Whitepaper

Die 6 wichtigsten Datenschutz-Tipps

TRUSTED SHOPS

Inhaltsverzeichnis

Einleitung

Datenschutz kostet viel Zeit und Nerven. Bereits das Herausfiltern der wirklich wichtigen Pflichten ist für Sie als Shopbetreiber großer Arbeitsaufwand, der Ihnen alles andere als leicht von der Hand geht? Noch dazu wollen Sie natürlich die Erwartungen Ihrer Kunden erfüllen. Und das ohne juristische Vorkenntnisse? Ganz schön kompliziert!

Wir helfen Ihnen, sich einen Überblick zu verschaffen, welche gesetzlichen Anforderungen Sie auf jeden Fall erfüllen müssen. Außerdem unterstützen unsere Rechtsexperten Sie mit wertvollen Praxistipps bei der Umsetzung.

1. Datenschutzerklärung

Eine der wesentlichsten Pflichten, die Sie erfüllen müssen, ist die Datenschutzerklärung – und das nicht nur in Ihrem Online-Shop, sondern auch bei eBay oder Amazon. Denn wenn Sie personenbezogene Daten verarbeiten, müssen Sie laut Art. 13 bzw. 14 DSGVO hierüber aufklären. Dies soll die Datenverarbeitung für Ihre Shopbesucher transparent machen und erfolgt bei Internetpräsenzen über die Datenschutzerklärung. Was dort neben Art, Umfang und Zweck jedes Verarbeitungsvorgangs genannt werden muss, ist im Einzelnen:

- Name und Kontaktdaten des Verantwortlichen, ggf. dessen Vertreters und ggf. eines Datenschutzbeauftragten
- Rechtsgrundlagen gem. Art. 6 DSGVO, aufgrund derer die Verarbeitungen erfolgen (z. B. Einwilligung des Betroffenen oder Vertrag mit diesem) sowie ggf. die berechtigten Interessen
- Empfänger (Kategorien) der personenbezogenen Daten; bei Empfängern in Drittländern zudem Informationen zu geeigneten Garantien
- Speicherdauer bzw. Kriterien für deren Festlegung
- Hinweis auf die verschiedenen Rechte des Betroffenen nach der DSGVO (Auskunft, Berichtigung, Löschung oder Einschränkung, Widerspruch, Datenübertragbarkeit)
- Hinweis auf das Recht des Betroffenen, eine erteilte Einwilligung jederzeit zu widerrufen, ohne dass dies die Rechtmäßigkeit der Verarbeitung bis zu diesem Zeitpunkt berührt
- Hinweis auf das Beschwerderecht des Betroffenen bei einer Aufsichtsbehörde
- evtl. Pflicht oder Erforderlichkeit der Bereitstellung der personenbezogenen Daten sowie mögliche Folgen der Nichtbereitstellung
- Vorliegen einer automatisierten Entscheidungsfindung (inkl. Profiling) sowie deren Logik, Tragweite und angestrebte Auswirkung auf den Betroffenen

Gemäß Art. 12 Abs.1 S.1 DSGVO müssen Sie zudem alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln. Darüber hinaus müssen die Informationen leicht auffindbar sein.

Machen Sie es sich noch einfacher! Mit unserem Rechtstexter können Sie Ihre Datenschutzerklärung ganz leicht selbst erstellen. Mit wenigen Klicks und ohne juristische Vorkenntnisse. Natürlich ist Ihre Datenschutzerklärung individuell und DSGVO-konform. Ganz egal ob B2B oder B2C, ob für Ihren Shop, eBay oder Amazon.

Und das ist noch nicht alles: Dank unseres Update-Services halten Sie Ihre Texte immer auf dem aktuellen Stand. Über 560.000 Mal wurde unserer Rechtstexter schon durchlaufen. Qualität, der man vertrauen kann - die von uns erstellten Rechtstexte wurden noch nie erfolgreich abgemahnt.

2. Verarbeitungsverzeichnis

Unternehmen, die personenbezogene Daten verarbeiten, sind verpflichtet, nachzuweisen, dass sie die Vorschriften zum Datenschutz einhalten. Aus diesem Grund müssen Unternehmen zum Zweck der Dokumentation gemäß Art. 30 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten führen. Dieses müssen Sie auf Verlangen den Aufsichtsbehörden (z. B. bei einer Prüfung) jederzeit aushändigen können – natürlich immer auf dem aktuellen Stand. Das Verzeichnis muss folgende Angaben beinhalten:

- Name und die Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Kategorien der betroffenen Personen und personenbezogener Daten
- Kategorien der Datenempfänger
- Angaben zur Übermittlung in Drittländer und angemessenen Garantien
- Löschfristen für die verschiedenen Datenkategorien
- Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, die Sie zur Absicherung der Daten eingerichtet haben

Hierfür haben wir in unserem Produkt Datenschutz 360 eine Lösung für Sie eingebaut, die Sie ganz ohne juristische Vorkenntnisse nutzen können. Erstellen Sie ganz einfach Ihr individuelles Verzeichnis und passen es immer dann an, wenn sich Änderungen bei Ihnen ergeben. Damit Sie bei dieser komplizierten Datenschutz-Anforderung nicht den Überblick verlieren, führt Sie unsere Software in klar strukturierten Schritten zum Ziel. Zudem stellen wir Ihnen über 150 bereits vordefinierte Verfahren zur Verfügung (z.B. Google Analytics, DHL oder PayPal).

3. Datenschutz-Unterweisungen

Aus Art. 39 Abs. 1 lit. b DSGVO ergibt sich, dass Sie alle Mitarbeiter in Ihrem Unternehmen schulen (unterweisen) müssen, die an der Verarbeitung von „personenbezogenen Daten“ beteiligt sind oder Zugang zu diesen haben. Personenbezogene Daten verbergen sich fast überall: In Personalakten, Nutzerkonten des Online-Shops, Webanalysetools etc.

Schulungen im Datenschutz sind übrigens nicht nur deshalb wichtig, weil es eine gesetzliche Pflicht hierzu gibt. Vielmehr zeigt auch die praktische Erfahrung, dass zahlreiche Datenpannen direkt oder indirekt durch eine fehlende Sensibilisierung der Mitarbeiter verursacht werden.

Datenschutz-Unterweisungen bedeuten erhöhten Aufwand für Sie. Schließlich müssen Sie diese Schulungen entweder selber durchführen oder aber durch eine fachkundige Person durchführen lassen. Mit uns können Sie diesen Punkt ganz einfach abhaken. Im Rahmen von Datenschutz 360 schulen unsere erfahrenen Juristen Sie und Ihre Mitarbeiter in einem einstündigen Online-Webinar im Umgang mit Daten von Mitarbeitern, Kunden und Partnern und darin, wie Sie vertrauliche Daten vor dem Zugriff Dritter schützen. Die Teilnahme bestätigen wir Ihnen mit einem Zertifikat.

4. Auftragsverarbeitungs-verträge

Sofern Sie personenbezogene Daten von anderen Stellen (v. a. Dienstleistern) verarbeiten lassen, liegt oftmals eine sog. Auftragsverarbeitung vor. Um DSGVO-konform zu handeln, müssen Sie hierfür Verträge zur Auftragsverarbeitung schließen (Art. 28 Abs. 3 DSGVO), sogenannte AV-Verträge. In diesen müssen Sie insbesondere folgende Punkte regeln:

- Weisungsgebundenheit des Auftragsverarbeiters
- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien von betroffenen Personen
- Rechte und Pflichten des Verantwortlichen
- Bedingungen für den Einsatz von Unterauftragnehmern

Und wieder kommt Datenschutz 360 ins Spiel: Egal ob Serverhosting, Newsletterversand oder Trackingsoftware - unser Muster AV-Vertrag in drei verschiedenen Sprachen (Deutsch, Englisch und Französisch) bietet Ihnen eine rechtssichere Grundlage. Kommentare unserer Rechtsexperten an den wichtigen Stellen erleichtern Ihnen die individuelle Anpassung. So kommen Sie schnell an Ihr Ziel.

5. Antwortschreiben an Ihre Kunden

Das Gesetz räumt Ihren Kunden umfassende Rechte ein. Beispielsweise können sie von Ihnen gemäß Art. 15 DSGVO Auskunft über die zu ihrer Person gespeicherten Daten sowie über eine ganze Menge zusätzlicher Informationen rund um deren Verarbeitung verlangen.

Neben allen personenbezogenen Daten einer betroffenen Person, die Sie gespeichert haben, müssen Sie ihr auf Anfrage auch folgende Informationen mitteilen:

- Die Verarbeitungszwecke
- Die Kategorien der verarbeiteten Daten
- Die Empfänger der personenbezogenen Daten bzw. die Empfängerkategorien
- Die Speicherdauer der Daten oder, wenn dies nicht möglich ist, die Kriterien zur Bestimmung dieser Dauer
- Das Bestehen anderer Betroffenenrechte, nämlich auf Berichtigung und Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch dagegen
- Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

- Bei personenbezogenen Daten, die nicht beim Betroffenen erhoben wurden, alle verfügbaren Informationen über ihre Herkunft
- Ggf. das Bestehen einer automatisierten Entscheidungsfindung, inkl. Profiling sowie aussagekräftige Informationen über die diesen Vorgängen zugrundeliegende Logik und über die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für den Betroffenen

Das bedeutet, dass Sie jederzeit über eine schnell zugreifbare und detaillierte Übersicht der erforderlichen Angaben verfügen müssen, was bei einer erheblichen Anzahl verarbeiteter Daten und einem ggf. komplizierten Verarbeitungsprozess ein beträchtlicher Aufwand ist.

Sie haben ein Auskunftsersuchen zu verarbeiteten Daten eines Kunden erhalten und müssen schnell reagieren? Mit unseren Muster-Schreiben im Datenschutz 360-Kundenkonto haben Sie immer die rechtssichere und passende Antwort griffbereit – auch für die praxisrelevanten Ausnahmen oder besondere Konstellationen. Einfach ausfüllen und genau so zurücksenden. Fertig.

6. Was ist bei einer Datenpanne zu tun?

Auch wenn etwas schiefgeht, ist es wichtig, dass Sie planvoll vorgehen und die kurzen Fristen kennen, die für den Umgang mit Datenschutzverletzungen gelten.

Durch interne Sensibilisierung und Prozesse sollten Sie Datenschutzpannen oder negative Aufmerksamkeit der Aufsichtsbehörden von Vornherein vermeiden. Sollte es aber dennoch mal zu einem solchen Vorfall kommen, müssen Sie bestimmte Regeln beachten.

„Datenschutzpanne“ kann heißen, dass eine besonders große Menge von Daten oder besonders sensible Daten verloren gegangen sind, z. B. weil Server angegriffen wurden. Aber auch andere, weniger schwere Fälle können Behörden als solche einstufen, z. B. wenn von Ihnen angebotene Dienste oder eingesetzte Tools in Bezug auf die Verarbeitung von Daten fehlerhaft agiert haben.

So gehen Sie am besten vor:

- Ruhe bewahren, keine kurzfristigen Maßnahmen wie Mailing an Betroffene, Löschen von irgendwelchen Verläufen etc.
- Dokumentieren: Was genau ist passiert? Welche Daten sind betroffen? Welche Personen (Käufer,Mitarbeiter,...) sind betroffen?
- Zeitnah handeln: Bei meldepflichtigen Vorfällen haben Sie bis zur Meldung an die Datenschutzbehörde nur 72 Stunden Zeit.
- Sofern vorhanden: Datenschutzbeauftragten frühzeitig mit einbeziehen. Es ist seine Aufgabe,Informationen zu sammeln, zu bewerten und auf dieser Grundlage anschließend zu entscheiden, was unternommen werden muss.

Alle beteiligten Stellen sollten gemeinsam die Auswirkungen des Sachverhalts auf Prozesse, Produkte und Compliance zusammentragen. Ist die Auswertung abgeschlossen, werden gemeinsam Maßnahmen festgelegt, die für den konkreten Fall unternommen werden müssen.

Mit Datenschutz 360 können Sie im Fall einer Datenpanne der Checkliste in Ihrem Kundenkonto folgen und so Schritt für Schritt Ihre To-Dos abhaken.

Die Vertrauensmarke in Europa

Sie haben weitere Fragen zum Thema Datenschutz?
Das Trusted Shops Team hilft Ihnen gerne weiter.

+49 221 77536-7490

shop@trustedshops.com

20181221-de