

# Third-Party-Cookies - Browser-Cookies und Session-Handling

- [Einführung und kurze Problembeschreibung](#)
- [Mögliche Lösungen](#)
  - [Computop Paygate-Parameter "Custom"](#)
  - [Zusätzliche Weiterleitung nach Rückkehr des Käufers in Ihrem Shop](#)
  - [Anpassen der Cookie-Definition](#)
- [Betroffene Implementierungen](#)

## Einführung und kurze Problembeschreibung

Aktuelle Webbrowser blockieren immer häufiger sogenannte Cookies von Drittanbietern, um die Privatsphäre des Internetnutzers zu schützen. Viele Shop-Implementierungen benutzen jedoch für das sog. Session-Handling genau diese Cookies, um dort beispielsweise die SessionId zu speichern.

Durch das Blockieren dieser Cookies verliert der Shop des Händlers die Informationen (z. B. SessionId), wenn der Käufer zu den Paygate-Zahlungsseiten weitergeleitet wurde und nach Abschluss der Zahlung zum Shop zurückkehrt.

## Mögliche Lösungen

### Computop Paygate-Parameter "Custom"

Sie können den Paygate-Parameter "Custom" verwenden, um einen benutzerdefinierten Parameter (wie sessionId oder mehr) an Paygate zu übergeben, und Paygate gibt Ihre "Custom"-Werte zurück, wenn der Verbraucher zu Ihrem Shop zurückkehrt.

Der Parameter "Custom" ist nicht verschlüsselt. Mehrere Parameter können durch "|" getrennt in der Anfrage verkettet werden und werden in der Antwort durch "&" getrennt zurückgegeben. Dies ermöglicht eine sehr einfache Implementierung.

Beispiel für einen Request: `Custom=sessionId=123|customerId=456`

Beispiel für eine Antwort: `sessionId=123&customerId=456`

### Zusätzliche Weiterleitung nach Rückkehr des Käufers in Ihrem Shop

Nach einer erfolgreichen Zahlung wird der Käufer zu der URL "URLSuccess" umgeleitet, die Sie im Zahlungsrequest angegeben haben.

Bei der ersten Weiterleitung ignoriert der Webbrowser das gespeicherte Cookie – da diese Weiterleitung von einem Drittanbieter Paygate initiiert wurde – und die sessionId geht verloren.

Sobald Sie eine zweite Weiterleitung in Ihrem Shop initiieren, unmittelbar nachdem der Käufer zurückgeleitet wurde, wird das erneut Cookie geladen – da diese Weiterleitung von der ursprünglichen Seite initiiert wurde.

### Anpassen der Cookie-Definition

Sie können beim Erzeugen des Cookies sog. Drittanbieter explizit zuzulassen. Bitte beachten Sie die Browserkompatibilität, wenn Sie diese Option verwenden.

Ein Cookie wird normalerweise mit folgenden Informationen erstellt:

```
Set-Cookie: sessionId=<your-sessionId>; Domain=<your-domain>; Path=/; HttpOnly; Secure
```

Fügen Sie das Attribut Secure hinzu. SameSite = None (SameSite = None arbeitet nur mit Secure zusammen) beim Erstellen des Cookies mit Ihrer sessionId:

```
Set-Cookie: sessionId=<your-sessionId>; Domain=<your-domain>; Path=/; HttpOnly; Secure; SameSite=None
```

Stellen Sie daher sicher, dass diese Attribute entsprechend definiert sind. Diese bedeuten:

Attribut	Beschreibung
sessionId	Key / Value, den Sie im Cookie speichern möchten, z. sessionId, sessionid, id, SESSIONID, ...
Domain	Best Practice: Stellt sicher, dass der Webbrowser nur die von dieser Domäne gespeicherten Cookie-Werte liest (z. B. <a href="#">shop.merchant.com</a> ).
Path	Best Practice: Dieser Pfad muss in der URL vorhanden sein. Andernfalls sendet der Browser das Cookie nicht.
HttpOnly	Best Practice: Stellt sicher, dass JavaScript nicht auf das Cookie zugreifen kann

Secure	Best Practice: Das Cookie wird nur dann an den Server gesendet, wenn die Anforderung über https erfolgt. So wird sichergestellt, dass vertrauliche Informationen nicht unverschlüsselt über http gesendet werden.
SameSite	Neu: Dieses Attribut deaktiviert das Blockieren von Cookies von Drittanbietern, sodass die Informationen verfügbar sind, nachdem der Käufer in Ihren Shop zurückgekehrt ist. Bitte beachten Sie, dass dieses Attribut nur funktioniert, wenn auch Secure verwendet wird.

## Betroffene Implementierungen

- Kreditkartenzahlungsformular "[paySSL.aspx](#)"
- SEPA-Lastschrift-Zahlungsformular "[PaySDD.aspx](#)"
- Hosted Payment Page "[paymentPage.aspx](#)"