DSGVO und Shopware
Das müssen Sie jetzt wissen

shopware

Vorwort

Die eCommerce Branche muss sich ständig neuen Herausforderungen stellen und diese meistern. Sowohl Unternehmen als auch Verbraucher und die Politik haben stets neue Anforderungen an die Branche. Besonders im Bereich Datenschutz wurde der Ruf nach Verbesserung in den vergangenen Jahren immer lauter. Schließlich wurde die EU aktiv und hat neue, grenzübergreifende Standards geschaffen.

Am 25. Mai 2018 wird die europäische Datenschutz-Grundverordnung (DSGVO) wirksam und löst nationale Regelungen ab. Mit dieser wird die Verarbeitung personenbezogener Daten EU-weit vereinheitlicht. Darüber hinaus gilt sie für alle Unternehmen und Institutionen, die in der EU tätig sind und mit personenbezogenen Daten wie Namen, Adressen, Bankdaten, Geburtstagen, Fotos usw. arbeiten.

Personenbezogene Daten sollen durch die DSGVO besser geschützt werden und der Verbraucher soll den Umgang durch mehr Transparenz in der Verarbeitung besser nachvollziehen können. Außerdem soll durch die DSGVO der Datenaustausch zwischen Unternehmen reibungsloser ablaufen.

Solche Veränderungen hören sich für den Verbraucher gut an, setzen sich aber natürlich nicht von alleine um - sie beanspruchen Zeit und intensive Bearbeitung. Unternehmen sollten sich daher rechtzeitig mit der Novellierung befassen. Besonders im eCommerce sollten Sie deshalb vorbereitet sein und Ihren Shop an das neue Datenschutzrecht anpassen.

In diesem Kompendium möchten wir Ihnen alles Wissenswerte zur DSGVO näherbringen: Was hat sich verändert und welche Auswirkungen wird sie auf Ihren Onlineshop haben? Erhalten Sie Einblicke in die Ansicht von Experten von Trusted Shops und Protected Shops sowie interessante Praxistipps.

Stefan Heyne

Vorstand,
shopware AG

Inhalt

1. Worum geht es bei der Datenschutz-Grundverordnung?

Acht Fragen an Legal Expert Rafael Gomez-Lus

Frage 1: Aus welchem Grund wurde die DSGVO aufgesetzt?
Das Hauptziel der Datenschutz-Grundverordnung ist die Harmonisierung des europäischen Datenschutzes. Ein weiteres Ziel ist, mit einem aktualisierten Datenschutzrecht der rasanten technischen Entwicklung der digitalen Gesellschaft gerecht zu werden, was die veraltete Richtlinie aus dem Jahr 1995 nicht mehr erreichen konnte. Das Datenschutzrecht wird zudem erheblich gestärkt, insbesondere durch neue, wirksame Sanktionsmechanismen.

Frage 2: Wer ist von der neuen Datenschutz-Grundverordnung betroffen?
Alle Unternehmen, die personenbezogene Daten verarbeiten, sind von der Datenschutz-Grundverordnung betroffen. Auch kleinere und mittlere Online-Händler müssen die Anforderungen der Datenschutz-Grundverordnung einhalten. Unternehmen mit weniger als 250 Mitarbeitern sind normalerweise von der besonders aufwändigen Anforderung zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten (vormals „Verfahrensverzeichnis“) freigestellt. Ausnahme: Personenbezogene Daten werden nur gelegentlich verarbeitet. Diese Bedingung ist im Bereich E-Commerce allerdings nicht gegeben, weil Kundendaten regelmäßig verarbeitet werden. Demnach sind auch kleinere und mittlere Online-Händler dazu verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Frage 3: Worin sehen Sie die größten Herausforderungen für betroffene Unternehmen?
Die größten Herausforderungen für Unternehmen sind, ihre Prozesse, bei denen personenbezogene Daten verarbeitet werden, DSGVO-konform zu gestalten und entsprechend zu dokumentieren.

Wie viel Aufwand ein Unternehmen tatsächlich benötigt, hängt stark davon ab, inwiefern sie bereits das bisherige Recht eingehalten haben. Bei Unternehmen, die beim Thema Datenschutz bereits gut aufgestellt sind, ist der Aufwand wesentlich geringer als bei Unternehmen die fast von Null anfangen.

Frage 4: Welche Chancen sehen Sie in der neuen Datenschutz-Grundverordnung?
Der Datenschutz wird nicht zuletzt aufgrund der hohen Sanktionen ein neues Standing in Unternehmen gewinnen. In der Vergangenheit herrschte oft die Meinung, der Datenschutz habe keine Zähne. Das hat dazu geführt, dass manche (insbesondere sehr große) Unternehmen lieber eine Sanktion riskiert haben, als ihre Geschäftspraktiken anzupassen. Dies könnte sich künftig nachhaltig ändern, sodass Datenschutz-Compliance als wichtige Grundvoraussetzung für geschäftliche Tätigkeiten wahrgenommen wird.

Frage 5: Wer profitiert am meisten von der DSGVO?

Kunden und Nutzer von Diensten im Internet profitieren von einem besseren Schutz ihrer persönlichen Daten. Unter den Gewinnern werden auch Unternehmen sein, die effiziente Lösungen für die Einhaltung der DSGVO anbieten. Anbieter, die beim Thema Datenschutz bereits vorgeleistet haben, werden sich in einer vorteilhaften Position sehen.

Frage 6: Wann ist mit Strafen zu rechnen und wie sehen Sanktionen für Unternehmen aus?

Die Bedingungen für die Verhängung von Geldbußen werden in Art. 83 DSGVO beschrieben. Wenn Unternehmen die Anforderungen der DSGVO wie z. B. hinsichtlich der Datenverarbeitungsgrundsätze oder der sog. „Betroffenenrechte“ nicht einhalten, riskieren sie Sanktionen. Bei besonders schwerwiegenden Verstößen drohen Geldbußen von bis zu 20 Millionen Euro bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes. Unternehmen mit entsprechender rechtlicher Beratung verfolgen deshalb voraussichtlich einen risikobasierten Ansatz zu: je höher die mit einer Datenverarbeitung verbundenen Risiken sind, desto höher muss auch die Sorgfalt des Unternehmens sein.

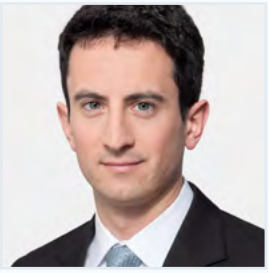
Frage 7: Welche Maßnahmen sollten Unternehmen treffen, damit sie auf die DSGVO vorbereitet sind?

Die konkreten Maßnahmen, welche Unternehmen treffen müssen, sind unterschiedlich. Der erste Schritt wird sein, sich einen Überblick über die aktuellen Verfahren innerhalb des Unternehmens, bei denen personenbezogene Daten verarbeitet werden, zu verschaffen. In einem Online-Shop sind dies z. B. Tracking Tools, Newsletter-Dienste oder Bonitätsprüfungen. Diese Verfahren sind in einem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren, welches jederzeit von Datenschutzbehörden im Rahmen von Prüfungen angefordert und untersucht werden kann.

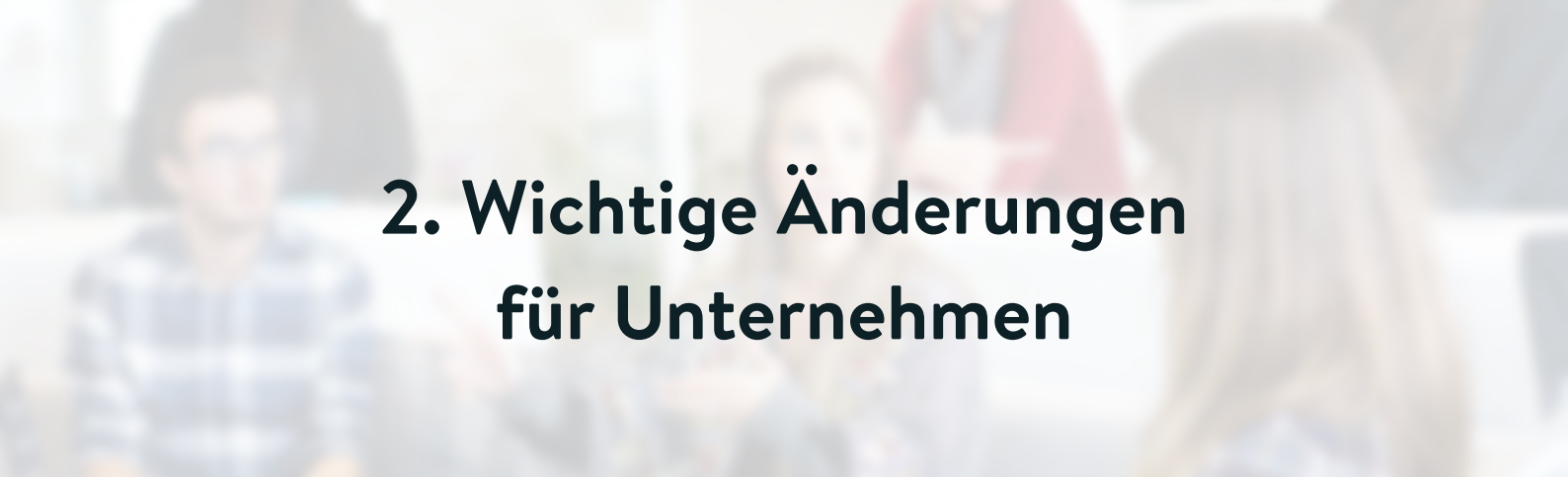
Die Datenschutzerklärung und die Einwilligungserklärungen des Online-Shops sind an die Anforderungen der DSGVO anzupassen. Die neuen Regelungen der „Betroffenenrechte“ sind zu beachten, also die Rechte jedes Einzelnen gegenüber den für die Verarbeitung Verantwortlichen. Weiterhin ist einen Reaktionsplan für die Meldung von Datenpannen einzuführen und nicht zuletzt sind alle bestehenden Verträge zur Auftragsverarbeitung mit Dienstleistern wie Web-Hostern oder Anbietern von Tracking-Tools zu prüfen und in den allermeisten Fällen auch zu erneuen.

Frage 8: Wann sollten die Unternehmen mit der Umsetzung der Maßnahmen beginnen?

Die DSGVO gilt ab dem 25. Mai 2018. Anbieter wie Trusted Shops helfen hierbei mit praktischen Lösungen für Online-Händler, damit diese ihren Online-Shop DSGVO-konform gestalten können.



__Rafael Gomez-Lus__ ist Legal Expert Spain und EU der Trusted Shops GmbH und zugelassener spanischer Rechtsanwalt. Er hat sein Studium der Rechtswissenschaften an der Universität Zaragoza absolviert und einen Master in International Business an der Grenoble Ecole de Management in Frankreich abgeschlossen. Zudem ist er Autor eines spanischen Handbuchs für Onlinehändler und von Whitepapern zum Verbraucherrecht in Spanien.



2. Wichtige Änderungen für Unternehmen

1. Einwilligung
Unternehmen, die personenbezogene Daten erheben möchten, müssen sich im Voraus eine Einwilligung von den betroffenen Personen einholen, in der diese ausdrücklich der Verarbeitung ihrer personenbezogenen Daten zustimmen, wenn es keine gesetzliche Erlaubnis für die Datenverarbeitung gibt (z. B. weil die Daten nicht für die Erfüllung eines Vertrags mit einem Kunden erforderlich sind). Zusätzlich ist jeder Einwilligungserklärung ein Hinweis beizufügen, der die Betroffenen über ihre Rechte unterrichtet, die Einwilligung jederzeit widerrufen zu können. Die Einwilligung und die Information über den Widerruf müssen nach dem „Simplizitätsgebot“ in einem verständlich formulierten und leicht zugänglichen Text vorhanden sein. Unternehmen müssen nachweisen können, dass die betroffenen Personen der Datenverarbeitung zugestimmt haben.

2. Rechenschaftspflicht (Artikel 5 Absatz 2,24 Absatz 1)
Unternehmen, die personenbezogene Daten verarbeiten, haben die Rechtsgrundsätze der Datenschutz-Grundverordnung einzuhalten. Dabei handelt es sich um die Rechtmäßigkeit der Datenverarbeitung, die Verarbeitung der Daten nach Treu und Glauben, das transparente Verarbeiten der Daten, die Zweckmäßigkeit der Datenverarbeitung, die Berücksichtigung der Datenminimierung bei der Datenerhebung, die Erhebung der richtigen Daten, die Berücksichtigung der Speicherbegrenzung sowie das Einhalten der Integrität und Vertraulichkeit bei der Datenverarbeitung. Die Unternehmen müssen die Einhaltung der genannten Rechtsgrundsätze nachweisen können („Rechenschaftspflicht“). Dafür bedarf es der Einführung und Anwendung eines Datenschutzmanagements, in dem die Rollen und Verantwortlichen im Datenschutz klar definiert und die Arbeitsabläufe in Unternehmen festgestellt sind, wenn es um die Verarbeitung personenbezogener Daten geht.

3. Datenmitnahme
Jeder hat das Recht, die einen selbst betreffenden Daten, die von einem Unternehmen erzeugt werden, in einem elektronischen Format ausgehändigt zu

bekommen und diese Informationen einer anderen Stelle zu übermitteln, sofern:

- Die Verarbeitung auf einer Einwilligung der Betroffenen Person beruht
- Die Verarbeitung mittels automatisierter Verfahren geschieht

Die betroffenen Personen können von Unternehmen ebenfalls verlangen, dass die Daten direkt an einen weiteren Empfänger weitergeleitet werden, wenn dies technisch für das die Daten herausgebende Unternehmen möglich ist.

4. Recht auf Vergessenwerden

Betroffene Personen haben das Recht, eine Löschung der von den Unternehmen erhobenen Daten zu verlangen. Die Unternehmen sind verpflichtet, die erhobenen Daten zu dieser Person umgehend zu löschen, wenn insbesondere:

- Der Zweck für die Erhebung der personenbezogenen Daten nicht mehr erforderlich ist und auch alle Aufbewahrungsfristen abgelaufen sind, z. B. aus dem Handels- oder Steuerrecht.
- Die betroffene Person Widerspruch gegen die Datenverarbeitung einlegt und keine Gründe für die Verarbeitung vorliegen.
- Die Verarbeitung der personenbezogenen Daten nicht rechtmäßig erfolgt ist.
- Die personenbezogenen Daten sind zu löschen, weil das Unionsrecht oder das Recht der Mitgliedsstaaten das vorgibt.

5. Strafen (Artikel 83 DSGVO)

Die Strafen bei Verstößen gegen die Datenschutz-Grundverordnung sind deutlich erhöht worden. So können Bußgelder in Höhe von bis zu 20.000.000,00 € oder bis zu 4% des weltweit erzielten Jahresumsatzes anfallen. Bei leichteren Verstößen gegen die Datenschutz-Grundverordnung können Strafen von bis zu 10.000.000,00 € oder 2% des weltweit erzielten Jahresumsatzes anfallen. Dabei wird die Summe fällig, die für das Unternehmen den höheren Betrag darstellt.

6. Einfachere Beschwerdeanträge für Betroffene

Durch die Vereinheitlichung der Datenschutzregelungen auf EU-Ebene, ist es für betroffene Personen, die sich in ihren Datenschutzrechten verletzt sehen, einfacher, Beschwerdeanträge einzureichen. Das ist vor allem dadurch bedingt, dass Beschwerdeanträge in Zukunft bei den Datenschutzbehörden des eigenen Landes eingereicht werden können. Die betroffene Person muss nicht mehr ihre Beschwerde in dem Land einreichen, in dem das verantwortliche Unternehmen seinen Hauptsitz hat.

7. Marktortprinzip → räumlicher Anwendungsbereich

Das Marktortprinzip besagt, dass nicht nur in der Europäischen Union ansässige Unternehmen unter das Datenschutz-Grundgesetz fallen, sondern auch solche Unternehmen, dessen Angebot sich an einen bestimmten nationalen Markt in der Europäischen Union richtet, oder die betroffenen Personen, dessen personenbezogene Daten erhoben werden ihren Wohnsitz in der Europäischen Union haben. Dadurch sollen für alle Unternehmen, die auf dem Markt der Europäischen Union tätig sind, gleiche Wettbewerbsbedingungen geschaffen werden.

8. Verzeichnis aller Verarbeitungstätigkeiten (Artikel 30 DSGVO)

Die in einem Unternehmen für die Verarbeitung personenbezogener Daten zuständigen Personen haben ein Verzeichnis anzulegen, in das alle vorgenommenen Verarbeitungstätigkeiten aufzulisten sind. Dadurch schaffen Unternehmen Transparenz und sichern sich rechtlich ab. Auf Anfrage ist das Verzeichnis der zuständigen Behörde für Datenschutz offenzulegen. Folgende Informationen sollte das Verzeichnis besitzen:

- Namen und die Kontaktdaten der verantwortlichen Personen
- Den Zweck der Datenverarbeitung
- Eine Kategoriebeschreibung zu den betroffenen Personen und den personenbezogenen Daten
- Kategorien von Empfängern, die personenbezogene Daten zu Verarbeitung erhalten haben
- Nach Möglichkeit vorgesehene Fristen für die Löschung der unterschiedlichen Datenkategorien
- Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

9. Erweiterung der Informationspflichten (Artikel 13, 14 DSGVO)

Unternehmen, die personenbezogene Daten erheben oder von Dritten bekommen (z. B. Scorewerte von einer Auskunftei), haben den betroffenen Personen umfangreiche Auskünfte über die Datenerhebung zu erteilen. Die Informationen sind der betroffenen Person zum Zeitpunkt der Datenerhebung mitzuteilen. Unter anderem sind der betroffenen Person folgende Informationen mitzuteilen:

- Name und Kontaktdaten der verantwortlichen Person
- Kontaktdaten des Datenschutzbeauftragten
- Den Zweck und die Rechtsgrundlage für die Verarbeitung
- Die berechtigten Interessen, die mit der Datenverarbeitung verfolgt werden

10. Datenschutz-Folgenabschätzung (Artikel 35 DSGVO)

Besteht die Vermutung, dass durch die Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffene Person entstehen könnte, haben die Unternehmen vorab eine Datenschutz-Folgenabschätzung durchzuführen. Dabei werden im Voraus mögliche Auswirkungen der Datenerhebung für die betroffene Person ermittelt und aufgrund dessen abgewogen, ob eine Datenverarbeitung erfolgen soll oder nicht oder ob zusätzliche Schutzmaßnahmen zu treffen sind, mit denen die Risiken reduziert werden können.

11. Meldepflicht von Datenschutzverletzungen (Artikel 33 DSGVO)

Kommt es zu einer Verletzung der Datenschutzpflichten, müssen Unternehmen diese unverzüglich und spätestens innerhalb von 72 Stunden nach Bekanntwerden der Verletzung der zuständigen Aufsichtsbehörde mitteilen. In der Meldung sind die Art der Datenschutzverletzung, der Name und die Kontaktdaten des Datenschutzbeauftragten, eine Beschreibung der mutmaßlichen Folgen die

aus der Datenschutzverletzung, sowie eine Beschreibung der geplanten Maßnahmen die zur Behebung der Verletzung ergriffen werden. Hat die Datenschutzverletzung hohe Risiken für die betroffenen Personen, sind diese ebenfalls zu informieren, z. B. per eMail oder durch eine Meldung auf der Website des eigenen Unternehmens.

12. One-Stop-Shop Prinzip

Mit dem One-Stop-Shop Prinzip räumt die DSGVO europaweit tätigen Unternehmen die Möglichkeit ein, eine zentrale Anlaufstelle für die grenzüberschreitende Datenverarbeitung einrichten zu können. Die „federführende“ Aufsichtsbehörde ist am zentralen Verwaltungssitz des Unternehmens in der Europäischen Union einzurichten. Vor allem für große Unternehmen kann das One-Stop-Shop Prinzip eine wichtige Bedeutung haben.

13. Newsletterversand

Die für den Newsletterversand geltenden Regelungen bleiben grundsätzlich auch nach Einführung der Datenschutz-Grundverordnung bestehen. Es ist erforderlich, dass der eMail-Empfänger dem Erhalt von eMails ausdrücklich zustimmt. Für die Einwilligung ist ein Double-opt-in-Verfahren zu empfehlen, da dieses Verfahren auch im Zusammenhang mit der DSGVO als rechtssicher einzustufen ist. Dabei ist es wichtig, dass der Empfänger in der Einwilligung genauestens darüber in Kenntnis gesetzt wird, worin er einwilligt. Die Einwilligung des Empfängers hat auf freiwilliger Basis zu erfolgen und ist von dem Versender aufzubewahren. Eine Einwilligung durch Stillschweigen kommt nicht zustande.

3. Selbstcheck: Datenschutzbeauftragter

Sobald bestimmte Anforderungen erfüllt sind, müssen Unternehmen einen Datenschutzbeauftragten benennen. Das ist insbesondere der Fall, wenn regelmäßig zehn oder mehr Personen in Ihrem Unternehmen personenbezogene Daten verarbeitet.

Hier können Sie überprüfen, ob sie einen Datenschutzbeauftragten stellen müssen oder nicht.

4. Die nächsten Schritte

Viele Online-Händler denken, dass bis zur Umsetzung der DSGVO noch genügend Zeit sei. Doch die Zeit drängt, denn die Umsetzung einiger Maßnahmen ist zeitintensiv. Daher sollten Online-Händler rechtzeitig mit der Anpassung beginnen, denn bei einem Verstoß gegen die DSGVO drohen empfindliche Bußgelder, die bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten Jahresumsatzes betragen können. In diesem Beitrag haben wir die wichtigsten Maßnahmen, die von Online-Händlern rechtzeitig umgesetzt werden müssen, zusammengefasst.

Verarbeitungsverzeichnis aktualisieren

Zunächst empfiehlt es sich, sich in einer Bestandsaufnahme einen Überblick zu verschaffen, welche Daten im Unternehmen verarbeitet werden (z. B. Kunden-, Mitarbeiter-, Unternehmensdaten). Wie bisher ist jedes Verfahren bei dem personenbezogene Daten erfasst und bearbeitet werden, in einem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Ab dem **25.05.2018** können die Datenschutzaufsichtsbehörden Unternehmen jederzeit dazu auffordern dieses vorzulegen und bei einem Versäumnis Bußgelder verhängen. Der Inhalt des „Verzeichnisses für Verarbeitungstätigkeiten“ –wie es in der DSGVO bezeichnet wird- ähnelt dem der bisherigen Verfahrensverzeichnisse. Neu ist, dass nicht mehr der Datenschutzbeauftragte, sondern die Unternehmensleitung für das Führen des Verzeichnisses verantwortlich ist.

Rechtskonforme Einwilligung

Bei jeder Verarbeitung personenbezogener Daten auf Grundlage einer Einwilligung (z. B. beim Newsletter-Versand) muss der Betroffene künftig informiert werden, worin er einwilligt und auf eine Widerrufsmöglichkeit hingewiesen werden. Die Einwilligung hat freiwillig und durch eine eindeutige Handlung zu erfolgen (z. B. durch das Setzen eines Häkchens). Einmal erteilte Einwilligungen müssen jederzeit mit Wirkung für die Zukunft widerrufen werden können. Neu ist die Vorgabe, dass der Widerruf so einfach erfolgen können muss wie die Einwilligungserteilung. Achtung: Bereits eingeholte Einwilligungen behalten ihre Wirksamkeit nur, wenn sie bereits der neuen Rechtslage entsprechend eingeholt wurden.

Verschärfte Meldepflichten

Shopbetreiber müssen künftig Datenschutzverstöße, die die Rechte und Freiheiten der Betroffenen beeinträchtigen könnten, spätestens innerhalb von 72 Std. nach Bekanntwerden der zuständigen Aufsichtsbehörde melden. Zur Meldung gehören eine konkrete Beschreibung der Datenpanne (z. B. Hackerangriff oder Datendiebstahl), die Abschätzung etwaiger

Folgen, die Nennung der Kontaktdaten des Datenschutzbeauftragten und die Information, welche Maßnahmen bereits ergriffen wurden. Für Online-Händler bedeutet das erheblich mehr Aufwand. Da die Datenpanne dokumentiert und gemeldet werden muss, sollte im Betrieb sichergestellt werden, dass die kurze Frist auch eingehalten werden kann.

Datenschutzerklärung anpassen

Bereits jetzt sind Online-Händler verpflichtet, eine Datenschutzerklärung auf ihrer Webseite bereitzustellen. Diese Pflicht bleibt auch weiterhin bestehen, aber die Anforderungen an die Information und Belehrung der betroffenen Personen werden durch die DSGVO steigen. Dabei ist darauf zu achten, dass die technischen Erläuterungen präzise und zugleich verständlich sein müssen. Künftig ist nicht nur der Zweck der Datenverarbeitung zu nennen, sondern auch eine klare Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten. Bereits bestehende Datenschutzerklärungen müssen daher angepasst werden, falls sie noch nicht den Vorgaben der DSGVO entsprechen.

Fazit

Der Countdown läuft und Aussitzen ist keine Option. Bis zum 25.05.2018 müssen Shopbetreiber die Vorgaben der DSGVO umgesetzt haben. Da einige Maßnahmen zeitintensiv sind und je nach Umsetzungsstand im Unternehmen Handlungsbedarf besteht, sollte bereits jetzt mit der Umsetzung begonnen werden. Bei Nichtbeachtung oder Verstößen drohen ab dem 25.05.2018 hohe Bußgelder.

In fünf Schritten - mit der Umsetzung dieser Anpassungen sollten Händler rechtzeitig beginnen:

1. Bestandsaufnahme aller Datenverarbeitungsprozesse als Basis für die Anpassung an die Vorgaben der DSGVO durchführen.
2. Verarbeitungsverzeichnis aktualisieren und sicherstellen, dass alle Datenschutzverarbeitungsprozesse erfasst werden.
3. Einwilligungserklärungen (z. B. bei Newsletterversand) auf Transparenz und Wirksamkeit überprüfen sowie Widerrufserklärung der Einwilligungserklärung anpassen und nach neuem Rechtgestalten.
4. Sicherstellen, dass bei Datenpannen 72 Stunden Frist (Meldepflicht) eingehalten werden kann.
5. Datenschutzerklärung anpassen - Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten darlegen.

***Bernadette Mohme** ist Volljuristin und berät bei Protected Shops über die rechtlichen Entwicklungen in allen für den eCommerce relevanten Bereichen. Dabei übersetzt sie gerichtliche Entscheidungen ebenso wie neue gesetzliche Vorgaben in eine verständliche Sprache und gibt Handlungsanleitungen zur rechtskonformen Umsetzung im Webshop. Protected Shops stellt ein eigenes Modul für sichere Rechtstexte zur Verfügung.*

5. So ist Shopware auf die DSGVO vorbereitet

Sebastian Klöpper, shopware AG

Seit geraumer Zeit sind wir bei Shopware damit beschäftigt, in Zusammenarbeit mit den bekannten Zertifizierungsstellen sicherzustellen, dass das System den Anforderungen der im Mai in Kraft tretenden DSGVO genügt. Dabei hat sich herausgestellt, dass Shopware den Shopbetreibern bereits heute die notwendigen Funktionen bereitstellt, die sie brauchen, um die nötigen Einstellungen vorzunehmen, die die Regeln der DSGVO erfordern. So stellt Shopware etwa bereits in der regulären Endbenutzer-Dokumentation alle erforderlichen Werkzeuge bereit,
z. B. auch um personenbezogene Daten wieder aus dem System zu entfernen, was eine Kernforderung der neuen Datenschutzverordnung ist.

Wichtig: Shopware liefert nur die technische Basis. Für Einstellungen, Content bzw. Textbausteine und die Einhaltung der DSGVO ist der Shop- bzw. Seitenbetreiber selbst verantwortlich.

Hintergrundinformationen erfahren Sie in einem eigenen Wiki-Artikel.

***Sebastian Klöpper** ist als Director Research & Development für die Shopware Produkt-Roadmap und deren Umsetzung verantwortlich. Zusätzlich fallen die Bereiche Support, Qualitätssicherung und Dokumentation aller Shopware-Produkte in seinen Aufgabenbereich. Sebastian Klöpper ist bereits seit 2007 für die shopware AG tätig.*

6. Anlaufstellen und Zertifizierungen

Trusted Shops

Händlerbund

Protected Shops

European Commision

Original-Gesetztext

7. Glossar

Anbei findest Du eine Übersicht über wichtige, wiederkehrende Begriffe, wenn es um die DSGVO geht.

1. Aufsichtsbehörde
Eine unabhängige staatliche Einrichtung, die in jedem Mitgliedsstaat entsprechend den EU-Richtlinien errichtet wird, Unternehmen berät und überwacht, sowie Bußgelder und andere Maßnahmen bei Datenschutzverstößen verhängen kann.

2. Auftragsverarbeiter
Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die von Verantwortlichen dazu beauftragt wurden, persönliche Daten zu verarbeiten.

3. Biomerische Daten
Personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Attributen von natürlichen Personen, mit denen diese eindeutig identifiziert werden. (z. B. Gesichtsbilder oder daktyloskopische Daten)

4. Dateisystem
Jedes Gebilde, in dem personenbezogene Daten strukturiert gesammelt werden und anhand bestimmter Kriterien verfügbar sind. Dabei ist es irrelevant ob die Daten zentral, dezentral oder nach funktionalen oder geografischen Aspekten geordnet werden.

5. Dritter
Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die außer der betroffenen Person, den Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters berechtigt sind, personenbezogene Daten zu verarbeiten.

6. Empfänger
Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, denen personenbezogene Daten offengelegt werden.

7. Einschränkung der Verarbeitung
Die Kennzeichnung personenbezogener Daten mit dem Ziel, die weitere Verarbeitung dieser Daten einzuschränken.

8. Einwilligung
Eine von der betroffenen Person auf einen speziellen Fall bezogene, freiwillig und eindeutig abgegebene Willensäußerung, die bekundet, dass die betroffene Person der Verarbeitung seiner personenbezogenen Daten zustimmt.

9. Genetische Daten
Alle Daten, die Aufschluss über die vererbten oder erworbenen genetischen Merkmale einer natürlichen Person geben, anhand derer eine Person unmissverständlich zuzuordnen ist.

10. Gesundheitsdaten
Alle Daten, die sich auf die körperliche oder geistige Gesundheit von natürlichen Personen beziehen.

11. Profiling
Jede Form der automatisierten Verarbeitung persönlicher Daten, die mit dem Ziel erhoben wurde, personenbezogene Merkmale zu gewinnen. Vor allem solche wie Arbeitsleistungen, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsorte oder Ortswechsel, die dabei helfen, natürliche Personen zu analysieren oder Vorhersagen über diese zu treffen.

12. Pseudonymisierung
Eine Art der Verarbeitung personenbezogener Daten, die keine Rückschlüsse auf einzelne Personen zulässt.

13. Verantwortlicher
Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die allein oder gemeinsam über den Vorsatz der Verarbeitung von persönlichen Daten entscheiden.

14. Verarbeitung
Jeder Vorgang oder jede Vorgangsreihe der/die dazu dient, personenbezogene Daten zu erheben, zu erfassen, zu organisieren, zu ordnen, zu speichern, anzupassen, zu verändern, auszulesen, abzufragen, zu verwenden, offenzulegen, einzuschränken, zu löschen oder zu vernichten.

15. Verletzung des Schutzes personenbezogener Daten
Jede beabsichtigte oder unbeabsichtigte Verletzung der Datensicherheit, die zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung der Daten an unberechtigte Dritte führt, die diese dann verwenden.

8. Checkliste für Unternehmen: Diese Fragen sollten Sie sich jetzt stellen.

1. Was wird sich ändern?
2. Bin ich von der Verordnung betroffen und wenn ja, inwieweit?
3. Brauche ich einen Datenschutzbeauftragten? (siehe dazu Kapitel 3)
4. Wieviel Zeit brauche ich für die Umsetzung der Maßnahmen?
5. Welche Strafe erwartet mich, wenn ich den Stichtag nicht einhalte?
6. Wo bekomme ich Hilfe/Beratung bei der Umsetzung?

9. Kontakte / Touchpoints

shopware AG

Ebbinghoff 10

48624 Schöppingen

Fon: +49 (0) 2555 92885-0

Fax: +49 (0) 2555 92885-99

info@shopware.com

Protected Shops GmbH

Theresienhöhe 26

80339 München

Tel.: +49 (0)89 7298905 0

Fax: +49 (0)89 7298905 99

Email: info@protectedshops.de

Trusted Shops GmbH

Colonius Carré

Subbelrather Straße 15c

50823 Köln

Telefon: 0221 – 77 53 66

Fax: 0221 – 77 53 6 89

E-Mail: info@trustedshops.de