Kadonation NV Gordunakaai 61, 9000 Gent, Belgium
contact@kadonation.com

DATA PROCESSING POLICY

Last updated March 1st, 2022

Please provide this Data Processing Policy to your Data Protection Officer. In case you have questions about this Data Processing Policy or in case you require a signable version to enter a Data Processing Agreement, please contact our Data Protection Officer at compliance@kadonation.com.

1. INTRODUCTION

When Kadonation NV (Gordunakaai 61 BE-9000 Gent, VAT-number 0666.820.362, hereafter 'Kadonation') performs certain Services for a professional customer (hereinafter 'the Customer'), Kadonation shall have to process personal data for which the Customer is responsible as a Controller in accordance with the Privacy Legislation. This customer-oriented Data Processing Policy governs to the processing of personal data by Kadonation for the Customer. Relying on the Services of Kadonation implies the approval of the Customer with this Data Processing Policy.

2. DEFINITIONS

In this Data Processing Policy, the following concepts have the meaning described in this article (when written with a capital letter). Uncapitalized terms shall have the meaning as set out in the General Data Protection Regulation 2016/679.

Controller:	The entity, which determines the purposes and means of the processing of Personal Data, being in this case the Customer.
Processor:	The entity which processes Personal Data on behalf of the Controller, being in this case Kadonation.
Data Subject:	The natural person to whom the personal data relates and of whom the Customer wishes to have personal data processed by Kadonation.
Privacy Legislation:	(i) the General Data Protection Regulation 2016/679 of April 27, 2016; (ii) the Belgian Privacy Law of 30 July 2018; and/or (iii) the (future) Belgian legislation regarding the implementation of the General Data Protection Regulation.
Assignment:	All activities, such as but not limited to the Services, performed by Kadonation for the Customer, and any other form of cooperation whereby Kadonation processes personal data for the Customer, regardless of the legal nature of the agreement under which this processing takes place.
Services:	All services, provided by Kadonation to the Customer within the framework of the Assignment, implying the processing of personal data by Kadonation.
Sub-processor:	Any processor engaged by Kadonation to assist in the performance of the Services.

The Data Processing Policy includes the following annexes:

Annex I:	Overview of (i) the personal data, which parties expect to be processed, (ii) the categories of Data Subjects, which parties expect to be subject of the processing, and (iii) the way(s) of processing of the Personal Data, the purpose and means of such Processing
Annex II:	Overview and description of the technical and organizational security measures taken by Kadonation under this Data Processing Policy.
Annex III:	Overview of all Sub-Processors on which Kadonation appeals, including (i) the name of the Sub-Processors, (ii) their country of location and if they are located within or outside the EEA and (iii) the implemented safeguards (in case of transfer to Sub-Processors outside the EEA).

3. ROLES OF THE PARTIES

3.1. Parties acknowledge and agree that with regard to the processing of personal data, the Customer shall be considered 'Controller' and Kadonation 'Processor' in accordance with the Privacy Legislation.

4. THE ASSIGNMENT/SERVICES

4.1. The Customer owns and retains full control concerning (i) the processing of personal data, (ii) the types of personal data processed, (iii), the purpose of processing, and (iv) the fact whether such processing is proportionate (non-limitative).

4.2. The Customer acknowledges that by making use of the Services of Kadonation, the latter shall process personal data as provided by the Customer. Nonetheless, Kadonation shall only process the personal data upon request of the Customer and in accordance with its documented instructions, as described in Annex I, unless any legal obligation states otherwise.

4.3. Kadonation shall process the personal data in a proper and careful way and in accordance with the privacy legislation and other applicable rules concerning the processing of personal data.

4.4. The Customer acknowledges that the Customer is liable and responsible for the accuracy of the material and/or data it provided. Kadonation bears no responsibility with regard to adjustments and/or changes made to the personal data on the explicit request of the Customer.

4.5. Kadonation acts as a facilitator of the Services. Hence, the Customer shall be responsible on how it makes use of the Services and for all acts and omissions of its employees.

4.6. The Customer is liable and responsible for the content of the (personalised) messages generated or transmitted via the Services.

4.7. In case of misuse by the Customer of the Services, the Customer agrees that Kadonation can never be held liable in this respect nor for any damage that would occur from such misuse.

4.8. The Customer shall avoid any misuse of the Services. Therefore, the Customer shall safeguard Kadonation when such misuse would occur as well as for any claim from a Data Subject and/or third party due to such misuse.

4.9. The Customer acknowledges that data related to the use of the voucher that was gifted to the recipient can solely be reported to the Customer on an aggregated (anonymized) level as this personal data belongs to the Data Subject and is processed by Kadonation as a Controller.

5. SECURITY OF PROCESSING

5.1. Taking into account the state of the art, Kadonation implements appropriate technical and organizational measures for the protection of (i) personal data – including protection against careless, improper, unauthorized or unlawful use and/or processing and against accidental loss, destruction or damage – (ii) the confidentiality and integrity of personal data, as set forth in Annex II.

6. SUB-PROCESSORS

6.1. The Customer acknowledges and agrees that Kadonation may engage third-party Sub-processors in connection with the Assignment. In such case, Kadonation shall ensure that the Sub-processors are at least bound by the same obligations by which Kadonation is bound under this Data Processing Policy.

6.2. Kadonation added a list (cfr. Annex III) concerning the current Sub-processors on which it appeals for the performance of the Assignment.

- Kadonation shall:
  - Update the list whenever a Sub-processor changes (e.g. a new Sub-processor was added, a Sub-processor was substituted, etc.);
  - Clearly indicate and timestamp the changes in the list;
- Kadonation will notify the Customer (e.g. through the platform) when changes to the list are made. If the Customer wishes to exercise its right to object to a Sub-processor, it shall notify Kadonation in writing and in a reasoned manner by the latest within thirty (30) days after the notification.

6.3. In the event the Customer objects to a new Sub-processor and such objection is not found unreasonable, Kadonation will use reasonable efforts to (i) make available to the Customer a change in the Services or (ii) recommend a commercially reasonable change to the Customer's use of the Services to avoid processing of personal data by the objected new Sub-processor without unreasonably burdening the Customer.

- If Kadonation is, however, unable to make available such change within a reasonable period, the Customer may terminate the Assignment / the Services, by providing written notice thereof to Kadonation within a reasonable time, if:
  - The Services cannot be used by the Customer without appealing to the objected new Sub-processor; and/or
  - Such termination solely concerns the Services which cannot be provided by Kadonation without appealing to the objected new Sub-processor;

6.4. Kadonation shall be liable for the acts and omissions of its Sub-processors to the same extent as if it would be performing the Services itself, directly under the terms of this Data Processing Policy.

7. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

7.1. Kadonation shall only transfer personal data upon request of the Customer and/or in accordance with its documented instructions, unless Kadonation is required to do so by EU or member state law. In such a case, Kadonation shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

7.2. Any transfer of personal data outside the EEA by Kadonation to a third party whose domicile or registered office is in a country which does not fall under the adequacy decision enacted by the European Commission, shall be additionally subject to one or more of the listed EU-approved safeguards: Closing a data transfer/processing agreement with such recipient, which shall contain valid standard contractual clauses as adopted by the European Commission; and/or binding corporate rules; and/ or certification mechanisms.

8. CONFIDENTIALITY

8.1. Kadonation shall maintain the Personal Data confidential and thus not disclose nor transfer any personal data to third parties without the prior written agreement of the Customer, unless when such disclosure and/or announcement is required by law or by a court or other government decision (of any kind). In such case Kadonation shall, prior to any disclosure and/or announcement, discuss the scope and manner thereof with the Customer.

8.2. Kadonation ensures that its personnel, engaged in the performance of the Assignment, are informed of the confidential nature of the personal data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Kadonation ensures that such confidentiality obligations survive the termination of the employment contract.

8.3. Kadonation ensures that its access to personal data is limited to such personnel performing the Assignment in accordance with the Data Processing Policy.

9. NOTIFICATION

9.1. Kadonation shall use its best efforts to inform the Customer within a reasonable term when it: (i) Receives a request for information, a subpoena or an inspection or audit from a competent public authority in relation to the processing of personal data, or; (ii) Has the intention to disclose Personal Data to a competent public authority, or; (iii) Determines or reasonably suspects a data breach has occurred in relation to the Personal Data.

9.2. In case of a Data Breach, Kadonation notifies the Customer without undue delay after becoming aware of a data breach and shall provide – to the extent possible – assistance to the Customer with respect to its reporting obligation under the Privacy Legislation; and undertakes – as soon as reasonably possible – to take appropriate remedial actions to make an end to the data breach and to prevent and/or limit any future data breach.

10. LIABILITY

10.1. Both parties are solely liable for all damage, claims and/or fines of third parties, authorized supervisory authorities or Data Subjects that are the result of their own breach of or non-compliance with (i) the provisions of this Data Processing Policy, and (ii) the Privacy Legislation or other applicable rules concerning Personal Data. Each party indemnifies the other party in this regard.

10.2. In case of breach/non-compliance as described in Article 10.1, the infringing party is liable to the other party and must reimburse the latter for all damages and costs, including reasonable attorney's fees, (legal) expenses and damage resulting from a such breach/non-compliance.

11. RIGHTS OF THE DATA SUBJECTS

11.1. If a Data Subject requests to exercise his/her rights and the Customer itself, in its use of the Services, does not have the ability to correct, amend, block or delete the personal data, Kadonation shall offer cooperation and assistance with any commercially reasonable request by the Customer to facilitate such actions.

11.2. Kadonation shall promptly notify the Customer if it receives a request from a Data Subject for access to, correction, amendment, or deletion of that Data Subject's personal data. Kadonation shall, however, not respond to any such Data Subject request without the Customer's prior written consent except to confirm that the request relates to the Customer to which the Customer hereby agrees.

12. RETENTION, RETURN AND DELETION OF THE PERSONAL DATA

12.1. The Personal Data that was provided to Kadonation by the Customer shall only be retained as long as needed to provide the Services or the Assignment between the Customer and Kadonation, including after-sales service for the recipient, such as retrieving of voucher codes.

12.2. For separate orders:

12.2.1. Personal Data will be anonymized after expiration of the validity of the voucher.

12.2.2. In case the vouchers were assigned a lifetime validity, Personal Data is retained in our critical databases for ten (10) years, after which the Personal Data will be anonimyzed. The voucher code will remain valid but Kadonation will not be able to trace voucher codes to original recipients. For non-critical databases, the Personal Data is removed after one (1) year.

12.3. Personal Data that is processed by Kadonation under a Kadonation Select service, will follow policies 12.2.1 and 12.2.2 upon termination of the agreement after a retention period of one (1) year.

12.4. From-to messages/video messages/kudos that are directed to the end user are retained. They are connected to the account of the recipient and consultable after expiration of the voucher.

13. CONTROL

13.1. Kadonation undertakes to provide the Customer with all information, required by the Customer to allow verification whether Kadonation complies with the provisions of this Data Processing Policy.

13.2. In this respect Kadonation shall allow the Customer (or a third party on which the Customer appeals) to undertake inspections – such as but not limited to an audit – and to provide the necessary assistance thereto to the Customer or that third party. Every cost, arising out of such inspections, is borne by the Customer, unless the result of such inspection indicates that Kadonation has failed to perform the Services in accordance with this Data Processing Policy.

14. TERM

14.1. The Data Processing Policy lasts as long as the Assignment has not come to an end.

Kadonation NV Gordunakaai 61, 9000 Gent, Belgium
contact@kadonation.com

ANNEX I: OVERVIEW OF THE PERSONAL DATA

CATEGORIES OF THE PERSONAL DATA

In the context of the Agreement and the forthcoming provision of Services, Kadonation may need access to and may need to process on behalf of the Customer the following categories of personal data, the scope of which shall me determined exclusively by the Customer itself:

- First name
- Last name
- Salutation
- e-mail
- address
- Date of birth
- Job title
- Language
- Date of entry into service (commencement of the employment)
- Years of experience
- Content of the personalized message on the gifts or gift-related articles
- Company entity
- Company address
- Department or team name
- Team manager
- Content of the Kudos messages

DATA SUBJECTS

In the context of the Agreement and the forthcoming provision of Services, Kadonation may need access to and may need to process on behalf of the Customer the following categories of personal data of the following data subjects, the scope of which shall me determined exclusively by the Customer itself:

Customer's selected recipients of the Kadonation products:

- (Ex)-employees
- Freelancers
- Agents
- Business partners
- Serviceproviders

Customer's representatives, employees and other staff engaged in the purchase or personalisation of the vouchers or gift-related articles:

- Team managers
- Employees

THE USE (= WAY(S) OF PROCESSING) OF PERSONAL DATA AND THE MEANS AND PURPOSES OF PROCESSING

Use

- Storage
- Consultation
- Processing to provide the requested services, such as delivery of digital of physical gift vouchers or gift related articles

Means of the processing

- Kadonation software/application/platform

Purpose of the processing, i.e., Performance of the Assignment / Services (non-limited):

- Personalising the gifts and gift-related articles
- Distributing the gifts and gift-related articles
- Hosting the Personal Data
- Enabling the Customer to create user accounts
- Enabling the Customer to easily consult/adjust/delete the Personal Data
- Enabling the Customer and other employees to give Kadonation Kudos
- Sending the Data Subjects information regarding the vouchers or other products they received via the Customer

Kadonation NV Gordunakaai 61, 9000 Gent, Belgium
contact@kadonation.com

ANNEX II: DESCRIPTION OF SECURITY MEASURES

Technical and organisational measures, which are inspired by ISO27001 standards, are implemented by Kadonation in accordance with article 32 of GDPR legislation. They are continuously improved by Kadonation according to feasibility and state of the art.

TECHNICAL SECURITY MEASURES

Logical access control and authentication

Two-factor authentication is applied on critical applications involved in the processing of personal data (token expires every 30 seconds).

SAML integration (SSO) for Kadonation Select

When the Customer is a Kadonation Select tenant: Kadonation Select allows for SAML integration (SSO) to allow identity providers (IdP) to pass authorization credentials to Kadonation Select to authenticate Kadonation Select users and admins. When SSO via SAML is not applied, a login and a password is required. The password complexity is determined, and the application will prohibit the use of passwords that do not respect the determined level of complexity. When the customer's Kadonation Select account is activated, a 2-step verification process is required upon first login.

Risk assessment through penetration testing

Yearly system security is validated by an external party. This includes penetration testing and system and infrastructure vulnerability assessment.

Physical access control

Our office is locked with an electronic device which allows access logging. Access rights are restricted to authorised personnel only. An alarm system is in place and all access routes are monitored. The alarm system is connected to a 24/7 emergency centre.
Inactivity timeouts of no longer than 10 minutes are applied to all laptops and mobile devices of our employees.

Logging and monitoring

Logging is performed on each critical and high-risk application used for the processing of personal data. The log files include modification, deletion, errors logs and log in attempts. Log files are time stamped and adequately protected against tampering and unauthorised access. Clocks are synchronised to a single reference time source. Actions of the system administrators, including addition/deletion/change of user rights are logged. There is no possibility of deletion or modification of log files content. A monitoring system processes the log files and produces reports on the status of the system, including downtime, and notifies for potential alerts. Alerts are categorised according to severity to automatically notify the technical team and the CTO in case of critical events. Logs never contain passwords, password attempts or voucher codes. Depending on the application, the logs are only accessible for C-level management, the technical support team and/or the development team.

Encryption of data at rest

All data at rest is encrypted using AES-256 encryption algorithms. All passwords and all gift voucher codes are hashed.

Multi-tenant segregation of databases

Kadonation Select is a multi-tenant SaaS application; each tenant has a separate subdomain for the application as well as segregated user databases (services segregation).

Encryption of data in transit

When access to, or communication with, a database or application is performed through the internet, communication is encrypted through cryptographic protocols (https access; SSL certified: TLS 1.3 supported). When transferring personal data to (sub)processors such as vendors, transfer is secured by SSL or sFTP. In case such transfer protocol is not (yet) available, datafiles are encrypted when transferred. A documented work-from-home policy is in place and governed by the HR department. The policy outlines confidentiality principles and prohibits the processing personal data via a public WiFi network.

Kadonation Select API

When an API is set up for the Customer, each API is encapsulated per tenant (customer) and is accessed by making HTTP requests to a specific endpoint URL; every endpoint is accessed via an SSL-enabled HTTPS (port 443). The API authenticates via personal access tokens, the tokens can be renewed any time.

Business continuity and backup

To ensure the ability to restore the availability and access to personal data conform to GDPR article 32, scheduled full backups of production virtuals, SQL databases and transaction logs are performed daily. The execution of back-ups is monitored to ensure completeness. Our back up procedures allow us to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. The level of targeted business continuity is defined as point in time recovery (PITR) with RPO = 0 (zero data loss) and RTO = 3 hours. Back-ups are given an appropriate level of physical and environmental protection. Copies of backups are encrypted and securely stored offline in different locations.

Data deletion/disposal

Paper based media containing personal data is shredded upon disposal. Laptops and mobile phones are formatted through disk scrubbing upon decommissioning.

Fraud detection

Fraud detection systems are applied on B2C and B2B order systems.

ORGANISATIONAL SECURITY MEASURES

Data protection policy and other procedures for the protection of personal data

Kadonation's principles for the security and protection of personal data are described in a Data Protection Policy. The Data Protection Policy is reviewed and approved by c-level management. It is revised on an annual basis, and whenever necessary. Other procedures governing the protection

of personal data include: a laptop policy, a mobile device policy, a work-from home policy and a social media policy which are defined by HR. They document clear rules for their proper use and outline confidentiality principles towards personal data.

Defined roles and responsibilities

Kadonation has an appointed Chief Information Security Officer (CISO) who is responsible for IT security management and monitoring the implementation of technical security measures. The CISO collaborates with a designated data protection officer (DPO) who monitors overall compliance with GDPR. These two roles are therefore segregated. GDPR and security topics are discussed in a scheduled and regular GDPR management meeting including the data protection officer, CEO, CISO and other C-level management.

Access control policy

Specific access rights to our applications are allocated to each role involved in the processing of personal data. The access control policy is documented, detailed, and determines the appropriate rules, rights, and restrictions for specific user roles towards all applications, including access authorization and application owner. Applications are categorised in low/medium/high/critical risk levels based on their access to personal data and business continuity. All access rights are quarterly reviewed and checked upon onboarding and offboarding of an employee.

Password policy

A password policy is defined, documented and applicable for all applications. The policy includes instructions, password length, complexity, and validity period.

Change management

All changes to IT systems used for the processing of personal data are registered. Change requests are approved and monitored by the CISO. Regular monitoring of this process is implemented. Software development is performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is performed, dummy data is used.

Cloud policy

The storage of files containing personal data on a laptop hard disk, mobile phone or external device such as USB or SD devices is prohibited. All files are to be stored in the designated folders which are subject to access control and logging. The availability of hardcopy, such as printing personal data is to be restricted to the minimum necessary. In case personal information is made available in hardcopy, the storage is to be limited to the minimum necessary and the hardcopy is to be shredded upon disposal.

Incident response procedure

An incident response procedure is in place to ensure effective and orderly response to incidents pertaining personal data.

Confidentiality of the personnel

All employees are bound by a confidentiality clause under their employment contract, which ensures confidentiality of the personnel both in terms of technical expertise and personal integrity with respect to article 32(4) of GDPR.

Training

Employees, including relevant freelancers, involved in the processing of personal data are properly educated about GDPR legislation through regular training events and awareness campaigns. All developers are trained on a technical level about secure coding.

Processor management

Formal guidelines and procedures covering the processing of personal data by the data (sub)processors are defined, documented and agreed between Kadonation and its (sub)processors to ensure the same level of security as mandated in our security policy, proportionate to the category of the personal data to be processed.

Kadonation NV Gordunakaai 61, 9000 Gent, Belgium
contact@kadonation.com

ANNEX III: OVERVIEW OF SUB-PROCESSORS

Name and purpose of the Sub-processor	Country and location within or outside EEA	Implemented safeguards (in case of transfer outside EEA)
Google Cloud Platform and Google Workspace (Cloud hosting provider)	Third country entity Datacenter located within EEA	■ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Amazon Web Services (AWS) (Cloud hosting of voucher print files and visual material)	Third country entity Datacenter located within EEA	■ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
vBridge BV (Cloud architecture consulting)	Belgium (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Mirto cvba and Mirto vzw (Printing and handling services for paper-based vouchers or gift related articles)	Belgium (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Pondres Direct Mail BV (Printing services and handling services for paper-based vouchers or gift related articles)	The Netherlands (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Bloomgift BV (Vendor of gift articles via Kadonation Select platform)	The Netherlands (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Belgunique BV (Vendor of gift articles via Kadonation Select platform)	Belgium (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms
Apideck BV (API architecture and integration with Kadonation Select platform)	Belgium (within EEA)	☐ Standard contractual clauses ☐ Binding corporate rules ☐ Certification mechanisms

- The use of Sub-processors depends on the scope of the assignment (printed vouchers / digital vouchers / gift articles / Kadonation Select API integration / use of personal data on the vouchers).
- In case of non-nominative digital vouchers that are sent to the Customer, none of the above sub-processors are employed as in such case, no personal data is processed by Kadonation as a Processor.

Revision history

- Pondres Direct Mail BV added 01/10/2021
- Vanhalst BV deleted 01/03/2022
- AWS revised 01/03/2022
- Bloomgift BV added 01/03/2022
- Belgunique BV added 01/03/2022
- Apideck BV added 01/03/2022