Privacy Policy

Impact Flows — Impact Up

Version 1.0 | Effective Date: June 2026 | IMPACT UP SAS — RCS Paris 931 751 507

1. Introduction

IMPACT UP SAS (**"Impact Up"**, **"we"**, **"us"**, or **"our"**) is committed to protecting the personal data of all individuals who interact with our services. This Privacy Policy describes how we collect, use, store, share, and protect personal data in connection with the **Impact Flows** platform — a SaaS solution designed for non-profit organisations (NGOs), associations, and fundraising operators to manage and monitor their financial flows, donation mandates, and payment operations.

This Policy is issued in accordance with the General Data Protection Regulation (EU) 2016/679 (**"GDPR"**), the French Data Protection Act (*Loi Informatique et Libertés* as amended), and applicable payment services regulations.

By accessing or using Impact Flows, you acknowledge that you have read and understood this Privacy Policy. If you are acting on behalf of an organisation, you confirm that you are authorised to do so and that the organisation accepts this Policy.

2. Data Controller

For the purposes of the GDPR, the data controller in respect of personal data processed directly by Impact Up for its own purposes is:

Legal name	IMPACT UP SAS
Registration	RCS Paris — SIRET 931 751 507
Registered address	5 avenue du Général Leclerc, 75014 Paris, France
Capital	€100.00
Contact email	support-flows@impactup.io
DPO / Privacy contact	privacy@impactup.io (or via the above address)

Where Impact Up processes personal data on behalf of a client organisation acting as data controller, such processing is governed by the Data Processing Agreement (DPA) entered into between the parties, consistent with Article 28 GDPR.

3. Scope of this Policy

This Privacy Policy applies to personal data processed in connection with:

- The Impact Flows web application (*https://impactflows.io*) and associated APIs;
- Account registration, onboarding and KYC verification processes;
- Payment processing, transaction management, and mandate handling via Stripe;
- Technical support, communications and contractual administration;
- Security monitoring, incident management, and fraud prevention.

It applies to all natural persons whose data is processed, including: authorised users of client organisations (NGO administrators, operators), fundraisers and team leaders, donors whose data is captured via donation forms, and contacts of Impact Up.

4. Categories of Personal Data Collected

4.1 Account & Identity Data

- Full name, professional email address, job title and organisation name;
- Identity documents submitted for KYC verification (government-issued ID, proof of address);
- Digital signatures and acceptance timestamps for contractual purposes.

4.2 Payment & Financial Data

- Tokenised payment instrument references (handled by Stripe — raw card numbers and CVV are **never stored** by Impact Up);
- Bank account details (IBAN/BIC) transmitted to Stripe for mandate creation;
- Transaction identifiers, amounts, dates, statuses, and audit trails;
- Mandate and recurring donation records.

4.3 Donor Data (processed as Processor)

- First name, last name, contact details, donation pledge details captured via digital forms;
- Welcome-call and callback records where applicable.

Note: Impact Up processes donor personal data strictly as a data processor on behalf of the client NGO or operator acting as data controller. The applicable processing rules are set out in the DPA.

4.4 Technical & Usage Data

- IP addresses, browser type, operating system, device identifiers;
- Session tokens, login events, authentication logs;
- Application activity logs (page views, exports, form submissions, payment operations);
- Cookies and analytics data (see Section 9).

4.5 Communications Data

- Email correspondence and support ticket content;
- In-app notifications and activity logs.

5. Purposes and Legal Bases for Processing

The table below sets out each processing activity, its purpose, and the applicable GDPR legal basis.

Processing Activity	Purpose	Legal Basis	Retention
Account creation & KYC	Identity verification; regulatory onboarding (AML/CFT)	Art. 6(1)(b) — contract; Art. 6(1)(c) — legal obligation	Duration of contract + 5 years

Processing Activity	Purpose	Legal Basis	Retention
Service delivery	Providing Impact Flows platform, dashboards, payment management	Art. 6(1)(b) — contract performance	Duration of contract + 12 months
Payment processing	Processing donations, mandates, recurring transactions via Stripe	Art. 6(1)(b) — contract; Art. 6(1)(c) — legal obligation	5 years (payment law)
Fraud & AML monitoring	Detecting fraud, money laundering, terrorism financing (TRACFIN obligations)	Art. 6(1)(c) — legal obligation; Art. 6(1)(f) — legitimate interest	5 years minimum
Security & access logging	System security, intrusion detection, incident response	Art. 6(1)(f) — legitimate interest	12 months rolling
Technical support	Responding to support tickets, resolving incidents	Art. 6(1)(b) — contract; Art. 6(1)(f) — legitimate interest	3 years
Legal & compliance	Defending rights, litigation, regulatory audits	Art. 6(1)(c) — legal obligation; Art. 6(1)(f) — legitimate interest	As required by law
Analytics & improvement	Aggregated usage statistics for platform improvement	Art. 6(1)(f) — legitimate interest (anonymised where possible)	24 months

Where Impact Up processes personal data as a data **processor** on behalf of a client organisation, the legal basis for such processing is determined by the controller and set out in the applicable DPA.

6. Sharing of Personal Data & Sub-processors

Impact Up does not sell personal data. We may share personal data with the following categories of recipients:

6.1 Authorised Sub-processors

Stripe (Stripe Payments Europe, Ltd.)	Payment processing, tokenisation, mandate management. Stripe is PCI-DSS certified. Data transferred under EU Standard Contractual Clauses. Privacy: https://stripe.com/privacy
Cloud infrastructure provider	Hosting of application servers and databases within the EU/EEA.
Email delivery provider	Transactional emails (account notifications, support responses).
Identity / KYC verification service	Document verification required under AML obligations.

An up-to-date list of sub-processors is available upon written request to privacy@impactup.io. Clients are notified of material changes to sub-processors in accordance with the DPA.

6.2 Legal & Regulatory Authorities

As a payment agent subject to AML/CFT regulations, Impact Up is required by law to report suspicious transactions to competent authorities including TRACFIN. In such cases, only the minimum necessary information is disclosed. Associated funds may be frozen pending investigation.

6.3 Business Transfers

In the event of a merger, acquisition, or sale of assets, personal data may be transferred as part of the transaction. We will notify affected parties as required by applicable law.

7. International Data Transfers

Impact Up primarily processes personal data within the European Economic Area (EEA). Where personal data is transferred to a third country outside the EEA (e.g., via Stripe's global infrastructure or other sub-processors), such transfers are subject to appropriate safeguards in accordance with GDPR Chapter V, including:

- European Commission adequacy decisions;
- Standard Contractual Clauses (SCCs) as approved by the European Commission;
- Binding Corporate Rules (BCRs) where applicable.

Details of applicable safeguards are available upon request from privacy@impactup.io.

8. Data Retention

Personal data is retained only for as long as necessary for the purposes described in this Policy, or as required by applicable law. Key retention periods are:

- **Active accounts:** for the duration of the contractual relationship;
- **Post-termination export window:** 12 months after contract end (client data export);
- **Financial transaction records:** minimum 5 years (payment services law, AML);
- **KYC/identity documents:** minimum 5 years after relationship end;
- **Security & audit logs:** 12 months rolling;
- **Support communications:** 3 years from closure;
- **Legal evidence / litigation hold:** until final resolution.

After the retention period, data is securely deleted or anonymised. Certain transaction and activity logs may be retained beyond these periods where required by banking, payment, or anti-fraud regulations.

9. Cookies and Tracking Technologies

The Impact Flows web application uses cookies and similar tracking technologies for the following purposes:

Strictly necessary cookies	Session management, authentication tokens (MFA), CSRF protection. These cannot be disabled — they are essential for security.

Analytics cookies	Aggregated usage statistics to improve platform performance. No data is shared with third-party advertising networks.
Preference cookies	Storing user interface preferences (language, display settings).

Non-essential cookies are only placed with your consent. You may manage cookie preferences via the cookie banner presented on first login, or by contacting us. Analytics data is used solely for service improvement and is not sold or shared with third parties for commercial purposes.

10. Your Rights Under the GDPR

Subject to applicable law and the conditions set out in the GDPR, you have the following rights in relation to your personal data:

Right of access (Art. 15)	Request a copy of all personal data held about you. We respond within 14 business days.
Right to rectification (Art. 16)	Request correction of inaccurate or incomplete personal data.
Right to erasure (Art. 17)	Request deletion of personal data, subject to legal retention obligations.
Right to restriction (Art. 18)	Request that we restrict processing in certain circumstances.
Right to data portability (Art. 20)	Receive your personal data in a structured, machine-readable format.
Right to object (Art. 21)	Object to processing based on legitimate interests or for direct marketing.
Right not to be subject to automated decisions (Art. 22)	Not to be subject to solely automated decisions with significant legal effects.
Right to withdraw consent	Where processing is based on consent, withdraw it at any time without affecting prior lawful processing.

To exercise any of these rights, submit a written request to: **privacy@impactup.io**. We may verify your identity before processing the request. If you are dissatisfied with our response, you have the right to lodge a complaint with the French supervisory authority: **CNIL — Commission Nationale de l'Informatique et des Libertés**, 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07 — www.cnil.fr.

11. Security Measures

Impact Up implements technical and organisational security measures appropriate to the risk, including:

- Mandatory multi-factor authentication (MFA) for all Impact Flows accounts;
- Encryption of data in transit (TLS 1.2+) and at rest;
- Tokenisation of payment data via Stripe (PCI-DSS compliant);
- Role-based access control (RBAC) with least-privilege principle;
- Continuous activity logging, anomaly detection, and audit trails;
- Formal vulnerability management and patching programme (see Security Policy v1.0);
- Incident response procedures including breach notification obligations;

- Regular security reviews and, where applicable, CISO/DPO oversight.

Despite these measures, no system is entirely immune to security risks. Users are responsible for maintaining the security of their own credentials and devices in accordance with our Security Policy.

12. Children's Data

Impact Flows is intended solely for use by professionals and organisations. We do not knowingly collect personal data from individuals under the age of 18. If you believe that a minor's data has been submitted to our platform, please contact us immediately at privacy@impactup.io.

13. Updates to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our services, legal obligations, or regulatory requirements. The current version is always accessible within the Impact Flows application. Material changes will be communicated to registered users by email or in-app notification at least 30 days before taking effect, unless a shorter notice period is required by law.

14. Contact & DPO

For any questions, requests, or complaints relating to this Privacy Policy or to the processing of your personal data, please contact:

Privacy / DPO contact	privacy@impactup.io
Support	support-flows@impactup.io
Postal address	IMPACT UP SAS — Data Privacy 5 avenue du Général Leclerc 75014 Paris, France
Supervisory authority	CNIL — www.cnil.fr

15. Acknowledgement

By signing below, the authorised representative of the Client Organisation acknowledges having read and accepted the terms of this Privacy Policy on behalf of their organisation.

Date:	____	**Location:**	_______________________________________
Name & Title:	____		
Signature:			

Please initial each page and write "Read and approved" followed by your signature on this page.