DATA PROTECTION & PRIVACY POLICY

PaperWorks Online Ltd.

Version 1.0 – 24 December 2025

Owner / DPO: Michael Byrne (CEO)

Next review: 24 June 2026

1. PURPOSE & SCOPE

This policy sets out how PaperWorks Online Ltd. ("we", "our", "us") meets our obligations under:

- Regulation (EU) 2016/679 (GDPR)
- Irish Data Protection Act 2018
- ePrivacy Directive 2002/58/EC (as amended) – cookie rules
- PCI DSS v4.0 (for payment-card data)

It applies to all personal data processed in connection with our on-line stationery shop, customer services, marketing, HR, finance and any third-party suppliers who touch that data.

2. DEFINITIONS

"Personal data" – any information relating to an identified or identifiable natural person.

"Processing" – collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, erasure or destruction.

"Special-category data" – not intentionally processed; if accidentally received will be immediately deleted.

3. DATA PROTECTION PRINCIPLES (Art. 5 GDPR)

We adopt the six core principles and the accountability obligation:

1. Lawfulness, fairness & transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity & confidentiality (security)

- Accountability – we must demonstrate compliance.

4. LAWFUL BASES WE RELY ON

TableCopy

Activity	**Lawful basis**	**Legitimate-interest rationale (where used)**
Selling & delivering products	Contract	N/A
Sending order / shipping e-mails	Contract	N/A
Keeping accounting records	Legal obligation (Irish Companies Act)	N/A
Fraud prevention & charge-backs	Legitimate interest	Protect business from financial loss
Abandoned-cart e-mail (≤ 2 reminders)	Legitimate interest	Recover lost sales (minimal privacy impact)

Website analytics (Google Analytics 4, anonymised IPs)	Consent (cookie banner)	N/A
Marketing newsletters	Consent (double opt-in)	N/A

5. WHAT DATA WE COLLECT

Customers / prospects

- Identity: name, billing/shipping address, phone, e-mail
- Payment: card brand & last-4 digits only (full PAN never stored) – processing via PCI-validated gateway (Stripe)
- Transaction: products, quantities, prices, discounts, VAT, timestamps
- Technical: IP, device type, browser, cookies (see § 14)
- Marketing: preferences, click-through logs

Suppliers / couriers

- Contact names, bank details (for payment), VAT numbers

Employees / job applicants

- CV, payroll, tax info, performance reviews – covered separately in HR Security Policy.

6. HOW WE COLLECT

- Direct: order checkout, account creation, contact form, phone, competition entry
- Automated: cookies, server logs, Shopify & Stripe dashboards
- Third parties: An Post dispatch API (tracking), Google (Analytics), Facebook (pixel only after consent).

7. PURPOSE & RETENTION

TableCopy

Purpose	Retention	Trigger for deletion
Sales contract fulfilment	7 yrs (Irish Revenue rule)	+7 yrs after last invoice
Marketing consent	Until user unsubscribes or 2 yrs inactivity	Unsubscribe link / e-mail request
Cookies	See § 14	Browser settings / cookie banner
CCTV (office entrance)	30 days	Auto-overwrite
Job applicant CVs	6 months if not hired	Date of rejection

Data is deleted or anonymised on schedule; backups expire after 90 days.

8. DATA SUBJECT RIGHTS (Art. 12-22)

Everyone may:

- Access – receive copy of personal data
- Rectification – correct inaccurate data
- Erasure – “right to be forgotten” (not where legal retention applies)
- Restrict processing – temporary freeze
- Data portability – CSV export of orders/account data
- Object – to legitimate-interest processing
- Withdraw consent – at any time (does not affect prior lawfulness)
- Lodge complaint – with Irish Data Protection Commission (DPC)

How to exercise: e-mail privacy@paperworks.ie or use the “Download my data” / Delete account” buttons in customer portal. We respond within 30 days (extendable by 2 months for complex requests). No fee unless manifestly unfounded.

9. CHILDREN

We do not knowingly sell to under-13s. If we discover such an account we will delete it.

10. SECURITY OF PROCESSING (Art. 32)

- HTTPS/TLS 1.3 everywhere (A+ SSL Labs rating)
- Database encrypted at rest (AES-256) – keys in cloud KMS
- Unique accounts + MFA for all staff (see Access Control Policy)
- Annual penetration test & quarterly vulnerability scans
- Pseudonymised order IDs in logs; full card data never logged
- Incident-response plan & 72-h breach notification to DPC where risk to rights is likely
- Processor agreements (Art. 28) with every sub-processor – list maintained in “Processor Register”.

11. INTERNATIONAL TRANSFERS

Primary data stays in EU (Dublin AWS region). Where US processors are used (Google, Stripe, Mailchimp) we rely on:

- Commission Implementing Decision 2021/914 – EU Standard Contractual Clauses (SCCs) – Module 2 (controller-processor) or Module 3 (processor-processor) as applicable, plus Transfer-Impact-Assessment (TIA) on file .
  No data is stored in jurisdictions without adequacy or SCCs.

12. SHARING & DISCLOSURE

We never sell personal data. Recipients:

- Stripe – payment processing
- An Post / DPD – delivery

- Google (Analytics) – website stats (IP anonymised)
- Mailchimp – e-mail marketing (only after consent)
- Accountant & auditor – statutory accounts (NDA)
- Law-enforcement – when legally compelled (warrant)

All third parties are vetted for security & privacy compliance.

13. PRIVACY BY DESIGN / DEFAULT

- Collect only fields required to complete checkout (no optional “title”, “date-of-birth”).
- Default opt-in is “NO” for marketing; pre-ticked boxes forbidden.
- New features undergo DPIA-lite checklist; full DPIA performed if high-risk profiling.

14. COOKIES & SIMILAR TECHNOLOGIES

Essential cookies (basket, session, CSRF) – no consent needed.

Analytical / Marketing cookies – deployed only after active consent via banner (granular on/off).

Cookie list & lifespan displayed; withdrawal mechanism always visible.

ePrivacy consent logged (timestamp, IP hashed).

15. DATA BREACH MANAGEMENT

- Internal escalation within 4 h of discovery
- DPC notification ≤ 72 h where risk to rights is likely (Art. 33)
- Customer notification without undue delay if high risk (Art. 34)
- Template e-mails & decision tree in Incident Response Policy
- Post-incident review & root-cause report stored 3 yrs

16. RECORDS OF PROCESSING ACTIVITIES (Art. 30)

Maintained in Google Sheet “RoPA” containing: processing activity, purposes, categories, data subjects, recipients, retention, technical measures, DPIA status. Updated quarterly.

17. TRAINING & AWARENESS

- All staff complete GDPR & PCI fundamentals at induction
- Annual refresher quiz (pass 80 %)
- Records kept 3 yrs for audit

18. CONTACT DETAILS

Data Protection Officer (DPO) – Michael Byrne (non-mandatory under GDPR but appointed for accountability)

E-mail: privacy@paperworks.ie

Postal: PaperWorks Online Ltd., 123 Stationery Ave, Dublin 8, Ireland

You may also contact the Irish Data Protection Commission: info@dataprotection.ie

19. CHANGES TO THIS POLICY

Any material change (e.g. new processor, purpose) will be:

- Uploaded to website with new version number & “last updated” date
- E-mailed to active customers and/or highlighted in newsletter

20. DOCUMENT CONTROL

Owner: Michael Byrne (acting DPO)

Location: …/ISMS/POL-05-Data-Protection-Privacy.pdf

Public mirror: https://paperworks.ie/privacy-policy

Related docs:

- Cookie Policy (subset)
- Processor Register (Annex A)
- DPIA templates (Annex B)
- Incident Response Policy