Security & Data Protection Overview

Effective Date: [08/01/2025]
Last Updated: [10/07/2025]

At **No Gifts Please, Inc.**, keeping your data safe isn't a box we check — it's the foundation of how we operate.
Every contribution, photo upload, and registry detail is protected by bank-level security and industry-standard encryption.

This Security & Data Protection Overview ("**Overview**") explains how we safeguard your information, how payments are protected, and what to do if something doesn't look right.

---

1. Payment Encryption

All payments on No Gifts Please are handled through **Stripe Connect**, one of the world's most trusted payment processors.

- Every transaction uses **TLS (Transport Layer Security)** encryption — the same standard banks and Fortune 500 companies use.
- Payment details (credit and debit card numbers) are **never seen, stored, or transmitted** by No Gifts Please. They go directly from your browser to Stripe's encrypted servers.
- Stripe is **PCI Level 1 Compliant**, the highest level of payment security certification available.

When you see "https://" in our URL, it means your connection is secure. Always make sure that padlock icon appears before entering payment information.

---

2. Account Verification & Stripe Connect

All Registry Owners must verify their identity through **Stripe Connect** before receiving payouts. This verification process:

- Confirms the registry is linked to a real person (not a fake or fraudulent account).
- Requires accurate personal and banking information.
- Helps prevent money laundering, fraud, and identity misuse.

Stripe handles all verification data directly and stores it securely.
No Gifts Please does **not** have access to your banking credentials, Social Security number, or payout details.

---

3. Secure Infrastructure

Our website and database are hosted through **Framer**, **Softr**, and **Airtable**, which use enterprise-grade encryption and access controls.

- All communication between your browser and our servers is **protected by SSL (Secure Sockets Layer)**.
- Data stored in our systems is **encrypted at rest** and accessible only to authorized No Gifts Please personnel who require it for operational purposes.
- Backups are maintained securely and automatically purged according to our retention policy.

We also use **firewall protections**, **limited access permissions**, and **multi-factor authentication** for internal systems.

---

4. Limited Data Retention

We keep only the data necessary to provide our service — nothing more.

- Registry data (names, event info, photos) is retained for up to **12 months after registry closure**, then securely deleted or anonymized.
- Payment data is stored exclusively by Stripe and subject to its retention policies.
- Support correspondence and logs are kept for a limited period (typically ≤ 24 months) for quality and fraud-prevention purposes.

When data is no longer needed, it’s permanently erased from our systems.

---

5. Monitoring & Threat Prevention

Our systems automatically monitor for unusual patterns, such as:

- Abnormal contribution amounts or rapid payment activity
- Repeated failed login attempts

- Suspicious registry duplication or impersonation

When anomalies are detected, we review them manually and may:

- Temporarily freeze the account
- Request additional verification
- Notify affected users

We also work directly with **Stripe's fraud-prevention team** to block suspicious transactions in real time.

---

6. Reporting Suspicious Activity

If something seems off — a strange email, an unfamiliar charge, or an unexpected payout — tell us immediately.

✉ **info@nogiftsplease.com**
Please include:

- Your name and registry link
- A description of what seems suspicious
- Screenshots or relevant emails if available

We investigate all reports within **24–48 hours** and coordinate with Stripe if necessary.

If you ever receive an email claiming to be from No Gifts Please but you're unsure, **do not click any links**. Forward it to us, and we'll confirm whether it's legitimate.

---

7. User Best Practices

Security is a partnership. Here are a few ways you can help protect your account:

- Use a **strong, unique password** for your registry dashboard.
- Never share your login credentials.
- Log out after using a shared or public device.
- Keep your browser and operating system updated.
- Verify that any Stripe communications come from **@stripe.com**.

A little caution goes a long way.

---

8. Legal & Regulatory Compliance

No Gifts Please complies with:

- **PCI-DSS** (Payment Card Industry Data Security Standard) requirements via Stripe.
- **GDPR (General Data Protection Regulation)** and **CCPA (California Consumer Privacy Act)** principles for transparency and user rights.
- Applicable U.S. and international data-protection laws regarding secure handling and deletion.

We also review our practices annually to maintain compliance and strengthen safeguards.

---

9. Incident Response

In the unlikely event of a data breach or security incident, we will:

1. Notify affected users promptly via email.
2. Coordinate with Stripe and hosting providers to contain the issue.
3. Cooperate with relevant authorities if required by law.
4. Review and improve internal systems to prevent recurrence.

Your trust is our top priority, and transparency is part of that trust.

---

10. Contact & Support

If you have questions about this Overview or any security matter:
✉ **info@nogiftsplease.com**
🌐 www.nogiftsplease.com
🎗 **No Gifts Please, Inc.**
[731 E Broad St. Columbus, Ohio 43205]

We're here to help and typically respond within **one business day**.