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

kadonation

DATA PROCESSING POLICY – KADONATION NV

Classification: Public / Last version: July 2025 / Last updated: 3-10-2025 / Last reviewed: 17-07-2025

1. INTRODUCTION

KADONATION NV is a company incorporated and existing under the laws of Belgium, with registered office at Gordunakaai 61, 9000 Gent, Belgium with company number BE-0666.820.362 (hereinafter '**Kadonation'**).

When you, a professional Customer (hereinafter the '**Customer'**), rely on the Kadonation Platform and/or Services, Kadonation shall **(i)** have access to Personal Data (as defined hereinafter) and/or **(ii)** will have to process Personal Data for which the Customer is responsible as a Controller in accordance with the Privacy Legislation (as defined hereinafter).

This data processing policy (hereinafter '**Data Processing Policy'**) applies to the Processing of Personal Data by Kadonation for the Customer and determines (**i**) how Kadonation will manage, secure and process the Personal Data, and (**ii**) both parties' obligation to comply with the Privacy Legislation.

By relying on the Platform and/or Services of Kadonation, the Customer acknowledges to have read and accepted this Data Processing Policy and consequently the way Kadonation Processes the Personal Data.

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.

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;
Controller:	The entity, which determines the purposes and means of the processing of Personal Data, being in this case the Customer;
Data Importer:	The recipient of Personal Data/Processor of Kadonation in a third country, which is not subject to an adequacy decision of the European Commission;
Data Subject:	The natural person to whom the Personal Data relates and of whom the Customer wishes to have Personal Data Processed by Kadonation, as identified in **Annex I**;
Data Breach:	Unauthorized disclosure, access, abuse, loss, theft or accidental or unlawful destruction of Personal Data, which are Processed by Kadonation on behalf of the Customer;
End-User	Any individual authorized by the Customer to access and use the Platform on behalf of the Customer (such as employees, freelancers, subcontractors);
Personal Data:	Any information relating to an identified or identifiable natural person (i.e. the Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Platform:	The Kadonation webshop or the Kadonation Select platform, through which the Customer can **(i)** purchase products and/or services, **(ii)** create and manage End-Users and their roles, **(iii)** access informational documentation related to the products and/or services, and **(iv)** access the helpdesk;
Privacy Legislation:	**(i)** the General Data Protection Regulation 2016/679 of April 27, 2016 ('GDPR'); **(ii)** Directive 2002/58/EC of the European Parliament and Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector ('e-privacy directive') (including all future legislative changes and amendments/revisions thereof); and/or **(iii)** all (future) national laws regarding the implementation of the GDPR;
Process/Processing:	Any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, including, but not limited to: collection, recording, organization, structuring, storage,

kadonation

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data;

Processor: The entity which processes Personal Data on behalf of the Controller, being in this case Kadonation;

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 subject of the Processing, **(ii)** the categories of Data Subjects, which parties expect to be subject of the Processing, **(iii)** the retention period for each Processing, and **(iv)** the use (i.e. 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 in order to protect the Personal Data that are being Processed during the performance of the Services.

Annex III: Overview of all Sub-Processors on which Kadonation appeals, including **(i)** the name of the Sub-Processors, **(ii)** their country of location, **(iii)** if they are located within or outside the EEA and **(iv)** 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. Further, Kadonation is allowed to engage Sub-processors pursuant to the requirements set forth in **Article 7.**

3.2. Each Party shall comply with its respective obligations under the Privacy Legislation with respect to the Processing of the Personal Data.

4. THE ASSIGNMENT/SERVICES

4.1. 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.

4.2. The Customer acknowledges that:

✔ Kadonation acts as a facilitator of the Services. Hence, the Customer shall be responsible on how and to what extent it makes use of the Services;

✔ Kadonation allows the Customer to make adjustments and/or changes to the Personal Data and shall never consult or adjust these Personal Data itself, unless the Customer requests Kadonation to do so. Kadonation bears no responsibility with regard to adjustments and/or changes made to the Personal Data on the explicit request of the Customer;

✔ The Customer is responsible for all acts and omissions of the End-Users (i.e. in case the End-User does (not) take sufficient measures to protect its account on the Platform). The Customer shall inform the End-Users of the applicable Privacy Legislation, this Data Processing Policy and/or all other relevant legislation and assure the End-Users act compliant;

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

✔ 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;

✔ The Customer shall comply with all laws and regulations (such as but not limited to the retention period or rights of the Data Subject) imposed on it by making use of the Services.

4.3. The Customer shall avoid any misuse of the Services and/or the Platform. In case of misuse by the Customer and/or the End-User, the Customer agrees that Kadonation can never be held liable in this respect nor for any damage that would occur. Therefore, the

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

Customer shall safeguard Kadonation when such misuse would occur as well as indemnify Kadonation for any claim from a Data Subject and/or third party due to such misuse.

5. OBJECT

5.1. The Customer acknowledges that as a consequence of 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.

5.2. The Customer owns and retains full control concerning **(i)** how Personal Data must be Processed by Kadonation, **(ii)** the types of Personal Data Processed, **(iii),** the purpose of Processing, and **(iv)** the fact whether such Processing is proportionate (non-limitative).

5.3. Furthermore, the Customer acknowledges that it is responsible for:

✔ the accuracy, quality and legality of (the collection and transfer of) the Personal Data provided by the Customer and/or the Data Subject;

✔ compliance with all transparency and lawfulness requirements under the Privacy Legislation and/or other regulations for the collection and Processing of the Personal Data and the transfer thereof to Kadonation;

✔ ensuring compliance of its instructions with the Privacy Legislation.

5.4. Customer shall inform Kadonation without undue delay if it is not able to comply with its responsibilities under this Article or the applicable Privacy Legislation.

6. SECURITY OF PROCESSING

6.1. Kadonation takes the security of the Processing activities very seriously. 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**.

7. SUB-PROCESSORS

7.1. 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.

7.2. Kadonation added a list (cfr. **Annex III**) concerning the current Sub-processors on which it appeals for the performance of the Assignment, which includes the identities of those Sub-processors and their country of location.

✔ 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 list was updated.

7.3. In the event the Customer objects to a new Sub-processor and such objection is well founded 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, under the following condition:

- 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;

And this by providing written notice within a reasonable time.

7.4. Kadonation takes responsibility 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.

8. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

8.1. The Customer recognizes that Kadonation is entitled to transfer and store the Personal Data to countries outside the EEA for the purpose of providing the Services and fulfilling its obligations, and provided that such transfer/storage is done in accordance with the Privacy Legislation regarding additional safeguards. In particular, any transfer of Personal Data outside the EEA by Kadonation to a third party whose registered office is in a country which does not fall under an adequacy decision enacted by the European Commission (a list of appropriate third countries is available on the European Commission's website), shall be additionally subject to one or more of the listed EU-approved safeguards:

✔ Closing a **data transfer agreement** with the third country recipient, which shall contain the **standard contractual clauses** ('SCC'), as adopted by the European Commission in Decision (EU) 2021/914. Before the transfer takes place, the Data Importer has to guarantee Kadonation that an adequate level of privacy compliance is ensured in this third party country; and/or;

✔ **Binding corporate rules**. The Data Importer has to guarantee Kadonation that an adequate level of privacy compliance is ensured in the third party country; and/or;

✔ **Certification mechanisms.**

In the event the transfer (or disclosure) of the Personal Data to a third country is required by EU law or EU member state law to which Kadonation is subject to, Kadonation shall inform the Customer of that legal requirement before the transfer/disclosure, unless that law prohibits such information on important grounds of public interest.

8.2. If necessary, take **supplementary measures** in relation to the entity receiving the Personal Data to ensure that the Personal Data remains protected in accordance with the applicable Privacy Legislation.

Furthermore, Kadonation shall take all reasonable efforts to oblige the Data Importer to implement sufficient guarantees and measures to protect the Personal Data and ensure the effectiveness of the protection of the SCC's, binding corporate rules and/or certification mechanisms.

8.3. In case of non-compliance by a Data Importer or where protections in the third country are not adequate, Kadonation shall – at its sole discretion – either:

✔ Suspend the transfer of Personal Data to the Data Importer / such third country until the issue has been solved, or;

✔ Terminate the transfer of Personal Data to the Data Importer / such third country and request the Data Importer to delete the Personal Data in its possession.

9. CONFIDENTIALITY

9.1. 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 transfer 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.

9.2. 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.

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

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

10. NOTIFICATION

10.1. Kadonation shall use its best efforts to inform the Customer within a reasonable term when it:

- ✔ 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;
- ✔ Has the intention to disclose Personal Data to a competent public authority, or;
- ✔ Determines or reasonably suspects a data breach has occurred in relation to the Personal Data.

10.2. In case of a Data Breach, Kadonation:

- ✔ Notifies the Customer without undue delay after becoming aware of a Data Breach. In the event the Customer wishes so, Kadonation shall provide – to the extent possible – assistance to the Customer with respect to its reporting obligation under the Privacy Legislation;
- ✔ 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.

11. LIABILITY

11.1. 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.

11.2. In case of breach/non-compliance as described in **Article 11.1**, 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.

11.3. The liability of Kadonation for a breach of this Data Processing Policy is limited as described in the applicable contractual documentation (i.e. terms & conditions B2B).

12. RIGHTS OF THE DATA SUBJECTS

12.1. 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.

12.2. 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.

12.3. Notwithstanding the foregoing, the Customer remains responsible for compliance of such Data Subject requests.

13. RETENTION, RETURN AND DELETION OF THE PERSONAL DATA

13.1. Kadonation shall only retain the Personal Data 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.

13.2. For separate orders, Personal Data will be anonymized after expiration of the validity of the voucher.

13.3. Personal Data that is processed by Kadonation under a Kadonation Select service, will follow the policy described in **Article 13.2** upon termination of the agreement after a retention period of one (1) year.

13.4. From-to personalized messages/video 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.

13.5. All the foregoing does not apply, and Kadonation may therefore continue to retain the Personal Data if – and only to the extent that – it is required to do so pursuant to a legal obligation imposed on Kadonation.

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

14. COMPLIANCE AND INSPECTIONS

14.1. Upon Customer's request, Kadonation undertakes to provide the Customer with all information and to the extent as requested by law to allow verification whether Kadonation complies with the provisions of this Data Processing Policy.

14.2. In this respect Kadonation shall allow the Customer to undertake inspections – such as but not limited to an audit – and to provide the necessary assistance thereto to the Customer. The Customer must notify Kadonation at least thirty (30) working days in advance. The performance of inspections may in any case not cause any delay in the performance of the Services by Kadonation.

14.3. All inspection costs are exclusively 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.

15. TERM

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

16. UPDATES

16.1. This Data Processing Policy may be updated from time to time by Kadonation, in which case Kadonation shall notify you through its website or Platform. In any event, the latest version of this Data Processing Policy can always be accessed on the Kadonation website, as well as on the Platform.

16.2. You can find our archived Data Processing Policy here: https://kadonation.com/en/compliance-security

17. GOVERNING LAW & JURISDICTION

17.1. This Data Processing, including its Annexes, shall be governed by the law and subject to the jurisdiction clause as provided in the Assignment.

18. CONTACT | DPO

18.1. Kadonation has appointed a Data Protection Officer (or "DPO") to ensure its compliance with Privacy Legislation. If you have any questions with regard to this Data Processing Policy or the manner in which Kadonation Processes the Personal Data, please contact our DPO via email: compliance@kadonation.com.

DPO
Name: Deloitte Accountancy BV/SARL
Email: compliance@kadonation.com
Company number: BE 0443.578.822
Address: Luchthaven Brussel Nationaal 1 J, 1930 Zaventem, Belgium

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

kadonation

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 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

RETENTION PERIODS

Kadonation shall retain all Personal Data as long as the Assignment is not terminated (and the Data Subject did not request deletion). Once the Assignment is terminated, Kadonation shall retain all Personal Data as long as legally required. All Personal Data shall be kept at least one (1) year after the Assignment is terminated, to enable the Customer to export its data. When the retention period expires, all Personal Data shall be permanently deleted, or at least anonymized.

THE USE 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
BTW BE-0666.820.362
E: compliance@kadonation.com

kadonation

ANNEX II: DESCRIPTION OF SECURITY MEASURES

Technical and organizational measures, which are inspired by ISO27001 standards, are implemented by Kadonation in accordance with article 32 of GDPR legislation and 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 of 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 online in Google Cloud.

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

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.

ORGANIZATIONAL 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.

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.

ANNEX III: OVERVIEW OF SUB-PROCESSORS

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

kadonation

An up-to-date list of sub-processors can be found here: https://trustcenter.kadonation.com/subprocessors