Kadonation NV | Gordunakaai 61, 9000 Gent
BTW BE-0666.820.362
E: contact@kadonation.com

RESPONSIBLE DISCLOSURE POLICY – KADONATION NV

Classification: Public / Last version: 04/08/2026 / Last updated: 04/08/2026 / Last reviewed: 04/08/2026

Thank you! We're grateful to the security researchers who help us keep our gifting platform safe. If you've found a vulnerability, this policy explains how to report it to us responsibly — and what you can expect from us in return.

1 OUR PROGRAMME

At Kadonation, keeping our platform safe and reliable is a priority. We adhere to the **ISO 27001** standard for information security, and we value the role security researchers play in helping us reduce cyber risk. If you believe you have discovered a potential cyber threat or security issue affecting the confidentiality, integrity or availability of Kadonation's information, systems or services (a "**vulnerability**"), please report it to our team using the method below. To protect our customers, we treat all information about a vulnerability as confidential, and we ask you not to publicly disclose, discuss or confirm the details of any potential security issue until we have investigated and resolved it.

2 RULES OF ENGAGEMENT

We encourage security research into our products and services. To keep everyone safe, and to keep you within the protection of Belgian law (see below), please keep your testing **necessary and proportionate**: limit it to what is strictly needed to find and demonstrate a vulnerability, and stop as soon as you have done so.

What you may do (if proportionate)

- Investigate and demonstrate a vulnerability using access strictly limited to what is necessary to prove it.
- If, while doing so, you incidentally encounter personal data or confidential information: stop immediately, do not view more than needed, do not copy or store it, and tell us in your report.
- Test only your own account(s) or accounts you have explicit permission to use, wherever possible.

What is strictly prohibited

- Going beyond what is necessary and proportionate to find and demonstrate the vulnerability.
- Modifying, deleting or destroying any data, or attempting to do so.
- Copying, retaining, disclosing or using Kadonation data beyond the minimum needed to demonstrate the issue.
- Denial-of-service (DoS/DDoS), volumetric or resource-exhaustion testing, or anything that disrupts the availability of our services.
- Social engineering (including phishing) of Kadonation employees, contractors, customers or other related parties.
- Posting, transmitting, uploading, linking to, sending or storing malware that could affect our services, products or customers.
- Sending unsolicited or unauthorised e-mail or other messages via our systems.
- Publicly disclosing, discussing or confirming a vulnerability before we have resolved it and agreed to disclosure (see "The Belgian legal framework" below).

Kadonation does not waive any rights or claims in respect of activities that fall outside these rules of engagement or outside the protection of Belgian law.

Out of scope (we may not action these)

The following are generally not eligible for recognition unless you can demonstrate a concrete, exploitable impact:

- Reports of weak or insecure SSL/TLS ciphers or certificates without a demonstrated exploit.
- Clickjacking without a demonstrated security impact.
- Output from automated scanners without a working proof of concept.
- Third-party services, platforms or infrastructure we do not control.

3 REPORTING A SECURITY ISSUE

You can responsibly report a potential vulnerability to the Kadonation team by e-mailing compliance@kadonation.com. To help us investigate your report, please follow this structure:

- The affected product or service, including the affected URL(s).
- Your name and contact details (if you prefer not to share personal data, you may contact us anonymously or under a pseudonym).
- The date, time and time zone on which the potential vulnerability was discovered.
- The IP address used when the potential vulnerability was discovered.
- Steps to reproduce the issue, and its potential impact.

You may submit your report in **Dutch, French or English**.

4 NEXT STEPS

After you submit your report, you will receive confirmation of receipt within **5 business days**. We will use the information you provide to improve the security of our systems. We may also use it in notifications to regulatory authorities, to comply with the law, or to assist government or law-enforcement bodies. Once the issue has been resolved, we will **communicate publicly** about the nature of the vulnerability and the measures taken.

5 THE BELGIAN LEGAL FRAMEWORK

Because Kadonation is a Belgian company, you are also protected by Belgian law. Independently of this policy, the **Law of 26 April 2024 ("NIS2 Law", art. 22–23)** allows any person acting without fraudulent or malicious intent to search for and report vulnerabilities in ICT products or services subject to Belgian law, and offers a legal safe harbour against certain offences — provided all statutory conditions are strictly met, including:

- a **simplified notification within 24 hours** of discovery, to Kadonation **and** to the Centre for Cybersecurity Belgium (CCB);
- a **full notification within 72 hours** of discovery, to Kadonation **and** to the CCB;
- acting only within what is necessary and proportionate; and
- **no public disclosure** without the CCB's agreement.

Reporting to us under this policy satisfies the notification to Kadonation, but does **not** replace notification to the CCB if you wish to rely on the statutory protection. More information: ccb.belgium.be/cert/vulnerability-reporting-ccb.

6 PRIVACY

If you have provided your personal data, we may contact you for further information to help us investigate your report. We process any personal data you provide solely to handle your report, on the basis of our legitimate interest in the security of our systems (art. 6(1)(f) GDPR), and retain it only as long as necessary for that purpose.
For more information on how we handle your personal data, please see our privacy statement: kadonation.com/be-nl/privacy.

7 RECOGNITION

Kadonation does not offer any fixed payment or bug bounty for reporting potential or confirmed security vulnerabilities through this responsible disclosure programme. We do, however, greatly appreciate every submission. Where a report has genuinely helped us improve our security, we may, entirely at our own discretion and depending on the nature and impact of the issue reported, provide a small token of appreciation, for example a Kadonation gift voucher.