Privacy Policy

Last update June 7, 2021

Preamble

This confidentiality policy addresses you as a user of the internet site https://vistacard.app (hereinafter “the Site”) and the mobile app (hereinafter “the App”) in view to informing you about how your personal data, if any, can be collected and processed by VISTACARD.

For us, respecting your private life and your personal data is a priority and we are committed to processing your data in strict conformity with the Law on Computing and Freedom of January 6, 1978 (hereinafter referred to as the “CF law”) since amended, and the European Union’s General data protection regulations of April 27, 2016 (hereinafter referred to as “GDPR”).

Whatever the case, we are committed to abiding by the two following essential principles:

1. You remain in control of your personal data;
2. Your data are processed transparently, confidentially and securely.

Article 1. Identity and address of the data controller

The controller of your data is VISTACARD (company n° 898 318 720) located at 15 rue des Halles – 75001 Paris.

For more information on our address

Legal reminder: The data controller is, with respect to the Law on Computing and Freedom, the entity that defines the resources and objectives of the processing performed. When two data controllers or more define the objectives and objectives of the processing together, they are jointly responsible for the processing (or joint managers). The subcontractor is an entity that processes the personal data on behalf of the data controller, it acts under the authority of the data controller and under their instructions.

VISTACARD is a simplified joint stock company with a sole partner and a paid-up capital of €1,000.00, enrolled on the Trade and Companies Registry of Paris under number 898 318 720, whose head office is at 15 rue des Halles – 75001 Paris, France.

Article 2. Collection and origin of the data

All the data concerning you are collected either directly from you (information communicated via the different forms on the Site and the App), or indirectly when you visit the Site and the App (login and browsing data).

In all cases, your data are collected and processed only to ensure the supply of different services, manage your subscription to Starter or Premium plan and respond to your requests for information.

The details of how your data are collected and processed is provided in the present Confidentiality Policy.

For further information

When necessary, we undertake, according to case, to obtain your consent and/or allow you to contest the utilization of your data for certain objectives, such as, the possibility of installing third party cookies on your computer/device for the purposes of measuring the audience of our internet site.

Article 3. Objectives and legal basis of processing

Your different data are collected and processed for:

1 / The use of the App (without creating a business card).

2 / The creation and management of your Starter or Premium account, your subscription and your invoices.

For further information

Legal basis:

- Contractual, processing is necessary to perform a contract or to carry out pre-contractual measures.

3 / Respond to your requests for information on our services and to manage client relations.

For further information

Legal basis:

- Your consent

4 / Manage and respond to your requests to exercise your “Computer and Freedom” rights.

For further information

Legal basis:

- Legal obligation (Law on Computing and Freedom and GDPR).

5 / Ensure the efficient operation and permanent improvement of our internet site, the App and its functionalities.

For further information

Legal basis:

- Our legitimate interest in guaranteeing the best level of operation and quality of our site by using in particular the statistics of visits to the site.
- Your consent when it is required.

Article 4. The data processed

The mandatory or optional nature of the personal data and possible consequences of a failure to respond regarding you are stipulated during their collection.

You can consult the details below of the personal data we may possess concerning you:

To use the App in general

- Your IP address,
- The IP addresses of your addressees,
- Your email address,
- The email addresses of your addressees,
- Your localization and your language,
- The localization and language of your addressees,
- The name and version of your device/browser,
- The names and versions of your addressees' devices/browsers,
- Your device/computer's operating system,
- The operating systems of your addressees.

To create and manage your Starter/Premium account, your subscription and your invoices

- Your name,
- Your first name,
- Your email address,
- Your password,
- The name of your company,
- Your postal address,
- Your town/city,
- Your country,
- Your zip code,
- The subject associated with your transfer,

- The message associated with your transfer,
- The customized URL of your link,
- The name of your files, their sizes and their types,

To respond your requests for information on our services and manage client relations

- Your name,
- Your email address,
- The subject of your message,
- Your message.

To manage your requests to exercise your “Computer and Freedom” rights

- Your name,
- Your first name,
- Your mobile phone number,
- Your email address,
- If necessary, a copy of your identity card.

Article 5. Addressees of your data

Within the limits of their respective attributions and for the objectives recalled in article 4, the main persons who may have access to your data are the following:

- The staff members authorized at VISTACARD;
- The companies responsible for hosting the data and files;
- The company responsible for management payments;
- The company responsible for sending transactional emails;
- When the situation arises, the jurisdictions concerned, mediators, accountants, auditors, lawyers, writ servers and bailiffs, debt collection agencies, the police or gendarmerie in the case of theft or judicial requisition, emergency services;
- The authorized personnel of our subcontractors;
- Third parties liable to install cookies on your terminals (computers, pads, mobile phones, etc.) when you give your consent.

Your data are not transmitted to any other person other than those mentioned above.

For further information on the list of our partners.

1 / The companies responsible for hosting the data and files:

- **Google Firebase**.
- **IONOS**.

2 / The company responsible for managing the payments:

- **Google or Apple**, depending on the device used (“in-app” purchase).

3 / The company responsible for sending the transactional emails:

- **The Rocket Science Group LLC d/b/a MailChimp**.

Article 6. Period of data conservation

We conserve your data only for the time required for the objectives pursued, as described in article 4, and summarized in the following table:

To use the App in general
1 year counting from the last use of the App.

To create and manage your Starter/Premium account, your subscription and your invoices:
3 years counting from the end of commercial relations.

To respond to your request for information on our services and manage client relations:
3 years counting from the end of commercial relations if you are a client or counting from your last contact if you are not yet a client.

To manage your requests to exercise your “Computing and freedom” rights:

1 year in the case of exercise of right of access or correction.

3 years in the case of right of right of opposition.

To ensure the efficient operation and permanent improvement of our internet site and its functionalities:
13 months. Beyond this period, the raw patronage data associated with a user name are deleted or anonymized.

Article 7. Your rights

In conformity with the Law on Computing and Freedom and the GDPR, you have the following rights:

- the right of access (article 15 GDPR), rectification (article 16 GDPR), updating, and completeness of your data;
- the right to block of erase your personal data (article 17 GDPR), when they are inexact, incomplete, equivocal, obsolete, or whose collection, utilization, communication or conservation is forbidden;
- the right to withdraw your consent at any time (article 13-2c GDPR);
- the right to limit the processing of your data (article 18 GDPR);
- the right to contest the processing of your data (article 21 GDPR);
- the right to the portability that your gave to us, when your data were subjected to automated processing based on your consent or on a contract (article 20 GDPR);
- the right to define the fate of your data after your death and to choose that we communicate (or not) your data to a third person appointed beforehand by you.

In the case of death and not having received instructions from you, we undertake to destroy your data, unless their conservation is necessary for purposes of proof or to satisfy a legal obligation.

You can exercise your rights by sending an email to: privacy@vistacard.app or by sending a letter to: VISTACARD – 15 rue des Halles – 75001 Paris.

Lastly, you can also make a claim to the supervisory authorities and to the CNIL in particular (https://www.cnil.fr/fr/plaintes).

Article 8. Login data and cookies

On our site we use login data and cookies (small files saved in your computer) that allow us to identify you, remember your visits to the pages you consult in particular, and measure the use made of our site.

You can consent, refuse or choose the type of cookies you accept to be installed on your computer terminals.

Article 9. Transfers of data outside the European Union

Concerning the nature of its activity, VISTACARD is led to carrying out transfers of your data to subcontractors outside the European Union.

VISTACARD makes certain commitments on this subject.

Recipients

First of all, VISTACARD does not transfer your data that it processes to third parties other than its internal services and service providers for the purposes of the processing, or to the legally authorized authorities at their request. When VISTACARD acts as a subcontractor, the only service provider acting as a subsequent subcontractor is GOOGLE which hosts the service in several European countries and outside the European Union.

In other words, VISTACARD does not give access to the data processed in its own interest or that of its customers to any partner whatsoever.

Providers

When VISTACARD uses service providers to provide it with certain tools or services involving personal data, the territory of the European Union will be systematically privileged as far as possible.

Exit from the Union with adequate protection by default

If the processing requirements imply an exit from the Union, VISTACARD favors the territories and entities which are the subject of an adequacy decision by the European Commission.

Formalization of adequate protection

If processing in the territory of the Union or in a territory benefiting from default protection proves to be impossible or unsuitable, VISTACARD could consider another type of transfer. In such a situation, VISTACARD undertakes to put in place adequate contractual protection, except in exceptional cases exhaustively listed by the GDPR.

Article 10. Security

VISTACARD and its possible subcontractors undertake to implement every technical and organizational measure to ensure the security of our processing of personal data and their confidentiality, in application of the Law on Computing and Freedom and the European General Data Protection Regulations (GDPR).

Consequently, VISTACARD takes useful precautions regarding the nature of your data and the risks incurred by our processing, to preserve data security and in particular prevent them from deformation, damage or access by unauthorized third parties.

Inherent to its design, VISTACARD incorporates several levels of protection: secured data transfer, encryption, network configuration and controls of applications and users, distributed over an open-ended and secured infrastructure.

Thus, VISTACARD implements the following measures:

- The files stored in are encrypted using AES (Advanced Encryption Standard), 256 bits.
- uses the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol to protect the data during transfer between the application and the servers.
- We regularly test the applications and infrastructure to identify possible breaches in security, strengthen their security and protect them against attacks.