VXODSGN
art direction by code

Terms & Conditions, Cardcam

VXO Design AB, Sweden

VAT-ID: SE559370502201

cardcam

Version: 1.7
Latest revision: 2024-02-08

Introduction

This document regulates the terms for the service Cardcam, digital business cards – a part of VXO Design AB. The document consists of these terms and the associated appendices regarding data processing agreements. All appendices and any amendment or additional agreements constitute an integrated part of the terms. In the event of any conflict between the content in these terms and the appendices, these terms shall prevail, and the appendices shall apply in numerical order (i.e., Appendix 1 takes precedence over Appendix 2, etc.).

Contact Person

The contact person for the provider is: Lotta Beving
Email: lotta@vxodesign.se
Phone: +46 70 – 884 21 83

Description of Service

Cardcam is a digitalized business card service where users can share their contact information through QR codes, saved directly in the user's digital wallet. The Cardcam Online Portal enables easy editing and updating of the information displayed in the QR code, ensuring that recipients always receive up-to-date information.

Payment and Invoicing

Primarily, payment is made directly at the purchase of individual Cardcams. Customers can also choose to prepay for several Cardcams at once and thus utilize any discounts. Customers may also be given the opportunity to purchase on invoice after agreement. A manual assessment is then made by VXO Design if the customer is entitled to it.

In cases where the customer has been entitled to invoicing, this occurs on a monthly basis in arrears upon issuing new business cards or updates in cases where these are charged. Payment must be made within thirty (30) days from receipt of the approved invoice and specified costs and any additional charges. Invoices are sent primarily electronically in PDF format or as e-invoice according to the buyer's specifications. Other payment methods may be agreed upon at a later date, e.g., advance payment according to agreement.

Currencies

In cases where the customer purchases services from VXO Design via the payment exchange Paddle, the base currency is Euro. Currency conversion depends on the customer's location. Special prices may apply for certain currencies. In cases where the customer is based in Sweden, the conversion is 10, i.e., 1 Euro will be charged as 10 SEK. 1 Euro is considered equal to 1 USD.

Prices

All prices excl. VAT.

- Price per new Cardcam: 49 Euro
- Setup fee: 0:-
- Monthly fee: 0:-
- Access to the portal: 0:-
- Number of portal administrators: Unlimited
- Access to support: 0:- (usually, see Customer Service section)
- Update personal information: 0:- / update
- First card design: 0:-
- Additional card design: 2* the price of a new Cardcam. Payment is primarily made by purchasing two Cardcams in the Cardcam Store (if the customer is not entitled to purchase via invoice) and leaving these unused, which can then be considered as two credits. The customer then contacts VXO Design, who designs the card and uploads it to the customer's portal, which then deducts the two credits. For purchases of more, e.g., personal design, a quote can be obtained.

Customer Service

Primarily by phone/video meeting/email, secondarily in person at VXO Design – at no cost and as soon as possible. Also, support within the municipality of Växjö is included if the order exceeds 15 cards. Other on-site support is charged with travel costs and an hourly rate of 99 Euros excl. VAT.

Contract Duration

The agreement enters into force on the day the buyer accepts the terms. The customer has the right to request at any time that their information be removed from Cardcam's system. This is done in accordance with the guidelines and terms specified in the associated data processing agreement.

Right of Withdrawal and Complaints

The customer has the right to cancel the purchase within 14 days from the day the service was activated (i.e., a Cardcam has been created), provided that the service has not begun to be used, i.e., the service has not been installed on any device. The right of withdrawal is exercised by notification to the Seller via mail/email/etc., where confirmation of the received notification shall be presented in case of dispute resolution. A fee of 25% of the purchase price will be applied.

If the delivered service is faulty, the customer has the right to make a complaint about the service. Complaints must be made within 30 days from the time the fault was discovered or should have been discovered. In the event of an approved complaint, the customer has the right to repair and redelivery in the first instance, a price reduction in the second instance, and in the third instance cancellation of the purchase.

Dispute Resolution

Disagreements should primarily be resolved through negotiation. However, a party is not prevented from taking legal action based on these terms and thereby initiating proceedings in a general court. These terms shall be interpreted and applied in accordance with Swedish law without the application of its choice of law rules.

Force Majeure

If a party is prevented from fulfilling its obligations under the terms due to circumstances beyond the party's control, which the party could not reasonably have been expected to anticipate at the time of entering into the terms, and cannot reasonably overcome or circumvent, such circumstances shall constitute a basis for exemption that leads to the postponement of agreed times for performance and relief from liability for damages and other possible penalties.

VXO Design AB shall not be held responsible for functional failures caused by third-party providers, including but not limited to Apple Wallet and Google Wallet, which may change, remove, or otherwise modify functions and services that Cardcam depends on.

Data Protection

We, as data processors, commit to protecting your personal data and will treat all such information in accordance with our Privacy Policy and applicable data protection laws. See appendices for detailed information.

User's Responsibility

You are responsible for ensuring that all information uploaded to the Cardcam service is accurate and does not violate any laws or third-party rights.

Changes to Terms

We reserve the right to change these terms at any time. The updated terms will be published on our website and notified at least two months plus the current month to existing purchasers for them to be valid.

Appendices:

- Data Processing Agreement – Sent in cases where DPA proposes for DPA agreement
- Data Processing Agreement – Appendix 1 - Specification
- Data Processing Agreement – Appendix 2 - Security Measures

Acceptance

These terms are accepted by the purchaser by ticking the box "I accept the terms" in connection with the purchase. The purchaser also confirms that they are authorized to bind the company to these terms and that they accept the terms in their entirety.

APPENDIX 1 - SPECIFICATION

Purpose

This Appendix 1 (Specification) specifies the processing of Covered Personal Data that the Data Processor performs on behalf of the Data Controller under the Data Processing Agreement.

The purpose of this Appendix 1 (Specification) is to clarify which processing and personal data are covered by the Data Processing Agreement and to fulfill the requirements of Applicable Data Protection Legislation regarding the obligation to specify categories related to a Data Processor's processing of personal data, see for example Article 28.3 GDPR.

Description of Processing of Covered Personal Data

<table>
<tr><td>The subject matter of the processing of personal data, as well as the nature and purpose of the processing</td><td>The DPA shall, as described in the Service Agreement, deliver the Cardcam service for digital business cards. The purpose of the personal data processing is to spread the registrant's contact information using QR codes.</td></tr>
<tr><td>Type of personal data</td><td>The following categories of Covered Personal Data are processed:
Contact information, e.g., first name, last name, email address, phone number, personal link</td></tr>
<tr><td>Categories of registrants</td><td>Employees at the Data Controller</td></tr>
<tr><td>Duration of the processing</td><td>Covered Personal Data will, unless the Data Controller instructs otherwise, be processed during:
For the duration of the Service Agreement and a maximum of 30 days thereafter</td></tr>
<tr><td>General description of technical and organizational security measures</td><td>The parties agree, without limiting their respective commitments regarding information security, that the Data Processor shall take the following security measures:
Security measures described in Appendix "Security Measures for Data Processing Agreement" to the Data Processing Agreement</td></tr>
<tr><td>Approved subcontractors</td><td>The following shall apply for the Data Processor's use of subcontractors for processing of Covered Personal Data:

The Data Processor is permitted to hire the subcontractors listed in the table below for the processing of Covered Personal Data:<table><tr><td><u>Subcontractor</u></td><td><u>Type of service</u></td></tr><tr><td>Digital Ocean, Germany
Google</td><td>Server
Data Center (only for Android phones)</td></tr></table>
The Data Processor shall inform the Data Controller about changes in accordance with the Data Processing Agreement.</td></tr>
</table>

Location of processing and transfer to third countries Covered Personal Data may only be processed at the following locations	• Within Sweden • Within the European Union (EU) or the European Economic Area (EEA) • For digital business cards issued for Android, the information shared is stored at Google's Datacenter. Data is primarily stored at data centers within the EU/EEA but may, in exceptional cases by Google, be distributed to data centers outside the EU/EEA. In these exceptional cases, data is stored in a distributed manner, meaning different data are stored at different locations in order to separate and prevent intrusion. Data is also stored in several different security layers and, of course, encrypted. More information about Google's secure servers and locations is available at https://www.google.com/about/datacenters/data-security/ and https://www.google.com/about/datacenters/locations/

APPENDIX 2 - SECURITY MEASURES

The Data Processor shall:

- Implement technical and organizational security measures to protect personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable laws.
- Ensure that these measures reflect the latest technological development, risks, and costs.
- Guarantee that employees and others who have access to the personal data are bound by confidentiality and follow guidelines from the Data Controller.
- Include, where appropriate, pseudonymization, encryption, and the ability to restore data following incidents.
- Monitor and report any deficiencies or incidents to the Data Controller promptly.
- If subcontractors are used, ensure that they comply with the same requirements set out in this agreement and inform the Data Controller of any changes.
- Regularly update their security measures in light of changes in technology and the threat landscape.

The Data Processor shall implement and maintain appropriate technical and organizational security measures to protect personal data without the right to special compensation for this.

The security measures of the Data Processor shall achieve the level of protection required by applicable law and, upon its entry into force, the General Data Protection Regulation (GDPR), and otherwise be appropriate considering technical possibilities, implementation costs, specific risks with the processing, and the extent to which the processed personal data is, or is likely to be perceived as, sensitive.

The Data Processor is responsible for conducting its operations in a way that ensures adequate information security. The Data Processor shall ensure that employees, consultants, and others for whom the Data Processor is responsible, who process or have access to the personal data, are bound by an appropriate confidentiality commitment and are informed about how personal data processing may occur in accordance with instructions from the Data Controller.

The technical and organizational security measures of the Data Processor shall be taken considering the latest development, implementation costs, the nature, scope, context, and purposes of the processing, including risks to the rights and freedoms of natural persons of varying likelihood and severity, to ensure an appropriate level of security relative to the risk.

The implementation of security measures by the Data Processor shall, where appropriate, include pseudonymization and encryption of personal data, the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security, special consideration shall be given to the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. The Data Processor shall regularly monitor the effectiveness of its security measures and report any deficiencies or incidents to the Data Controller without undue delay. This includes serious security incidents that may have affected the integrity, confidentiality, or availability of the personal data.

If the Data Processor engages subcontractors to process personal data, these subcontractors must meet the same requirements for security measures and data protection as those set out in this agreement. The Data Processor shall inform the Data Controller about the use of new or changed subcontractors and ensure that there is a written agreement with each subcontractor.

Considering the continuous development of technology and changes in the threat landscape, the Data Processor commits to regularly updating and improving its security measures to continue providing a level of protection that is appropriate relative to the identified risks.

VXO Design AB, 2023-06-03