be handled in accordance with applicable data-protection law. Nothing in this Agreement extends a statutory notification deadline.

10 Compliance boundaries

- 10.1 Each Party shall comply with Applicable Law relating to export controls, sanctions, anti-bribery, competition, product control, national security and regulated technical data.
- 10.2 The Disclosing Party shall identify known export classifications, controlled-technology restrictions or contractual flow-down requirements before disclosure where reasonably practicable. The Receiving Party shall not export, re-export, provide remote access to or transfer controlled information contrary to an identified restriction or Applicable Law.
- 10.3 This Agreement does not authorise the exchange of information for price fixing, market or customer allocation, bid coordination, output restriction or any other anticompetitive purpose. Where the Parties are actual or potential competitors, they shall limit exchanges to what is objectively necessary for the Purpose and use clean-team or aggregation safeguards where appropriate.

11 Ownership intellectual property and reverse engineering

- 11.1 All Confidential Information remains owned by the Disclosing Party or its source. No right, title, licence or other interest in intellectual property is granted except the limited, revocable right to use Confidential Information for the Purpose.

- 11.2 Disclosure does not create inventorship, authorship, joint ownership, an obligation to assign, or a licence by estoppel, implication or exhaustion. Development, tooling, foreground intellectual property and feedback rights require a separate written agreement.
- 11.3 The Receiving Party shall not reverse engineer, decompile, disassemble, measure, analyse or test a sample, prototype, software object or other tangible embodiment to discover composition, source code, process parameters or design logic, except to the extent expressly authorised or a mandatory law makes the restriction unenforceable. Where lawful, the Receiving Party shall first request the necessary information from the Disclosing Party.
- 11.4 No residuals licence applies. Information retained in unaided memory remains subject to this Agreement and may not be used outside the Purpose.

12 Introduced relationships and noncircumvention

- 12.1 Supplier, customer and opportunity identities disclosed by PartEnvoy are Confidential Information when not already demonstrably known to the Counterparty without restriction.
- 12.2 During the term and for twenty-four months after each introduction, the Counterparty shall not knowingly use Confidential Information to bypass PartEnvoy by directly or indirectly soliciting, negotiating or transacting with an Introduced Party concerning the same or a substantially related opportunity for the principal purpose of avoiding PartEnvoy's agreed role or fees.
- 12.3 Clause 12.2 does not prohibit: a documented pre-existing active relationship disclosed to PartEnvoy promptly after the introduction; general advertising not directed using Confidential Information; an independently arising opportunity proved by contemporaneous records; or contact approved in writing by PartEnvoy.
- 12.4 This clause does not set PartEnvoy's remuneration, create exclusivity or require a transaction. Fees and commercial scope must be agreed separately. The restriction shall be interpreted no more broadly than reasonably necessary to protect PartEnvoy's confidential introductions and legitimate commercial interest.

13 Return retention and destruction

- 13.1 On written request or when the Purpose ends, the Receiving Party shall promptly stop use and, within ten business days, return or securely destroy Confidential Information and copies under its control, including derivative materials, subject to clauses 13.2 and 13.3.
- 13.2 The Receiving Party may retain: one restricted archival copy solely to demonstrate compliance or meet legal, regulatory, insurance or professional obligations; information subject to a documented legal hold; and automatically created backup copies that cannot reasonably be isolated, provided they remain protected, are not restored except for disaster recovery, and are deleted in the ordinary backup cycle.
- 13.3 The Receiving Party is not required to delete records that Applicable Law requires it to retain, but it shall restrict access and use to the retention purpose and destroy them when that requirement ends.
- 13.4 On request, an authorised representative shall certify material completion of return or destruction, identifying any permitted retention category without disclosing privileged information.

14 Term and survival

- 14.1 This Agreement begins on the Effective Date and continues for three years unless a Party terminates it on thirty days' written notice. Termination does not affect information disclosed before termination.
- 14.2 For Confidential Information that is not a Trade Secret or Personal Data, clauses 4 through 13 survive for seven years after the relevant disclosure.
- 14.3 Obligations concerning a Trade Secret survive for as long as the information remains a Trade Secret through no breach by the Receiving Party. Obligations concerning Personal Data survive for as long as Applicable Law or the permitted processing requires.
- 14.4 Clauses intended by their nature to continue, including ownership, remedies, governing law and accrued rights, survive termination.

15 Remedies and responsibility

- 15.1 Unauthorised use or disclosure may cause harm not adequately repaired by damages alone. A Disclosing Party may seek interim, injunctive or other equitable relief, including urgent proceedings, without limiting any other remedy and without being required to prove that damages are an adequate substitute, subject to the court's powers and Applicable Law.
- 15.2 Each Party remains liable for breach under Applicable Law. A limitation or exclusion in another agreement does not apply to this Agreement unless that other agreement expressly identifies this Agreement and the specific limitation intended to apply.
- 15.3 Nothing excludes or limits liability to the extent exclusion or limitation is prohibited by Applicable Law, including for fraud, wilful misconduct or infringement of another person's intellectual property rights where such liability cannot lawfully be excluded.
- 15.4 The rights and remedies under this Agreement are cumulative but do not permit double recovery for the same loss.

16 Authority no warranty and no obligation to proceed

- 16.1 Each Disclosing Party represents that it has authority to disclose its Confidential Information for the Purpose, subject to any restriction it communicates before disclosure.
- 16.2 Except for clause 16.1 and any non-excludable duty, Confidential Information is provided as is. The Disclosing Party does not warrant accuracy, completeness, fitness, manufacturability or non-infringement. The Receiving Party remains responsible for its own technical, commercial, legal and safety evaluation.
- 16.3 Neither disclosure nor this Agreement obliges a Party to continue discussions, disclose particular information, place or accept an order, grant exclusivity, select a supplier or enter another agreement. Either Party may end discussions subject to surviving obligations.

17 Privilege and publicity

- 17.1 Disclosure of material protected by legal professional privilege, litigation privilege or work-product protection is not intended to waive that protection. On notice of inadvertent disclosure, the Receiving Party shall stop review, secure the material and return or destroy it as directed, without prejudice to rights that cannot lawfully be waived.
- 17.2 Neither Party may use the other Party's name, logo, trademarks, project identity or the existence of discussions in advertising, case studies, press releases, customer lists or public statements without consent, except for a legally required disclosure handled under clause 8.

18 Relationship of the Parties

- 18.1 The Parties are independent contractors. This Agreement does not create a partnership, joint venture, fiduciary relationship, employment, agency, distributorship or authority to bind another Party.
- 18.2 No third party has a right to enforce this Agreement. A Party may nevertheless enforce its own rights concerning third-party Confidential Information it lawfully holds or is required to protect.

19 Notices

- 19.1 A notice under this Agreement shall be in English, identify this Agreement, and be delivered by hand, tracked courier or email to the address in Schedule 2. Email notice is effective when the sender receives no delivery-failure notice, provided that notices of termination, breach or legal proceedings are also sent by tracked courier within two business days.
- 19.2 A Party may update its notice details by notice. Operational security notices may be sent immediately to the security contact in Schedule 2 and need not await courier delivery.

20 Assignment and succession

- 20.1** Neither Party may assign, transfer or novate this Agreement without consent, except to an Affiliate or successor in a merger, reorganisation or sale of substantially all relevant business assets that is not a direct competitor of the other Party and assumes this Agreement in writing.
- 20.2** An assignment does not release the assigning Party from responsibility for a breach occurring before the assignment. Any prohibited assignment is ineffective to the extent permitted by Applicable Law.

21 Entire agreement and priority

- 21.1** This Agreement is the entire agreement on confidentiality and restricted use for the Purpose and supersedes prior discussions and understandings on that subject, while preserving rights accrued from earlier breaches.
- 21.2** A later written project agreement may supplement or replace this Agreement only if it expressly states the intended effect. For a direct conflict, the later specific term controls for that project; otherwise the obligations apply together.
- 21.3** Schedule 1 supplements this Agreement. A Schedule 1 restriction controls for its project where it expressly identifies the clause it varies; otherwise this Agreement controls.

22 General provisions

- 22.1** An amendment or waiver is effective only in writing and signed by authorised representatives. A delay or failure to exercise a right is not a waiver, and a waiver for one event is not a waiver for another.
- 22.2** If a provision is invalid or unenforceable, it shall be enforced to the maximum lawful extent and, where permitted, modified as little as necessary to make it enforceable while preserving its purpose. The remaining provisions continue in effect.
- 22.3** This Agreement does not prevent a Party from independently developing or acquiring products, services or relationships, provided it does not use Confidential Information or breach clause 12.

23 Governing law and disputes

- 23.1** This Agreement and any non-contractual obligation arising from it are governed by the laws of the Netherlands, excluding conflict-of-laws rules that would refer the matter to another law.
- 23.2** The courts of the Netherlands, District Court of Oost-Brabant, location 's-Hertogenbosch, have exclusive jurisdiction, except that a Party may seek urgent interim or protective relief in any court with jurisdiction over the person, information or assets concerned.
- 23.3** Before commencing ordinary merits proceedings, a Party shall give written notice of the dispute and allow ten business days for senior representatives to attempt resolution. This does not delay urgent relief, limitation periods or mandatory procedural steps.

24 Language counterparts and electronic signatures

- 24.1** This Agreement is executed in English. If translated, the English version controls to the extent permitted by Applicable Law.
- 24.2** The Parties may sign counterparts, each of which is an original and together form one instrument. Electronic signatures and exchanged signature pages are effective to the extent recognised by Applicable Law.

25 Execution

The authorised representatives below sign this Agreement on behalf of their respective Parties.

PARTENVOY	COUNTERPARTY
Legal name: Dániel Gergő Kis, trading as PartEnvoy	Legal name:
Name and title: Dániel Gergő Kis, proprietor	Name and title:
Signature:	Signature:
Date:	Date:

SCHEDULE 1 PROJECT AND HANDLING DETAILS

Complete this schedule when a project needs controls more specific than the main Agreement. A blank field does not reduce the protection in the main Agreement.

Project or RFQ reference	[INSERT]
Specific purpose	[INSERT OR STATE: AS DEFINED IN THE AGREEMENT]
Information categories	[DRAWINGS / CAD / PRICING / SUPPLIER IDENTITY / CUSTOMER IDENTITY / SAMPLES / OTHER]
Approved systems	[INSERT SECURE DATA ROOM, PORTAL OR TRANSFER METHOD]
Approved recipients	[INSERT NAMED TEAMS, AFFILIATES OR SUBCONTRACTORS]
Territory or transfer limits	[INSERT, IF ANY]
Special retention or destruction	[INSERT, IF ANY]
Other project-specific controls	[INSERT, INCLUDING EXPORT CLASSIFICATION OR CLEAN-TEAM RULES]

SCHEDULE 2 NOTICE AND SECURITY CONTACTS

DETAIL	PARTENVOY	COUNTERPARTY
Legal notice addressee	Dániel Gergő Kis, trading as PartEnvoy	[INSERT]
Postal address	Tongelresestraat 377, Eindhoven, Netherlands	[INSERT]
Notice email	contact@partenvoy.com	[INSERT]
Security contact	Dániel Gergő Kis	[INSERT]
Security email	notifications@partenvoy.com	[INSERT]
Telephone	+31 6 254 966 02	[INSERT]