Privacy Statement

Updated: July 2021

Your privacy & CCV

At CCV we think your privacy is very important, because you entrust CCV with your payment and personal data. We therefore would like to take this opportunity to explain how we protect your personal data.

CCV has been in the business of handling payment data – yours and those of millions of other people in Europe – for decades. The privacy of people whose personal data we process, is key for our business. We process these data because they are necessary to provide our services and products and to meet our legal obligations. CCV also processes personal data of its own employees. We consider it important to be transparent about our processing of personal data and to meet the requirements laid down in the EU General Data Protection Regulation ('GDPR') and other privacy legislation. For this reason we have published this Privacy Statement that describes how CCV processes personal data and how CCV ensures the protection of privacy when processing personal data.

For its work CCV has to comply with the following legislation:

- EU General Data Protection Regulation ("GDPR", Algemene Verordening Gegevensbescherming, AVG)
- Financial Supervision Act (Wet op het financieel toezicht, WFT)

- Prevention of Money Laundering and Terrorist Financing (Wet ter voorkoming van Witwassen en Financieren van Terrorisme, WWFT, SWG-FT)
- Telecommunications Act (Telecommunicatiewet, TW)
- General Data Protection Regulation Implementing Act (Uitvoeringswet Algemene Verordening Gegevensbescherming, UAVG)

CCV's operational processes are set up to ensure full compliance with the stringent requirements of each of the above-mentioned laws. In addition to this, we took technical and organizational measures to protect the transfer of data and data traffic and to ensure the safety of your and your customers' privacy.

Basic privacy principles

In a nutshell, our compliance with these laws means that we observe the following basic principles:

- We will only use (process) your personal data to perform our work and to execute an agreement with you.
- We will only collect and process data that we need in order to perform our work.
- We will only transfer data when required for example by the supervising authorities or by the police or justice officials and because we have the obligation to share the requested information with them (legitimate interest).
- In all other circumstances we will only process your personal data with your explicit permission,
- We will inform you of your rights (this is the purpose of this document).
- We will not take any action with regard to your personal data unless and until you give permission to take any action or when you ask us to take any action such as to correct your personal data or to remove them, if we still retain them under our retention policy
- We will ensure that your personal data are and remain correct.
- We will not retain your personal data for a longer period than necessary.
- We will protect your personal data against access by unauthorized parties, loss or destruction.
- We can demonstrate our compliance with these principles.

We treat all personal data extremely carefully and confidentially and we make sure that personal data are protected by effective security measures. The processing

operations that CCV perform are registered in a record of processing activities. A check is made to verify whether CCV is allowed to process the personal data, and also to make sure that CCV is not processing more personal data than necessary or mandatory. At CCV, we also ensure that only authorized persons are able to access personal data and that the personal data are not being used for impermissible purposes. If we engage any another company to perform certain processing activities, we make sure that the other company applies the same basic principles as we do at CCV to assure the careful treatment of personal data and the same level of protection.

CCV is required by law to adhere to statutory data retention periods for numerous processing operations. For all other processing operations, we do not save personal data longer than strictly necessary to fulfil the purposes for which the data was collected.

What personal data do we collect?

First name, last name, date of birth, company name, country, email address, physical address, phone number, gender, copy ID, contact history, account numbers, IP address, cookie-settings, cookies and data about your website visits. This data is collected via several forms on our website For more information regarding cookies, please visit our cookie statement.
CCV does not collect data that falls under the special categories of personal data (e.g. data revealing health, racial or ethnic origin, political opinions, religious or philosophical beliefs).

How do we collect personal data?

- Personal data provided by data subject himself;
- Public sources like, Chamber of Commers and Company records, Google;
- Personal data received by transaction monitoring.
- Personal data received by third parties

CCV is data controller and data processor

From a legal perspective, we fulfil a dual role when it comes to privacy. We record and manage personal data of our clients, your customers and our employees. Officially, we are a data controller in that capacity and, as such, accountable for the careful handling of data.

In addition, we process payment data on behalf of our clients, including ING, Equens, ACI and Bancontact. In that sense, we are a data processor. Our clients are data controllers and accountable for data handling. They expect us to meet specific requirements concerning handling of your data. These requirements are laid down in a partnership agreement. We carry out such agreements with utmost care. In both roles, we are committed to protecting your privacy with due care.

Your rights

We handle your data as carefully and as safely as possible. Should you want to verify this, it is good to know that you – as the owner of your personal data – have a number of rights:

Right to information

You have the right to be informed about our work processes that involve the handling and processing of your personal and payment data.
More about how CCV handles data >>

Right to inspection

You have the right to access the personal data about you that we have on record. If you want to exercise this right, we must first verify your identity before we can start retrieving your data. You will be send all the data about you that we have. We will also inform you of the details of our processing method, including the purpose, retention period, the parties that we share data with, and how data have been obtained. We aim to provide you with an overview of these data within one month. We will inform you if we expect that it will take more time than one month.
Submit a request for access to your data >>

Right to correction, restriction and deletion

You have the right to correct or supplement the personal data about you that we have on record. You also have the right to delete part of your data in order to restrict how much data we can use in the future. And you have what is known as the ‘right to be forgotten’, which means that all the data about you we have on record will be deleted. However, we are required by law to retain certain data, so

these we cannot delete.
Submit a request to change or delete data >>

Right to data transfer

You have the right to request the digital transfer to a different organization of data that CCV has on record about you. If you want to exercise this right, we will provide your data to you in a structured and generally accepted file format. We are only allowed to do this with personal data that you provided to us in person, or if you gave express permission to process such data, or with data we obtained as result of the fulfilment of our agreement. We aim to complete preparing the file for data transfer within one month. We will inform you if we expect that it will take more time than one month.
Submit a request for data transfer >>

Right of objection

If you think that we are wrongfully processing personal data about you, we encourage you to make this known to us. If your objection is justified, we will stop processing your personal data. You can also file an official complaint if you think your data are not being handled with due care. When we receive a complaint, we will carefully review our processes and work to eliminate any shortcomings we identify. We aim to address your complaint within five business days. We will inform you if we expect it will take more time. If we are unable to reach agreement, you have the option of submitting your complaint to the Dutch Data Protection Authority.
Submit a complaint to CCV >>
Submit a complaint to the Dutch Data Protection Authority >>

How we handle your data

We use a range of technological and organizational measures to protect your private data as effectively as possible. With certifications from national and international quality and safety standards organizations, we demonstrate how serious we are about protecting your privacy. These certifications include compliance with the Payment Card Industry Data Security Standard (PCI DSS). We use the following methods to protect your privacy in our work processes.

Triple data protection

1. First and foremost, responsibility for the careful handling of data rests with our colleagues whose day-to-day work involves the processing of personal data. They know how data are processed and have access to the content of applications. They also assess the proper functioning of all processes on a daily basis.
2. Internal policies, Compliance with rules and legislation and risk management is the responsibility of CCV's GRC department and CCV's data protection officer. CCV's privacy officers conduct risk analyses in the various departments and assess whether the processes comply with applicable laws and regulations.
3. Lastly, our independent internal audit department and the data protection officer will check if the aforementioned colleagues work together effectively, and whether we actually fulfil all our legal and business obligations.

Safeguarding work processes

A new work process can sometimes involve risks to your personal data. That is why we subject any new work processes to a Data Protection Impact Assessment (DPIA). We also conduct a risk analysis and a technical assessment, so we can be sure that the authorization process, security aspects and record keeping are compliant.

Record-keeping of processing activities

Detailed records are kept of all data processing operations that we carry out, to make sure that we can always trace what happens with your personal data. Our data protection officer will make sure that this record keeping is and remains complete and up-to-date.

Purpose of data usage

Personal data about employees will only be used to carry out our duties as an employer. Personal data about clients (such as name and contact details) will only be used to provide our services, such as but not limited to:

- Conclude or amend agreements and allow execution of (service) contracts;

- Allow compliance with legal obligations, such as CCVs KYC policy for new and existing clients, or Customer/Supplier Due Diligence Fulfil reporting obligations to the authorities
- Process and analyze payment transactions;
- Resolve disputes and disputed payment transactions;
- Prevent and address fraud, money laundering and other unlawful activities;
- Analyse data in order to improve our services and to enhance our products and services;
- Research (For research purposes CCV uses pseudonymized (not traceable to an individual person) personal data);
- Record telephone conversations in order to avoid misunderstandings and mistakes in contacts with clients or to record oral agreements or promises we make to you on the phone and to ensure that our staff handled issues correctly in telephone conversations;
- Initiate, coordinate and outsource work processes;
- Carrying out specific marketing activities.

Retention period

Personal data will not be retained for longer than is necessary for the intended purpose, and will not be retained beyond the statutory retention period. We ensure compliance with this retention period by keeping the retention period details and the corresponding personal data in the same location.

Anti-fraud measures

We work together with banks, credit card companies and other parties that combat fraud. To facilitate these efforts, it is sometimes necessary to share data with these parties. This always happens in compliance with legal requirements and only with the express permission of our data protection officer.

Internal training and awareness

Our employees are aware of the importance of privacy. They have been trained in protecting your privacy and keeping information secure. We make sure that this awareness and expertise stay up-to-date, for instance by offering an e-learning program and through regular internal information sharing. Our data protection officer and the corporate information security officer monitor these activities.

Our promise

CCV will disclose your personal data to other organizations only if it is legally required from us. For example, CCV is bound by obligations embodied in such legislation as the Anti Money Laundering and Terrorist Financing Prevention Act, the Sanctions Act and the Financial Supervision Act. As part of a fraud investigation, CCV might process data relating to criminal offences. We make agreements with organizations that receive your data from us about such matters as the security and confidentiality of your data. We keep a record of processing activities in which we register the purpose of processing, the grounds for processing, the retention period, the technical and organizational measures implemented, the type of personal data and the portability of personal data to third parties.

In the event of a data breach

No matter how effectively we perform our work, the risk of a data breach always exists. This can be the result of human error or have an external cause. A data breach is defined as a situation in which personal data is lost, ends up in the wrong hands or is otherwise exposed.

In the event of a data breach, immediate action is required. We will first examine which personal data have been affected. If the breach could potentially affect your rights and integrity, the data breach will be reported to the Dutch Data Protection Authority within 72 hours after discovery of the breach. In case there is a risk that your personal integrity may be affected, you will also be informed right away.

In addition, the breach will be thoroughly investigated. We will get to the bottom of what happened and determine which data has been exposed to risk, who or what might be the cause, and how we can prevent similar data breaches in the future. This approach enables us to tighten our security. Furthermore, we will carefully record any and all findings about the data breach to ensure we can learn from them in the future.

Reporting a data breach

Do you think a data breach may have occurred? Please inform us as quickly as possible, stating the reasons or the signals that your suspicion is based on.
Report a suspected data breach >>

Terms and definitions

Personal data

All information pertaining to an individual, for instance a name or e-mail addresses. It also includes data that indirectly relate to someone's identity, i.e. personal details such as an IP address, a card number or transaction data. Combined with other data, these details can be traced to an individual.

General Data Protection Regulation (GDPR)

European legislation regulating the careful processing and free movement of personal data. This Regulation was adopted and became applicable in all EU member states on 27 April 2016, subject to a two-year transition period to enable organizations to make their administrative and operational processes compliant with the new law, which became enforceable on 25 May 2018.

General Data Protection Regulation Implementing Act

The transposition of European legislation into domestic law, such as the Dutch Uitvoeringswet Algemene Verordening Gegevensbescherming(UAVG) ensure the GDPR is applied correctly. This Implementing Act supplements the GDPR and also carries forward elements from its predecessor legislation, the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens, WBP) or the Belgian Privacy Law of 1992.

Data Protection Authority

National regulators tasked with supervision and regulation on privacy. If you think that CCV is wrongfully processing your personal data or is not processing them correctly, and you are unable to reach agreement with us, you can get the Data Protection Authority involved (NL: AP, BE: Gba, DE: BDSG).

Financial Supervision Act

The Financial Supervision Act (Wet op het Financieel Toezicht, WFT) is a Dutch law that ensures financial markets operate effectively and safeguards the stability of the financial system. It also protects consumers and businesses against bankruptcy or objectionable actions by financial institutions.

Money Laundering and Terrorist Financing Prevention Act

The current national implementation law regarding the European Anti Money Laundering and terrorist financing regulations aimed at preventing companies from becoming involved, either knowingly or inadvertently, in money laundering or the financing of terrorist activities.

Authority for the Financial Markets

The Dutch regulator on the behaviour of financial institutions in the financial markets.

Telecommunications Act

The Dutch law (Telecommunicatiewet, TW) safeguarding the security of online networks (among other matters), and addressing consumer and privacy protection.

Data Protection Impact Assessment (DPIA)

A new work process can sometimes involve risks to your personal data. That is the reason that any new work processes of CCV is subject to a Data Protection Impact Assessment (DPIA). The GDPR sets out the requirements applicable to DPIAs.

Data controller

A person or organization that – individually or in collaboration with third parties – registers or manages personal data. The data controller is also responsible for how its data processing activities are structured and function. CCV is the data controller of the personal data of our clients.

Data processor

A person or organization that processes personal data on behalf of and on the instruction of the data controller. We are the data controller of payment data on behalf of a number of clients. A data processor and a data controller always conclude a contract setting out the terms and conditions that must be met to guarantee the security of personal data.

Client

A person that enters into a relationship with CCV, e.g. a visitor to our website, a person using our services or products, a supplier or a business partner.