DSGVO Posmodule.com

Allgemeine Beschreibung

Das Posmodule speichert und verarbeitet Rechnungsdaten um diese gemäß RKSV zu signieren. Dafür muss Posmodule als Addon zu Shopify durch den Shopify-Benutzer (Shop-Betreiber) hinzugefügt werden. Danach läuft der Signaturprozess im Hintergrund transparent und automatisch ab. Nach der erfolgreichen Signatur einer Rechnung wird ein Bon dann zurück an den Shopbetreiber geschickt, welcher dort vor Ort ausgedruckt werden kann.

Technische Beschreibung Installation

PosModule ist ein Addon für Shopify. Es wird mittels des OAuth Verfahrens in eine bestehende Shop-Umgebung eingebunden. Der Benutzer ist daher schon Kunde von Shopify und fügt wissentlich das PosModule Addon hinzu (Installation). Durch die Installation des Addon werden folgende Informationen des Shopbetreibers heruntergeladen: Shop Name, Anschrift, Emailadresse. Weiters wird vom Shopbetreiber die ATU Nummer und etwaige Kontaktdaten wie eine Telefonnummer abgefragt und gespeichert. Dies wird benötigt um die korrekte Funktionalität vom PosModule zu gewährleisten.

Technische Beschreibung Kassa-Kauf

Durch die Installation des PosModule werden noch keine Rechnungsdaten ausgetauscht. Hierfür muss der Shop-Betreiber im Addon zusätzlich für jeden Standort eine virtuelle Kassa kaufen. Der Kassenkauf läuft direkt über die Shopify Platform und es werden keine Kreditkartendaten oder ähnliches ausgetauscht. Stattdessen wird die Kassa direkt über Shopify abgerechnet und von Shopify dem Benutzer verrechnet.

Zusätzlich wird beim Kauf einer Kasse optional die iPad UID des Shopbetreibers gespeichert. Diese dient zum Rücksenden des signierten Bons welches anschließend im Shop ausgedruckt wird.

Datentransfer von Shopify zu PosModule (Upload Webhooks)

Durch den Kassenkauf werden s.g. Webhooks eingerichtet. Das bedeutet, dass das PosModule automatisch beim erfolgreichen Verkauf an Kunden des Shopbetreibers mit den Rechnungsdetails informiert wird. Diese Informationen inkludieren:

1. Rechnungsdetails, wie Artikelnamen, Anzahl, Preis, MwSt-Satz
2. Etwaige Kundendaten von Shopbetreibern werden zwar mitgesandt, aber nicht weiter verarbeitet und vor dem Speichern entfernt.
3. Versanddaten und Anschrift von Dritten werden ebenfalls entfernt und nicht gespeichert.

Diese Daten werden teilweise verworfen und teilweise gespeichert. Der Detailgrad der Daten kann technisch nicht anders realisiert werden, da Shopify selbst diese Daten so (und nur so) zur Verfügung stelle. s.g. Webhooks Daten von Shopify zum PosModule gesendet. Das PosModule verwendet den `Order/New` und `Order/Update` sowie den `refunds/create` Webhook. Mehr Informationen sind auf der Shopify Website ersichtlich: https://help.shopify.com/api/reference/webhook

Eine typische Payload eines WebHooks ist in folgendem JSON-Snippet ersichtlich:


```
{"id":353147027511,"email":"","closed_at":null,"created_at":"2018-04-11T11:13:58+02:00","updated_at":"2018-04-11T11:14:00+02:00","number":75536,"note":null,"token":"67d9ade5aa7b8
```

ada8676aeaa9a85de83","gateway":"cash","test":false,"total_price":"9.
90","subtotal_price":"9.90","total_weight":0,"total_tax":"1.65","tax
es_included":true,"currency":"EUR","financial_status":"paid","confir
med":true,"total_discounts":"0.00","total_line_items_price":"9.90","
cart_token":null,"buyer_accepts_marketing":false,"name":"#76536","re
ferring_site":null,"landing_site":"\/admin\/checkouts.json","cancell
ed_at":null,"cancel_reason":null,"total_price_usd":"12.20","checkout
_token":"bafbb1bf841506d3bd5bc3a95da7b0de","reference":null,"user_id
":100951495,"location_id":10160199,"source_identifier":"10160199-13-
15247","source_url":null,"processed_at":"2018-04-
11T11:13:58+02:00","device_id":13,"phone":null,"customer_locale":"en
","app_id":129785,"browser_ip":null,"landing_site_ref":null,"order_n
umber":76536,"discount_codes":[],"note_attributes":[],"payment_gatew
ay_names":["cash"],"processing_method":"cash","checkout_id":95703446
3287,"source_name":"pos","fulfillment_status":"fulfilled","tax_lines
":[{"title":"MwSt","price":"1.65","rate":0.2}],"tags":"","contact_em
ail":null,"order_status_url":"https:\/\/the-viennastore-
2.myshopify.com\/11193508\/orders\/67d9ade5aa7b8ada8676aeaa9a85de83\
/authenticate?key=e7b804ea4e6fc6232aca29aed29e533c","line_items":[{"
id":750524989495,"variant_id":20193425031,"title":"Wien Gin klein 40
ml","quantity":1,"price":"9.90","sku":"","variant_title":"","vendor"
:"Kesselbr\u00fcder","fulfillment_service":"manual","product_id":632
7416903,"requires_shipping":true,"taxable":true,"gift_card":false,"n
ame":"Wien Gin klein 40
ml","variant_inventory_management":"shopify","properties":[],"produc
t_exists":true,"fulfillable_quantity":0,"grams":0,"total_discount":"
0.00","fulfillment_status":"fulfilled","tax_lines":[{"title":"MwSt",
"price":"1.65","rate":0.2}],"origin_location":{"id":701425607,"count
ry_code":"AT","province_code":"","name":"THE
VIENNASTORE","address1":"Herrengasse
5","address2":"","city":"Wien","zip":"1010"}}],"shipping_lines":[],"
fulfillments":[{"id":333935968311,"order_id":353147027511,"status":"
success","created_at":"2018-04-
11T11:13:58+02:00","service":"manual","updated_at":"2018-04-
11T11:13:59+02:00","tracking_company":null,"shipment_status":null,"t
racking_number":null,"tracking_numbers":[],"tracking_url":null,"trac
king_urls":[],"receipt":[],"line_items":[{"id":750524989495,"variant
_id":20193425031,"title":"Wien Gin klein 40
ml","quantity":1,"price":"9.90","sku":"","variant_title":"","vendor"
:"Kesselbr\u00fcder","fulfillment_service":"manual","product_id":632
7416903,"requires_shipping":true,"taxable":true,"gift_card":false,"n
ame":"Wien Gin klein 40
ml","variant_inventory_management":"shopify","properties":[],"produc
t_exists":true,"fulfillable_quantity":0,"grams":0,"total_discount":"
0.00","fulfillment_status":"fulfilled","tax_lines":[{"title":"MwSt",
"price":"1.65","rate":0.2}],"origin_location":{"id":701425607,"count
ry_code":"AT","province_code":"","name":"THE
VIENNASTORE","address1":"Herrengasse
5","address2":"","city":"Wien","zip":"1010"}}]}],"client_details":{"
browser_ip":"188.20.241.252","accept_language":"de-
at","user_agent":"Shopify POS\/4.4.3 (iPad; iOS 11.3;
Scale\/2.00)","session_hash":null,"browser_width":null,"browser_heig
ht":null},"refunds":[]}

Danach wird unterschieden ob der Verkauf als POS Verkauf (also Bar-Verkauf) oder als Online-Shop verkauf getätigt wurde. Nicht-POS-Verkäufe werden verworfen und nicht gespeichert. Bar-Verkäufe werden zur weiteren Verarbeitung auf unbestimmte Zeit gespeichert.

Danach werden alle Transaktionen zu einem Webhook von den Shopify-Servern heruntergeladen. Diese werden dann mit bereits signierten Transaktionen abgeglichen und gegebenenfalls unsignierte Transaktionen werden signiert. Dabei wird intern der Umsatzzähler hinaufgezählt.

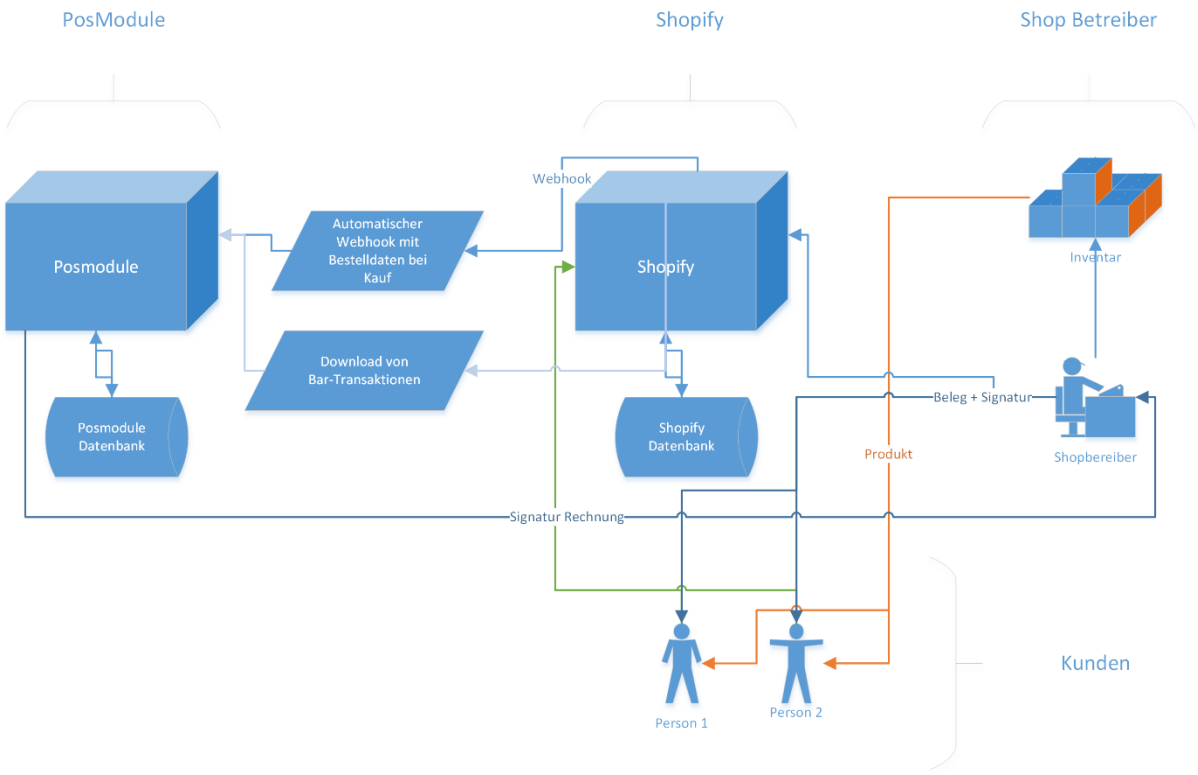
Eine typische Payload solch einer Transaktion ist in diesem JSON-Snippet ersichtlich:


```
{"id":592004907101,"order_id":467354615901,"amount":"80.00","kind":"
sale","gateway":"external-debit","status":"success","message":"Paid
via external-debit","created_at":"2018-04-
11T11:03:54+02:00","test":false,"authorization":null,"currency":"EUR
","location_id":244544,"user_id":107644232,"parent_id":null,"device_
id":717300,"receipt":{},"error_code":null,"source_name":"pos"}
```


Nach dem erfolgreichen Signieren wird die Signatur als QR Code zurück an das IPad des Shopbetreibers gesendet.

Der Versand der Daten erfolgt in verschlüsselter Weise (SSL, HTTPS).

Folgende Zeichnung zeigt den kompletten Informationsfluss schematisch auf:



Datentransfer von PosModule zu A-Trust

Um die Signatur zu generieren wird ein externes Service von A-Trust verwendet. Eine Signatur besteht aus den nach Steuersätzen getrennten Summen einer Rechnung. Es werden keine Persönlich Identifizierbaren Daten an A-Trust versendet, lediglich aggregierte Rechnungssummen (keine Einzelartikel). Diese werden dann von A-Trust mittels eines Zertifikats signiert und die Signatur wird anschließend dem Benutzer zur Verfügung gestellt.

Technische und Organisatorische Maßnahmen

Als Datenverarbeiter unterliegt das PosModule nicht nur der DSGVO, sondern auch alle Sub-Verarbeiter. PosModule hat hierzu von allen Service-Anbietern entsprechende Abkommen eingeholt, welche persönliche Daten verarbeiten oder speichern. Entsprechende Abkommen können über die Websites von Google:

https://cloud.google.com/terms/data-processing-terms

und

https://cloud.google.com/terms/eu-model-contract-clause

eingesehen werden. Darüber hinaus stellt PosModule sicher, dass die Technischen und Organisatorischen Maßnahmen intern erfüllt werden. Folgend eine Auflistung der Sicherheitsmaßnahmen und deren Anwendung.

Ort der Datenverarbeitung - Allgemein

PosModule betreibt virtuelle Server in der Google Cloud Engine. Hierzu sind Kubernetes container so eingerichtet, dass es keinerlei Wartung bedarf. Als Datencenter wurden sowohl für die Arbeitscontainer, als auch für die Datenbank Frankfurt, Deutschland gewählt.

All relevanten Informationen hierzu findet man bei Google: https://cloud.google.com/security/gdpr/

Es haben im Allgemeinen drei Personen Zugriff auf die Daten, Container und den Administrationsbereich, wobei diese durch eigene Benutzer getrennt sind. Die Benutzer sind typische Google Accounts welche der Google Cloud Engine mit bestimmten Rechten hinzugefügt werden können.

Martin Moschitz – Vollzugriff

Christian Nösterer – Admin Zugriff

Thomas Wiesner – Admin Zugriff

Weiters betreibt PosModule zwei Repositories für den eigentlichen Source-Code. Der Source Code ist in zwei Teile geteilt: ein PHP Backend welches die Admin-Konsole für Shopbetreiber bildet und ein Java-Backend welches für die Signaturen verantwortlich ist. Der Source-Code (ohne Benutzerdaten) liegt bei Bitbucket als Private Repositories. Die entsprechenden Abkommen können hier eingesehen werden:

https://www.atlassian.com/blog/announcements/atlassian-and-gdpr-our-commitment-to-data-privacy
https://www.atlassian.com/trust/privacy

Folgende Personen haben Zugriff auf den Source Code:

Thomas Wiesner – Vollzugriff

Christian Nösterer – Schreiben/Lesen

Zutrittskontrolle

Google gewährleistet durch die eigenen Datenzentren, dass ausschließlich autorisiertes Personal Zutritt erhält. PosModule selbst oder Mitarbeiter von PosModule haben keinen Zutritt zur Infrastruktur.

Zugangskontrolle

Zugang zur Administration der Server/Container kann ausschließlich über die Admin-Konsole erlangt werden. Benutzer müssen der Admin-Konsole über deren Google Account hinzugefügt werden. Dies ist nur Personen mit Vollzugriff möglich.

Zugriffskontrolle

Zugang zu den eigentlichen Daten haben gemäß Beschreibung ausschließlich die Personen welche unter „Ort der Datenverarbeitung“ aufgelistet sind, sowie Personen entsprechend der Datenverarbeitungs-Abkommen mit Google.

Benutzerkontrolle

Keine weiteren Personen als die Beteiligten Gründer (unter „Ort der Datenverarbeitung“ gelistet) haben Zugriff auf die Daten, außer der Benutzer selbst auf seine eigenen Benutzerdaten.

Durch das interne Design des PosModule können Unbefugte nicht auf die Persönliche Daten zugreifen. Es wird unterschieden: Persönliche Daten und Rechnungs-Daten.

Rechnungs-Daten: Die Rechnungsdetails werden zusammengefasst und ausschließlich die Gesamtsumme nach Steuersätzen aufgeschlüsselt wird danach weiterverarbeitet. Diese aggregierten Daten können von Benutzern über einen speziellen Link heruntergeladen und ausgedruckt werden (Signierter Bon).

Persönliche Daten (des Shopbetreibers): Können nur über die Shopify-Administrationsoberfläche eingesehen und geändert werden. Hierzu wird ein OAuth Mechanismus verwendet welcher garantiert, dass nur der richtige eingeloggte Benutzer auf die Daten zugriff erhält.

Persönliche Daten (der Kunden des Shopbetreibers): Werden nicht gespeichert und gegebenenfalls schon vor der Verarbeitung entfernt.

Übertragungskontrolle

Aus Administrations-Sicht: Es kann in der Google Cloud Console jederzeit überprüft und mitprotokoliert werden, wer wann auf welche Daten zugegriffen hat.

Aus User-Sicht: Daten werden bei Shopify eingegeben, danach an das PosModule automatisch übertragen. PosModule benutzt dann die Rechnungsdaten um eine Summe nach Steuersätzen zu ermitteln und schickt diese dann an die A-Trust weiter. Danach werden die Summen nach Steuersätzen, sowie die Signatur und das Rechnungsdatum als Download bereitgestellt. Alternativ kann der Benutzer auch einen „Automatischen Bondruck“ einstellen, wobei dann automatisiert die Signatur, die Summen nach Steuersätzen sowie das Rechnungsdatum an das iPad versandt werden. Der Versand erfolgt über verschlüsselte HTTPS Verbindungen, wobei das iPad über VoIP Push Nachrichten über das Vorliegen einer neuen Signatur zum Download informiert wird.

Eingabekontrolle

Daten werden ausschließlich am Beginn der Registrierung eingegeben und der Zeitpunkt wird festgehalten. Nachträgliche Änderungen sind nicht automatisiert möglich.

Transportkontrolle

Alle personenbezogenen Daten beinhaltenden Schnittstellen sind ausschließlich über verschlüsselte Verbindungen erreichbar. Es besteht die Weisung, dass personenbezogene Daten beinhaltende Datensätze nicht unverschlüsselt übertragen oder gespeichert werden. Vorhandene Datensätze dürfen außerhalb vom Produktivbetrieb nicht länger als 7 Tage gespeichert werden.

Wiederherstellung

Es werden über Google Cloud-Dienste regelmäßig Backups angefertigt. Diese sind im Störfall einfach wiederherzustellen. Ist durch den Störfall eine Signaturerstellung nicht möglich so wird Shopify darüber informiert und sendet entsprechende Webhooks wiederholt über einen Zeitraum von 48 Stunden. Datenbank-Sicherungen werden im Abstand von mindestens einem Tag angefertigt und direkt bei Google in Frankfurt gespeichert.

Datenintegrität

Durch interne Monitoring-Verfahren werden Fehler unmittelbar nach dem Auftreten an alle Beteiligten gemeldet. Monitoring basiert hier auf zwei Methoden. Signaturverfahren werden auf ihre Funktionalität geprüft und bei einem Ausfall der Signaturerstellungseinheit (oder einem Fehler) wird ein Email versandt. Dies bedeutet, dass bei Ausfall oder Störfall der A-Trust API zum Signieren von Rechnungen Emails an alle Beteiligten mit dem entsprechenden Fehler versandt werden.

Auf der Infrastruktur selbst ist ein Monitoring von Google in Betrieb welches die Server-Container ununterbrochen überwacht und bei Überschreiten gewisser Parameter alle Beteiligten informiert.

Google Cloud und Kubernetes Container sind Wartungsfrei und bedürfen keinerlei Updates der Infrastruktur. Dies bedeutet, dass die Software auf einer „managed Infrastructure“ läuft.

Datenerhebung, Aufbewahrung und Löschung

PosModule behält sich das Recht vor Benutzerdaten für einen Zeitraum von mindestens 24 Monaten aufzuheben. Sofern diese dann nicht mehr gebraucht werden, werden die Daten am 1. Juni bzw. 1. Dezember manuell entfernt. Folgende Daten werden auf jeden Fall aber weiterhin aufgehoben und für die einwandfreie Funktionalität von PosModule benötigt:

1. Email, Anschrift und UID von aktiven Benutzern (um neue Kassen kaufen zu können)
2. Das Datenerfassungsprotokoll
3. Die Laufenden Rechnungsdaten mit internen Belegnummern von noch aktiven Kassen

Folgende Daten werden jedenfalls gelöscht:

1. Bereits seit 24 Monaten inaktive Benutzer

Recht auf Datenerhebung und Löschung

Jeder Benutzer hat das Recht auf „vergessen werden“, sowie darüber informiert zu werden welche Daten gespeichert werden. Dazu ist es möglich eine Anfrage per Email zu stellen. Die dazugehörige Email-Adresse ist office@posmodule.com

PosModule behält sich das Recht vor durch Löschungsaufforderungen etwaige vorhandene Verträge zu kündigen, wenn ein einwandfreier Betrieb nicht mehr gewährleistet werden kann.

Graz am 12. Mai 2018