

# Datenschutz-Erklärung des „Cellarium“-Klosterladens

26. März 2018

## 1. Präambel

Der „Cellarium“-Klosterladen bietet diverse Waren, größtenteils aus Klöstern und von Ordensgemeinschaften, im Rahmen diverser Verkaufsausstellungen sowie online über den „Cellarium“-Online-Shop (<http://www.cellarium.at>) an. Personenbezogene Daten werden ausschließlich bei Käufen im Online-Shop erfasst.

Dann, wenn ein Kunde des Online-Shops eine Ware in den Einkaufskorb legt, wird eine Session für diese Transaktion in der Datenbank angelegt, die zunächst nur die IP-Adresse des zugreifenden Rechners und die gewählten Waren enthält und über eine eindeutige ID identifiziert wird. Kundendaten werden erst mit Beginn des eigentlichen Bestellvorganges erfasst; spätestens zu diesem Zeitpunkt (oder bei der Erstellung einer Anfrage über die Kontaktseite der Website) wechselt die Seite von HTTP zu HTTPS. Bei einer Bezahlung mit PayPal® werden die benötigten Kundendaten größtenteils über die PayPal®-Seite zur Verfügung gestellt; bei einer Bestellung gegen Rechnung werden die Daten vom Kunden selbst eingegeben. Der „Cellarium“-Online-Shop verwendet aus grundsätzlichen Erwägungen keine wie immer gearteten *User Tracking*- oder *Profiling*-Strategien. Der für Kunden zugängliche Teil des „Cellarium“-Online-Shops kommt ohne die Verwendung von Cookies aus.

## 2. Kundendaten – Bestellungen im „Cellarium“-Online-Shop

### 2.1. Erfasste bzw. gespeicherte Daten

- Browsertyp, Art des Zugriffs (mit/ohne JavaScript), IP-Adresse und -Name, Beginn und Abschluss der Session
- Bestellte Waren
- Zahlungsart (PayPal® oder Rechnung)
- Name (verpflichtend bei Bestellung), Titel
- Mailadresse (verpflichtend bei Bestellung)
- Telefonnummer (verpflichtend bei Bestellung)
- Lieferadresse (verpflichtend bei Bestellung)
- Rechnungsadresse (optional, wenn unterschiedlich von der Lieferadresse)
- Bemerkungen des Kunden
- Beim Kauf von alkoholischen Produkten: rechtsverbindliche Erklärung des Kunden, das Mindestalter für den Erwerb dieser Produkte erreicht zu haben
- Diverse Informationen zu PayPal-Transaktionen
- Zeitpunkt von Zahlung, Versand und internem Abschluss der Bestellung
- Soweit es automatisiert möglich war, eine Rechnung (einschließlich Transportkosten) zu erstellen, die Rechnung (bei PayPal®-Zahlung saldiert), ansonsten ein Angebot über die erstellten Waren.

### 2.2. Verwendung

Die erfassten Informationen sind erforderlich für die Abwicklung von Kauf, Zahlung und Versand der bestellten Waren. Die Transaktions-Informationen dienen gegenüber der Finanzbehörde als Beleg für den erfolgten Verkauf. Ein Zugriff auf die Daten ist über ein authentisiertes Administrationssystem ausschließlich den Eigentümern des „Cellarium“-Klosterladens möglich.

Bestellvorgänge, die ohne Eingabe von Kundendaten abgebrochen wurden, werden innerhalb von maximal 30 Tagen gelöscht; nicht abgeschlossene Bestellungen, bei denen bereits Kundendaten eingegeben wurden, werden so lange aufbewahrt, bis durch Rückfrage beim Kunden geklärt ist, ob der Abbruch der Bestellung versehentlich oder mit Absicht erfolgte, und dann ebenfalls gelöscht.

### **2.3. Einsichtmöglichkeit**

Kunden erhalten die von ihnen eingegebenen Daten vor dem Abschluss der Bestellung zur Kontrolle und allfälligen Korrektur nochmals angezeigt. Beim Abschluss der Bestellung erhalten sie eine Rechnung oder ein Angebot, die bzw. das die von ihnen eingegebenen Daten enthält. Es liegt in ihrem Ermessen, den „Cellarium“-Klosterladen über allfällige Fehler oder sonstige Mängel in diesen Daten in Kenntnis zu setzen. Fehlerhafte oder unvollständige Adressdaten können aber die Lieferung der bestellten Waren verzögern oder verhindern.

### **2.4. Weitergabe von Daten**

Eine Weitergabe von Daten, die der „Cellarium“-Klosterladen im Rahmen der Bestellungen von Kunden erhalten hat, an Dritte ist prinzipiell nicht vorgesehen. Davon ausgenommen ist der Versand von Waren durch eine vom „Cellarium“-Klosterladen beauftragte Versandfirma, der Name und Adresse des Empfängers und die zu versendenden Waren übergeben werden müssen. Darüber hinaus werden Kundendaten aber unter keinen Umständen an Dritte weitergegeben.

Bei einer Bezahlung über PayPal® im Zuge einer Transaktion wird an PayPal® nur der in Rechnung gestellte Gesamtbetrag übergeben, aber keine Details über die bestellten Waren und auch keine Kundendaten. (PayPal® seinerseits stellt hingegen dem „Cellarium“-Online-Shop den Namen der Käuferin / des Käufers und eine Lieferadresse zur Verfügung.)

### **2.5. Auskunftsrecht**

Jeder Person wird das Auskunftsrecht über die im „Cellarium“-Klosterladen potenziell über sie gespeicherten Informationen zugestanden.

### **2.6. Recht auf Berichtigung**

Kundendaten werden grundsätzlich bei jedem Kaufvorgang neu erhoben, entweder durch direkte Eingabe durch den Kunden oder bei einer Zahlung über PayPal® als Übergebatedaten aus PayPal®. Eine Berichtigung nach einem erfolgreichen Abschluss eines Kaufvorgangs ist daher weitgehend irrelevant; zuvor ist eine allfällige Berichtigung nicht nur möglich, sondern sogar erwünscht (siehe Punkt 2.3).

### **2.7. Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht**

Unter Berücksichtigung der gesetzlichen, insbesondere auch finanzrechtlichen, Randbedingungen und wichtiger Interessen des „Cellarium“-Klosterladens wird Anträgen auf Löschung von Kundendaten entsprochen. Soweit technische Gründe einer völligen Löschung von Transaktionsdaten entgegenstehen, aber eine Löschung unter den vorgenannten Randbedingungen grundsätzlich möglich ist, können die Kundendaten auf Wunsch so unkenntlich gemacht werden, dass eine Zuordnung zu einer bestimmten Person nicht mehr möglich ist. Abgesehen von der gesetzlich vorgeschriebenen buchhalterischen Verarbeitung von Kaufvorgängen werden die Transaktions-Daten in keiner Weise, etwa für Zwecke des Profilings, weiterverarbeitet; Zugriffe auf die Seiten des „Cellarium“-Online-Shops werden nur in neutralisierter Form statistisch ausgewertet.

## **2.8. Recht auf Datenübertragbarkeit**

Da jede Transaktion im „Cellarium“-Online-Shop in sich abgeschlossen und nicht mit allfälligen weiteren Transaktionen des gleichen Kunden verknüpft ist, ist die Menge der gespeicherten Daten im Wesentlichen auf den Inhalt der erstellten Rechnung oder des Angebots beschränkt, die dem Kunden ohnedies zugegangen sind. Grundsätzlich können Kundendaten aber in einem gängigen Format zur Verfügung gestellt werden.

## **2.9. Dauer der Datenspeicherung**

Die Speicherdauer von Transaktions-Datensätzen hängt vom finalen Status der Transaktion ab:

- Vor Eingabe von Kundendaten abgebrochene Kaufvorgänge: Werden innerhalb von 30 Tagen gelöscht, sobald sie mindestens einen Tag alt sind (um das Löschen gerade eben durchgeführter, noch nicht abgeschlossener Aktionen zu verhindern).
- Nach Eingabe von Kundendaten abgebrochene Kaufvorgänge: Werden gelöscht, sobald Kontakt mit dem Kunden aufgenommen und geklärt wurde, ob der Abbruch beabsichtigt oder unbeabsichtigt erfolgte; jedenfalls innerhalb von 30 Tagen.
- Abgeschlossene Kaufvorgänge: Die Daten müssen zumindest für die finanzrechtlich vorgesehene Aufbewahrungsfrist von sieben Jahren auch in elektronischer Form gespeichert bleiben. Da es jedoch nicht wahrscheinlich ist, dass der „Cellarium“-Online-Shop im Zusammenhang mit einem Kaufvorgang von sich aus mehr als drei Monate nach dem Kaufvorgang Kontakt aufnehmen muss, werden aus den elektronisch gespeicherten Kundendaten E-Mail-Adresse und Telefonnummer jedenfalls schon nach drei Monaten gelöscht. Da allerdings allfällige Rechtsansprüche von Kunden bis zu 30 Jahre nach Kaufabschluss geltend gemacht werden können, müssen in den (seltenen) Fällen, in denen Schadenersatz-Forderungen nicht denkunmöglich sind, die für eine Nachvollziehung des Kaufvorgangs erforderlichen Dokumente für diesen Zeitraum in einem gegen unberechtigte Zugriffe gesicherten Archiv aufbewahrt werden.

## **3. Kundendaten – Anfragen über die Kontaktseite des „Cellarium“-Online-Shops**

### **3.1. Erfasste bzw. gespeicherte Daten**

- Browsertyp, Art des Zugriffs (mit/ohne JavaScript), IP-Adresse und -Name, Beginn und Abschluss der Session
- Name (verpflichtend)
- Mailadresse (verpflichtend)
- Telefonnummer (optional)
- Bemerkungen des Kunden

### **3.2. Verwendung**

Die erfassten Informationen sind erforderlich für die Beantwortung von Anfragen über die Kontaktseite des „Cellarium“-Online-Shops. Ein Zugriff auf die Daten ist über ein authentisiertes Administrationssystem ausschließlich den Eigentümern des „Cellarium“-Klosterladens möglich.

Kundendaten, die wir im Rahmen von Anfragen über die Kontaktseite erhalten haben, werden innerhalb von 30 Tagen nach Beantwortung der Anfrage bzw. Bearbeitung einer gegebenenfalls daraus resultierenden Bestellung gelöscht, sofern keine wesentlichen Gründe (siehe Punkt 3.9) ihre Archivierung in einem gesicherten Archiv erforderlich machen.

### **3.3. Einsichtmöglichkeit**

Besucher des „Cellarium“-Online-Shops, die eine Anfrage über die Kontaktseite des Shops gestellt haben, erhalten eine Bestätigungs-Mail, die zumindest implizit alle von ihnen verpflichtend anzugebenden Informationen enthält.

### **3.4. Weitergabe von Daten**

Eine Weitergabe von Daten, die der „Cellarium“-Klosterladen im Rahmen von Anfragen von Kunden erhalten hat, an Dritte ist prinzipiell nicht vorgesehen. Sollte zur Beantwortung von spezifischen Fragestellungen die Weiterleitung der Anfrage an Dritte erforderlich sein, wird Sorge getragen, dass die Anfrage in einer anonymisierten Form weitergegeben wird.

### **3.5. Auskunftsrecht**

Jeder Person wird das Auskunftsrecht über die im „Cellarium“-Klosterladen potenziell über sie gespeicherten Informationen zugestanden.

### **3.6. Recht auf Berichtigung**

Die Kontaktdaten werden grundsätzlich bei jeder Anfrage über die Kontaktseite durch direkte Eingabe durch den Kunden neu erhoben und nicht gespeichert. Eine Berichtigung nach Abschluss der Beantwortung ist daher irrelevant; in der Regel wird eine wegen fehlerhafter Kontaktdaten (z.B. einer fehlerhaften Mailadresse) nicht beantwortbare Anfrage seitens des Kunden wiederholt werden müssen.

### **3.7. Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht**

Die Kontaktdaten – Name, E-Mailadresse und Telefonnummer – in Anfragen von der Kontaktseite des „Cellarium“-Online-Shops werden nach Beantwortung der Anfrage gelöscht. Ihre Weiterverarbeitung und Verwendung über die Zwecke der Beantwortung der Anfrage hinaus ist nicht vorgesehen. Die genannten Rechte werden den Kunden zugestanden; sie sind aber angesichts der genannten Behandlung der Daten weitgehend irrelevant.

### **3.8. Recht auf Datenübertragbarkeit**

Da jede Anfrage an den „Cellarium“-Online-Shop in sich abgeschlossen und nicht mit allfälligen weiteren Transaktionen des gleichen Kunden verknüpft ist, ist die Menge der gespeicherten Daten im Wesentlichen auf den Inhalt der Anfrage beschränkt; zudem werden die Kontaktdaten nach Beantwortung der Anfrage gelöscht. Grundsätzlich können sie aber, soweit noch vorhanden, in einem gängigen Format zur Verfügung gestellt werden.

### **3.9. Dauer der Datenspeicherung**

Die Kontaktdaten – Name, E-Mailadresse und Telefonnummer – in Anfragen über die Kontaktseite werden spätestens 30 Tage nach Beantwortung der Anfrage gelöscht, sofern sie nicht im Zusammenhang mit Transaktionen stehen, bei denen es nicht denkunmöglich ist, dass aus ihnen gegebenenfalls Rechtsansprüche des Kunden abgeleitet werden können (siehe Punkt 2.9). In diesem Fall werden sie bis zur Verjährung allfälliger Rechtsansprüche, also gegebenenfalls bis zu 30 Jahren, in einem gegen unberechtigte Zugriffe gesicherten Archiv aufbewahrt.

## **4. Datensicherheits-Maßnahmen**

Die Website des „Cellarium“-Online-Shops, (<http://www.cellarium.at>), wird zwar aus Performance-Gründen primär im HTTP-Mode angeboten, sie wechselt aber beim Aufruf aller Seiten, die die Eingabe personenbezogener Daten erfordern (konkret, die Bestell- und Kontakt-Seiten), automatisch in den HTTPS-Modus. Personenbezogene Daten werden

daher grundsätzlich nur mit *Secure HTTP* übertragen. Das Administrationssystem des „*Cellarium*“-Online-Shops läuft ausschließlich unter *Secure HTTP*. Ein Zugriff auf das Administrationssystem ist ausschließlich den Eigentümern des „*Cellarium*“-Klosterladens nach entsprechender Authentisierung möglich; Anmeldungen im Administrationssystem werden protokolliert. Ein Zugriff auf die im „*Cellarium*“-Online-Shop ermittelten personenbezogenen Daten ist ausschließlich aus dem Administrationssystem heraus möglich (sowie über speziell abgesicherte Schnittstellen zur technischen Wartung des Servers).

Der „*Cellarium*“-Online-Shop verwendet die Zahlungsfunktionen von PayPal®. PayPal® stellt relativ rigide Anforderungen an die Qualität der SSL-Verschlüsselung jener Websites, die seine Zahlungsfunktionen verwenden. Da sichergestellt sein muss, dass PayPal®-Transaktionen korrekt abgewickelt werden, wird implizit auch gewährleistet, dass der Webserver, auf dem der „*Cellarium*“-Online-Shop läuft, den aktuellen Sicherheits-Standards entspricht.

Beim Abschluss einer Bestellung durch den Kunden erhält dieser in einer Mail seine Rechnung sowie einen Link, über den die Rechnung auch von der Website des „*Cellarium*“-Online-Shops abgerufen werden kann. Der Name der Rechnungsdatei ist zufällig aus einer Auswahl von über  $10^{48}$  Möglichkeiten gewählt; es ist also so gut wie ausgeschlossen, dass Außenstehende den Namen dieser Datei erraten können. Zudem wird die Rechnungsdatei dann, wenn der Bestellvorgang seitens der „*Cellarium*“-Administration als abgeschlossen markiert wurde, so verschoben, dass sie nicht mehr über einen gewöhnlichen Web-Link abgerufen werden kann und nur mehr innerhalb des Administrationssystems des „*Cellarium*“-Online-Shops verfügbar ist.

Der gesamte Inhalt des „*Cellarium*“-Online-Shops einschließlich Administrationssystem wird über eine eigene Funktion auf Änderungen überprüft, wodurch sowohl Fehler im Dateisystem, aber auch allfällige Hacker-Angriffe, erkannt werden können.