Data Processing Agreement

Impact Flows — Impact Up

Version 1.0 | Effective Date: June 2026 | GDPR Article 28 Compliant

BETWEEN: IMPACT UP SAS, RCS Paris 931 751 507, 5 avenue du General Leclerc, 75014 Paris ("Processor")

AND: The Client Organisation identified in the Master Services Agreement ("Controller")

Preamble

This Data Processing Agreement (**"DPA"** or **"Agreement"**) is entered into pursuant to Article 28 of the General Data Protection Regulation (EU) 2016/679 (**"GDPR"**) between IMPACT UP SAS, acting as **Processor**, and the Client Organisation identified in the Master Services Agreement, acting as **Controller**.

This DPA forms part of, and is subject to, the Master Services Agreement (MSA) or General Terms and Conditions of Sale and Use (*CGVU*) governing the Client's use of the Impact Flows platform. In the event of conflict, this DPA prevails with respect to data protection matters.

The Parties have agreed to enter into this DPA to ensure that personal data processed by the Processor on behalf of the Controller is handled in accordance with applicable data protection law and in a manner that respects the rights of data subjects.

Article 1 — Definitions

For the purposes of this Agreement, the following definitions apply. Terms not defined herein have the meanings given in the GDPR.

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
Controller	The Client Organisation that determines the purposes and means of processing personal data through the Impact Flows platform.
Processor	IMPACT UP SAS, which processes personal data on behalf of the Controller.
Sub-processor	Any third party engaged by the Processor to carry out processing activities on behalf of the Controller, including Stripe and other technical sub-processors.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
Processing	Any operation performed on personal data, as defined in Article 4(2) GDPR.
Data Subject	The natural person to whom the personal data relates.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12) GDPR).
Services	The Impact Flows SaaS platform and related services provided under the MSA.
TOMs	Technical and Organisational Measures — security controls described in Annex II.
SCCs	Standard Contractual Clauses for international transfers adopted by the European Commission.

Article 2 — Subject Matter, Duration and Nature of Processing

2.1 Subject Matter

The Processor provides the Controller with access to the Impact Flows platform for the management of financial flows, donation mandates, fundraising campaigns, and associated operational data. In doing so, the Processor processes personal data on behalf of the Controller in accordance with the Controller's documented instructions.

2.2 Duration

This DPA takes effect on the date the Controller signs the MSA and remains in force for the duration of the Services. Upon termination, the Processor's obligations under this DPA continue to apply until all personal data has been returned or deleted in accordance with Article 11.

2.3 Nature of Processing

Processing operations carried out by the Processor on behalf of the Controller may include: collection, storage, structuring, retrieval, consultation, use, disclosure by transmission, erasure, and destruction of personal data, as necessary to deliver the Services.

Article 3 — Categories of Data and Data Subjects

3.1 Categories of Personal Data

The personal data processed under this DPA may include the following categories:

Category	Examples	Sensitivity
Identity & contact	Name, email, phone, professional title	Standard
KYC / identity documents	Passport, ID card, proof of address	High
Donor data	Donor name, contact details, donation pledge, payment method reference	High
Financial / payment	Tokenised payment references, IBAN (Stripe-held), transaction history	High
Operational / campaign	Mission details, fundraiser activity, team assignments, call records	Standard
Technical / logs	IP address, session tokens, authentication events, activity logs	Standard

Special categories of data (Article 9 GDPR): The Parties do not anticipate that any special categories of personal data will be processed under this DPA. The Controller shall not submit special category data to the platform without prior written agreement and implementation of additional safeguards.

3.2 Categories of Data Subjects

- Authorised users of the Controller (administrators, operators, team leaders);
- Fundraisers and teleactors employed or engaged by the Controller;

- Donors whose personal data is captured via digital donation forms;
- Individuals identified during KYC/AML verification.

Article 4 — Obligations of the Controller

The Controller represents, warrants and undertakes that:

- It has a valid legal basis (as defined in Articles 6 and, where applicable, 9 GDPR) for all processing activities instructed to the Processor;
- It has provided data subjects with appropriate privacy information regarding the processing of their personal data, including use of the Impact Flows platform;
- All instructions given to the Processor comply with applicable data protection law;
- It will promptly notify the Processor of any change in applicable requirements that may affect the Processor's obligations under this DPA;
- It has implemented appropriate internal policies and controls to ensure lawful processing;
- It is solely responsible for the accuracy, legality, and appropriateness of the personal data it submits to the platform.

Article 5 — Obligations of the Processor

5.1 Processing on Instructions Only

The Processor shall process personal data only on documented instructions from the Controller, including with regard to international transfers, unless required to do so by Union or Member State law. In such case, the Processor shall inform the Controller of that legal requirement before processing, unless prohibited by law on grounds of public interest. This DPA and the MSA constitute the Controller's documented instructions.

5.2 Confidentiality

The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to personal data is limited to personnel who need access for the purposes described in this DPA.

5.3 Security

The Processor shall implement and maintain the Technical and Organisational Measures (TOMs) set out in Annex II. These measures shall take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5.4 Sub-processors

The Controller hereby grants the Processor general written authorisation to engage sub-processors, subject to the conditions set out in Article 6. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

5.5 Assistance with Data Subject Rights

The Processor shall assist the Controller in fulfilling its obligations to respond to requests from data subjects exercising their rights under Chapter III GDPR (access, rectification, erasure, restriction, portability, objection), taking into account the nature of the processing. Such assistance shall be provided within 5 business days of the Controller's request.

5.6 Assistance with Compliance Obligations

The Processor shall assist the Controller in ensuring compliance with obligations under Articles 32–36 GDPR, including security obligations, breach notification, data protection impact assessments (DPIAs), and prior consultations with supervisory authorities.

5.7 Return and Deletion

At the choice of the Controller, the Processor shall, upon termination of the Services, delete or return all personal data to the Controller and delete existing copies, unless Union or Member State law requires storage. The Controller has a data export window of 12 months post-termination. After this period, data is securely deleted or archived subject to mandatory legal retention obligations.

5.8 Audit & Information

The Processor shall make available to the Controller all information necessary to demonstrate compliance with this Article, and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to reasonable notice (minimum 30 days) and confidentiality obligations. The Processor may charge reasonable costs for such assistance.

Article 6 — Sub-processors

The Processor maintains a list of approved sub-processors (**Annex I**). The Controller has reviewed and approved the sub-processors listed at the date of this DPA.

6.1 New Sub-processors

The Processor shall notify the Controller of any intended changes to sub-processors (additions or replacements) with at least **30 days' advance notice**. The Controller may object to such changes within 14 days of notification on reasonable data protection grounds by written notice. Where the Processor cannot accommodate the Controller's objection and the Parties cannot agree, either Party may terminate the relevant Services on written notice.

6.2 Sub-processor Obligations

The Processor shall impose, by written contract, the same data protection obligations as set out in this DPA on any sub-processor it engages. Where a sub-processor fails to fulfil its obligations, the Processor remains fully liable to the Controller.

Sub-processor	Role / Service	Location
Stripe Payments Europe, Ltd.	Payment processing, tokenisation, mandate management	EU / Ireland (PCI-DSS)
Cloud hosting provider	Infrastructure hosting (servers, databases)	EU / EEA
Email delivery provider	Transactional email notifications	EU / EEA

Sub-processor	Role / Service	Location
KYC / identity verification provider	Document verification for AML onboarding	EU / EEA

Full and current sub-processor list available on request: privacy@impactup.io

Article 7 — International Data Transfers

The Processor shall not transfer personal data to any country outside the EEA without ensuring that an adequate level of protection exists, using one of the following mechanisms:

- A European Commission adequacy decision for the destination country (Article 45 GDPR);
- Standard Contractual Clauses (SCCs) as adopted by the European Commission (Article 46(2)(c));
- Binding Corporate Rules (Article 47 GDPR), where applicable;
- Any other appropriate safeguard permitted under Article 46 GDPR.

The Processor shall document all international transfers and make records available to the Controller on request. Where SCCs apply, the Processor shall provide copies to the Controller upon request.

Article 8 — Personal Data Breach Notification

The Processor shall notify the Controller of any Personal Data Breach affecting the Controller's personal data without undue delay and, where feasible, **within 24 hours** of becoming aware of such a breach.

The notification shall include, to the extent available at the time of notification:

- A description of the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned;
- The name and contact details of the data protection officer or other contact point;
- The likely consequences of the breach;
- Measures taken or proposed to address the breach, including to mitigate its possible adverse effects.

Where not all information is available at the time of initial notification, the Processor shall provide additional information as it becomes available. The Processor shall document all breaches, including those not subject to notification obligations.

The Controller is solely responsible for notifying the competent supervisory authority (CNIL or equivalent) and affected data subjects in accordance with Articles 33 and 34 GDPR. The Processor shall provide reasonable assistance with such notifications upon request.

Article 9 — Data Protection Impact Assessments

Where a Data Protection Impact Assessment (DPIA) under Article 35 GDPR is required in connection with processing carried out by the Processor on behalf of the Controller, the Processor shall provide reasonable assistance, including by making available relevant information about the processing operations and applicable TOMs.

The Processor shall also assist the Controller with any prior consultation with a supervisory authority required under Article 36 GDPR.

Article 10 — Records of Processing Activities

The Processor shall maintain records of processing activities carried out on behalf of the Controller, as required under Article 30(2) GDPR. Such records shall include the name and contact details of the Processor, categories of processing, international transfers, and a general description of the TOMs in place.

Records shall be made available to the Controller and competent supervisory authorities on request.

Article 11 — Return and Deletion of Personal Data

Upon termination of the Services, and at the written request of the Controller, the Processor shall:

- Provide the Controller with a data export in a structured, commonly used format within the 12-month post-termination window;
- Securely delete all personal data after the export window, except where retention is required by applicable law (including AML, payment services, and tax regulations);
- Certify in writing to the Controller that deletion has been completed.

Mandatory retention periods under French and EU law (e.g., minimum 5 years for financial and AML records) prevail. Data retained for legal purposes is isolated from active processing and accessed only when legally required.

Article 12 — Liability

Each Party shall be liable for any damage caused to data subjects as a result of its failure to comply with the GDPR and this DPA, in accordance with the liability provisions of Article 82 GDPR.

The Processor's total aggregate liability under or in connection with this DPA shall be subject to the limitations set out in the MSA, except to the extent that applicable law prohibits such limitation.

Where the Processor has acted in breach of its obligations under this DPA, it shall be liable for any damage caused. Where a fine is imposed on the Controller by a supervisory authority due to the Processor's breach of this DPA, the Processor shall indemnify the Controller for the portion attributable to the Processor's actions or omissions, subject to the liability cap.

Article 13 — Governing Law and Jurisdiction

This DPA shall be governed by and construed in accordance with the laws of France, without prejudice to the mandatory provisions of the GDPR and any applicable Member State laws implementing the GDPR.

Any dispute arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of Paris, France, unless otherwise agreed in writing by the Parties.

Article 14 — Amendments and Updates

The Processor may amend this DPA from time to time to reflect changes in applicable law, supervisory guidance, or the Processor's processing activities. Material amendments will be notified to the Controller with at least 30 days' advance notice. Continued use of the Services after the effective date of amendments constitutes acceptance.

Where amendments are required to reflect changes mandated by law or regulatory guidance (e.g., new SCCs), they take effect on the legally required date without the need for separate agreement, provided the Processor gives reasonable notice.

Annex I — Approved Sub-processors

The following sub-processors are approved as of the effective date of this DPA. The Processor will notify the Controller of any changes in accordance with Article 6.

Sub-processor	Role	Location	Transfer Mechanism	Data Categories
Stripe Payments Europe, Ltd.	Payment processing, tokenisation, SEPA mandates, fraud detection	Ireland (EU)	Adequacy (EEA internal)	Payment, financial, identity
Cloud infrastructure (e.g., AWS / GCP EU)	Application hosting, database, object storage	EU / EEA	EEA internal	All categories
Email delivery provider	Transactional email (notifications, alerts, support)	EU / EEA	EEA internal	Identity, contact
KYC / AML verification provider	Identity document verification, watchlist screening	EU / EEA	EEA internal / SCCs	KYC / identity documents
Monitoring / observability provider	Application performance monitoring, error tracking	EU / EEA	EEA internal	Technical / logs

Annex II — Technical and Organisational Measures (TOMs)

The Processor implements the following TOMs, consistent with Article 32 GDPR and the Impact Flows Security Policy (v1.0):

Control Area	Measures Implemented
Access Control	Role-based access control (RBAC); least-privilege principle; unique named accounts; no shared credentials; mandatory MFA for all financial accounts.
Authentication	Mandatory multi-factor authentication (MFA/TOTP) for Impact Flows; strong password policy; account lockout after repeated failed attempts; session expiry.
Encryption in Transit	TLS 1.2+ enforced for all data in transit between client and server; HTTPS-only access; no plaintext transmission of sensitive data.
Encryption at Rest	Databases and object storage encrypted at rest using AES-256 or equivalent; encryption keys managed via secure key management service.
Payment Data Security	No storage of raw card numbers, CVV, or sensitive authentication data; tokenisation via Stripe (PCI-DSS Level 1 certified); SEPA mandate data held by Stripe.
Audit Logging	Comprehensive activity logging (authentication, data access, exports, payment events); logs retained for minimum 12 months; access to logs restricted to authorised personnel.
Vulnerability Management	Formalised vulnerability management programme; critical vulnerabilities remediated within 24–72 hours; regular security reviews and dependency scanning.
Incident Response	Documented incident response procedure; 24-hour breach notification to Controller; CISO/DPO oversight; post-incident review and remediation.
Business Continuity	Regular data backups with tested restoration procedures; service availability target 99% p.a.; disaster recovery planning; failover capability.
Vendor Security	Sub-processors assessed for security posture; contractual security obligations imposed; PCI-DSS compliance required for payment sub-processors.
Physical Security	Data centres operated by ISO 27001 / SOC 2 certified providers with physical access controls.
Data Minimisation	Collection limited to data strictly necessary for the stated purpose; periodic review of data held; pseudonymisation where technically feasible.
Personnel	Confidentiality obligations for all staff handling personal data; data protection training; background checks for personnel with access to sensitive data.

Signatures

IN WITNESS WHEREOF, the duly authorised representatives of the Parties have executed this Data Processing Agreement as of the date last signed below.

FOR THE CONTROLLER	FOR THE PROCESSOR — IMPACT UP SAS
Organisation name:	IMPACT UP SAS
Name & Title: _____	Name & Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

Please initial each page. Write "Read and approved" above your signature. Two (2) original copies to be executed — one for each Party.