VSV ASVAD

mll

Whitepaper

Datenschutz im Online-Handel

Zurich, 3. April 2018

Verband des Schweizerischen Versandhandels VSV

www.vsv-versandhandel.ch
Bahnhofplatz 1 | 3011 Bern

Meyerlustenberger Lachenal AG
Rechtsanwälte – Attorneys at Law

www.mll-legal.com | www.mll-news.com
Zürich | Genève | Zug | Lausanne | Brussels

Whitepaper – Datenschutz im Online-Handel

Das Datenschutzrecht in Europa steht vor grundlegenden Veränderungen. Auf EU-Ebene wird die Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 in Kraft treten. Ausgehend davon ist auch in der Schweiz eine Totalrevision des Datenschutzrechts im Gange. Welche konkreten Änderungen die Revision des schweizerischen Datenschutzrechts mit sich bringen wird und wann diese gelten werden, ist aktuell noch unklar.

Fest steht immerhin, dass sich der Schweizer Gesetzgeber zu einem grossen Teil am EU-Vorbild orientieren wird. Die Neuerungen werden branchenübergreifend alle Unternehmen und Organisationen sowie nahezu sämtliche Geschäftsprozesse betreffen. Gerade der gesamte Online-Handel ist stark von den einschneidenden neuen Regelungen betroffen und steht somit vor einer grossen Herausforderung.

Vor diesem Hintergrund zeigt das vorliegende Whitepaper in einem ersten Schritt auf, warum bereits das Inkrafttreten der EU-DSGVO für Mitglieder des VSV relevant ist. In einem nächsten Schritt werden die zentralen Themen und Vorgaben sowie der daraus resultierende Handlungsbedarf für den Online-Handel erklärt.

VSV ASVAD mll

Inhaltsverzeichnis

I. Datenschutz betrifft nahezu sämtliche Geschäftsvorgänge!

Die Erfahrungen aus der Praxis machen deutlich, dass sich Unternehmen vielfach gar nicht bewusst sind, wie weit die Vorschriften des Datenschutzrechts in ihren Unternehmensalltag hineingreifen.

> Das Datenschutzrecht gilt bei jedem geschäftlichen Umgang mit personenbezogenen Daten.

Die Tragweite zeigt sich bereits in der Aufzählung der relevanten „Verarbeitungen". Nach der gesetzlichen Umschreibung zählen hierzu insbesondere: „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung".

Beispiel:

Das Datenschutzrecht ist also nicht nur dann zu beachten, wenn die Anschrift von Kunden an ein Transportunternehmen übermittelt wird, sondern **auch bei rein internen Vorgängen**, wie wenn der Kunde in der Datenbank einer bestimmten Kundengruppe zugeteilt wird, um ihm „personalisierte" Werbung zukommen zu lassen.

Auch die Voraussetzung, dass es sich um *„personenbezogene Daten"* handeln muss, führt nicht zu einer derart weiten Einschränkung, wie häufig angenommen wird. Erforderlich ist zwar eine Information, die einer bestimmten (natürlichen) Person zugeordnet werden kann. Jedoch zählen hierzu insbesondere **auch pseudonymisierte Daten.** Wenn also beispielsweise in einer Datenbank die Personalien (Name, Adresse etc.) eines Kunden durch eine Nummer ersetzt werden, handelt es sich bei den Bestelldaten zu dieser Nummer immer noch um personenbezogene Daten, wenn eine Person im Unternehmen oder allenfalls gar ein Dritter die Nummer wieder dem Kunden zuordnen kann. Dieser Aspekt wird vielfach bereits im Zusammenhang mit den Grundfunktionen von Websites vernachlässigt und deshalb dem Datenschutz zu wenig Rechnung getragen.

Beispiel:

Sucht ein Nutzer im Onlineshop ein bestimmtes Produkt, hinterlässt er bereits beim blossen Aufruf des Onlineshops eine Vielzahl von technischen Daten (insb. die **IP-Adresse**). Diese werden (automatisch) auf dem Server des Onlineshops gespeichert und müssen aufgrund der Gerichtspraxis als personenbezogene Daten behandelt werden, selbst wenn der Nutzer seinen Namen nicht oder noch nicht mitgeteilt hat.

II. Warum und wann ist die DSGVO für CH-Unternehmen relevant?

Zwei der grundlegendsten Neuerungen gegenüber der bis Mai 2018 geltenden Rechtslage verdeutlichen, weshalb die DSGVO für Schweizer Unternehmen von grosser Relevanz ist: Zum einen verlangen die Vorschriften der DSGVO auch weit über die Grenzen des EU-Binnenmarkts hinaus Geltung. Zum anderen drohen bei Verletzung der Vorschriften Bussgelder in Millionenhöhe.

1. Wann ist die DSGVO auf Schweizer Unternehmen anwendbar?

Ausgehend von den einschneidenden Konsequenzen, die bei der Nichteinhaltung der DSGVO drohen, stellt sich die Frage, für wen diese Vorgaben überhaupt gelten. Dies lässt sich am besten anhand von verschiedenen beispielhaften Konstellationen erläutern. Wie die

nachfolgenden Beispiele deutlich machen, ist der Anwendungsbereich der Verordnung bewusst sehr weit gefasst.

> Die DSGVO gilt insbesondere **nicht nur für Datenbearbeitungen, die innerhalb der EU erfolgen.** Zudem sind die Vorschriften **auf zahlreiche Unternehmen ohne Niederlassung in der EU anwendbar**.

Von den neuen Vorgaben sind deshalb weit mehr Unternehmen ausserhalb der EU betroffen als von anderen EU-Regeln. Wenig überraschend ist deshalb vielen (noch) nicht bewusst, dass die DSGVO auch für sie gilt.

a. Schweizer Online-Shops mit Niederlassung in der EU

Eine erste Konstellation betrifft Fälle, in welchen es auf den ersten Blick nicht erstaunlich ist, dass die DSGVO Anwendung verlangt:

> Unternehmen mit Sitz in der Schweiz müssen die DSGVO einhalten, wenn sie über eine Niederlassung in der EU verfügen und im Rahmen der Tätigkeiten dieser Niederlassung personenbezogene Daten bearbeiten.

Als Niederlassung gelten insbesondere Tochtergesellschaften. Verfügt also eine Schweizer Muttergesellschaft über eine Tochtergesellschaft in der EU, die an Datenbearbeitungen der Mutter teilnimmt, z.B. indem sie ihr Daten über die bei ihr eingegangenen Bestellungen übermittelt, ist die DSGVO auch auf die Weiterverarbeitung der Daten durch die Muttergesellschaft anwendbar. Dasselbe gilt, wenn die Muttergesellschaft der Tochtergesellschaft Daten zur Bearbeitung übermittelt, resp. zugänglich macht.

Zu beachten ist jedoch, dass der Begriff „Niederlassung" weit verstanden wird. Erfasst werden auch blosse Zweigniederlassungen, Abteilungen oder allgemein „feste Einrichtungen".

Beispiel:

Deshalb kommen beispielsweise auch blosse Werbeniederlassungen, in welchen lediglich geringfügige Tätigkeiten ausgeübt werden, als Niederlassungen in Frage und ist die DSGVO grundsätzlich auf die in diesem Rahmen vorgenommenen Datenbearbeitungen anwendbar.

b. Schweizer Online-Shops ohne Niederlassung in der EU

1. Angebot von Waren oder Dienstleistungen an EU-Kunden

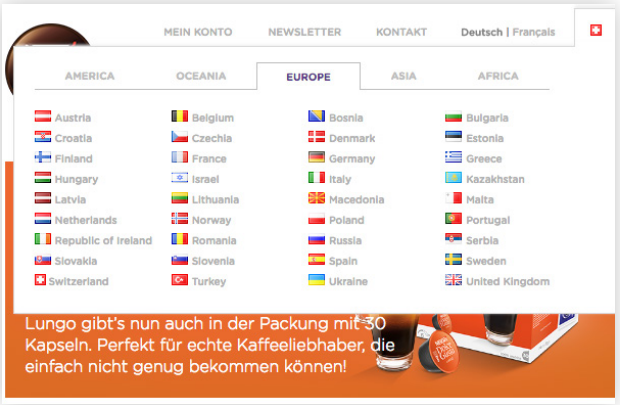
> Den Vorgaben der DSGVO sind auch Schweizer Unternehmen unterstellt, die ihre Waren oder Dienstleistungen an Kunden in der EU anbieten und in diesem Zusammenhang personenbezogene Daten bearbeiten.

Als „Anbieten" im Sinne der DSGVO gilt nur ein offensichtlich beabsichtigtes Angebot an Kunden in der EU. Dies dürfte jedoch gerade bei einer Vielzahl von Onlineshops regelmässig der Fall sein. Entscheidend ist dabei die Frage, ob der Onlineshop bewusst und gezielt Anstrengungen unternimmt, potentielle Kunden mit Wohnsitz in der EU anzusprechen und anzuwerben. Ist dies der Fall, ist das Angebot eben auf EU-Kunden ausgerichtet und diese Kunden können sich auf ihre Rechte unter der DSGVO berufen, wenn

das Schweizer Unternehmen ihre Daten entsprechend bearbeitet. Bei der Beurteilung, ob sich ein Angebot an EU-Kunden richtet, werden verschiedene Kriterien als Indizien herangezogen.

Beispiel:

Solche Indizien sind beispielsweise die Verwendung von Top-Level-Domains aus EU-Mitgliedsstaaten (.de,.at,.fr etc.), Drop-down-Menüs für die Wahl der Sprache oder „des Landes", die Angabe von Versandkosten in EU-Mitgliedstaaten oder die Zahlungsmöglichkeit in verschiedenen Währungen wie dem Euro.

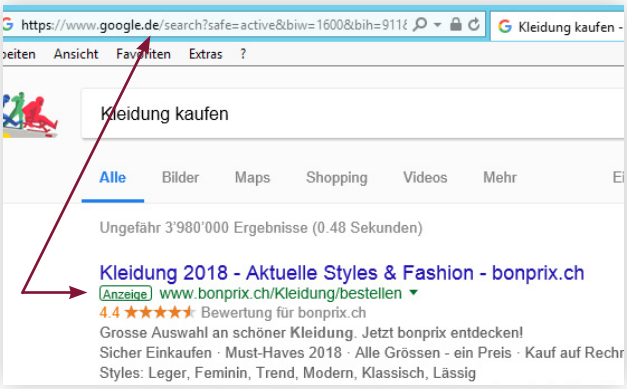


Quelle: www.dolce-gusto.ch (besucht am: 3.4.2018)

Wird für ein Angebot gezielt auf EU-Kunden ausgerichtete Online-Werbung gemacht (bspw. durch entsprechend geographisch geplante AdWords-Kampagnen), ist dies ein offensichtlicher Beleg dafür, dass sich das beworbene Angebot an Kunden im entsprechenden Gebiet richten soll. In diesen Fällen müssen daher die Vorschriften der DSGVO für die mit dem Angebot zusammenhängenden Datenbearbeitungen beachtet werden.

Beispiel:

Wer bei Google für die Keywords „Kleidung kaufen" Anzeigen für die Aufschaltung auf google.de bucht, richtet sein Angebot auch an deutsche Kunden. Folglich ist auf diese Anbieter grundsätzlich die DSGVO anwendbar.



Quelle: www.google.de (besucht am: 3.4.2018)

Zu einer erheblichen Ausweitung des Anwendungsbereichs führt schliesslich auch, dass **unentgeltliche Angebote ebenfalls erfasst** werden. Somit sind auch die Betreiber von reinen Informations-Websites der DSGVO unterstellt, wenn die Website (auch) auf Personen in der EU ausgerichtet ist und darüber bspw. Dienstleistungen an Kunden im EU-Ausland angeboten, resp. beworben werden. Massgebliche Kriterien für die Beurteilung der Ausrichtung sind hier unter anderem die Sprach-Versionen der Website, die Top-Level-Domain oder die Angabe der internationalen Vorwahl. Insbesondere ist jede Form von gezieltem Online-Marketing in den EU-Märkten ein klarer Beleg für die Ausrichtung.

2. Beobachten des Verhaltens von EU-Bürgern

> Zur Anwendbarkeit der DSGVO führt nicht nur das Anbieten von Produkten, sondern bereits die blosse Beobachtung des Verhaltens von Personen in der EU.

Damit zielt die Verordnung primär auf Internetsachverhalte ab. Gerade bei Onlineshops führt dieser Tatbestand in der Regel zur Anwendbarkeit der DSGVO. Davon erfasst sind Datenbearbeitungsvorgänge, mit welchen das Verhalten von Personen in der EU, meist zu Werbezwecken, nachvollzogen werden sollen.

Deshalb gelangt die DSGVO grundsätzlich bei sämtlichen Methoden des sog. User/Customer-Trackings, insbesondere denjenigen, die unter Rückgriff auf Cookies funktionieren, zur Anwendung.

Beispiel:

Setzt also bspw. ein Online Händler auf seiner Website Analyse-Tools zur Auswertung der Website-Besuche und des Klickverhaltens, wie bspw. Google Analytics ein, so muss von der Anwendbarkeit der DSGVO ausgegangen werden.

3. Beauftragung oder Auftrag von EU-Unternehmen

Ein weiterer Umstand, der dazu führt, dass Schweizer Unternehmen ohne Niederlassung in der EU der DSGVO unterstehen, sind sog. **Auftragsdatenverarbeitungsverhältnisse.** Dies ist relevant, wenn ein Schweizer Unternehmen ein anderes Unternehmen oder einen beliebigen Dritten damit beauftragt, eigene Daten (bspw. Mitarbeiter- oder Kundendaten) der Auftraggeberin allein zu deren Zwecken und in ihren Interessen zu bearbeiten.

Beispiel:

Nutzt ein Schweizer Unternehmen daher beispielsweise zur Speicherung von personenbezogenen Daten die Dienste eines Cloud-Speicher-Anbieters mit Niederlassung in der EU, ist die DSGVO anwendbar. Gleiches gilt umgekehrt, wenn beispielsweise ein Schweizer Unternehmen Personendaten im Auftrag eines EU-Unternehmens bearbeitet. Erfolgt die zentrale Datenbearbeitung eines internationalen E-Commerce-Unternehmens also beispielsweise durch ein Unternehmen in der Schweiz jedoch im Auftrag der zugehörigen EU-Unternehmen, müssen die Vorschriften der DSGVO durch die Schweizer Datenbearbeiterin beachtet werden.

Bei Auftragsverarbeitungskonstellationen kann die Beurteilung der Anwendbarkeit der DSGVO bzw. der Umfang der Anwendung der DSGVO im Einzelfall schwierig sein. Deshalb ist gerade in solchen Konstellationen eine sorgfältige Analyse der Datenbearbeitungen erforderlich.

2. Einschneidende Sanktionen bei Verstoss gegen Datenschutzvorschriften

Datenschützer bemängelten die bisher geltende Rechtslage bereits deshalb, weil die Sanktionen für Datenschutzverletzungen zu wenig abschreckend waren. Demzufolge hatten die datenbearbeitenden Unternehmen nur wenig Anreiz, um den Aufwand für die Datenschutz-Compliance genügend ernst zu nehmen.

Dies wird sich durch das Inkrafttreten der DSGVO nun drastisch verändern müssen:

> Künftig drohen bei Datenschutzverletzungen Verwaltungssanktionen in der Höhe von **bis zu 20 Millionen Euro oder 4% des weltweiten Umsatzes**, je nach dem welcher der beiden Beträge höher ist.

Der Bussgeldrahmen wurde damit EU-weit stark erhöht und vereinheitlicht. Inwieweit die zuständigen Aufsichtsbehörden von diesem „Strafrahmen" Gebrauch machen werden und wie häufig inskünftig tatsächlich Sanktionen ausgesprochen werden, lässt sich derzeit nur schwer abschätzen. In Kombination mit den bereits seit einiger Zeit zunehmend an Bedeutung gewinnenden Reputationsrisiken stellt aber jedenfalls bereits die Aussicht auf die Verwaltungssanktionen einen sehr gewichtigen Anreiz dar, sich mit der Einhaltung der datenschutzrechtlichen Vorgaben inskünftig viel ernsthafter auseinander zu setzen.

Darüber hinaus haben die von einer Datenbearbeitung betroffenen Personen verschiedene Möglichkeiten **ihre Rechte auf zivilrechtlichem Weg durchzusetzen.**

So können sie beispielsweise ein gerichtliches Verbot bestimmter Handlungen erwirken und unter Umständen Schadenersatz fordern. Namentlich in Deutschland drohen bei Datenschutzverletzungen zudem Abmahnungen durch Konkurrenten mit anschliessenden Gerichtsverfahren. Entsprechende Gerichtsentscheide sind gegenüber Unternehmen in der Schweiz in der Regel ohne weiteres vollstreckbar. Schliesslich sehen die nationalen Gesetze der Mitgliedstaaten weiterhin zusätzliche Straftatbestände für bestimmte Datenschutzverstösse vor.

III. Welche Grundprinzipien gelten im Umgang mit Personendaten?

Die DSGVO und auch die laufende Totalrevision des Schweizer Datenschutzrechts bringen weitreichende Neuerungen mit sich. Das neue Schweizer Datenschutzgesetz (DSG) wird zwar voraussichtlich in verschiedenen Punkten weniger weit gehen, als die neuen EU-Regelungen. Aufgrund des dargestellten weiten Anwendungsbereichs der EU-DSGVO werden jedoch, wenn überhaupt, nur sehr wenige Online-Händler nicht davon erfasst sein. Bei den nachfolgenden Erläuterungen liegt der Fokus deshalb auf den bereits feststehenden, ab dem 25. Mai 2018 geltenden, Vorgaben der DSGVO.

1. Es ist verboten, Personendaten zu bearbeiten, es sei denn...

Zentral aus der Sicht von Schweizer Unternehmen ist das in der DSGVO vorgesehene Konzept des sog. **„Verbots mit Erlaubnisvorbehalt“**:

> Nach diesem Konzept ist im Grundsatz jede Bearbeitung von personenbezogenen Daten verboten. Erlaubt ist eine Bearbeitung, bspw. von Kundendaten nur, wenn sich ein Unternehmen auf einen sog. Erlaubnistatbestand berufen kann, nach dem die Bearbeitung eben zulässig ist.

Die DSGVO nennt sodann auch die entsprechende Erlaubnistatbestände. Zulässig ist demnach die Datenbearbeitung gemäss DSGVO insbesondere gestützt auf:

- **eine Einwilligung**: Eine Datenbearbeitung ist zulässig, wenn sie auf einer wirksamen Einwilligung der betroffenen Person beruht. Die Anforderungen an eine gültige, rechtswirksame Einwilligung sind aber deutlich erhöht und entsprechen nicht der in der Schweiz bislang verbreiteten unternehmerischen Praxis im Umgang mit Einwilligungen (s. dazu unten).
- **einen Vertrag**: Eine Datenbearbeitung ist erlaubt, wenn sie zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist. Deshalb darf ein Online-Händler die Bestelldaten natürlich nach wie vor bearbeiten, soweit es für die vertragsgemässe Abwicklung der Bestellung notwendig ist. Dazu wird keine zusätzliche Einwilligung benötigt.
- **ein Gesetz**: Erlaubt sind Datenverarbeitungen, die zur Erfüllung einer gesetzlichen Verpflichtung (z.B. Aufbewahrungspflichten) erforderlich sind. Zu beachten ist, dass schweizerische Gesetze nicht unter diesen Erlaubnistatbestand fallen. Bei schweizerischen gesetzlichen Pflichten dürfte jedoch regelmässig ein überwiegendes Interesse gegeben sein (siehe nachfolgend).
- **ein überwiegendes Interesse**: Eine Datenbearbeitung kann schliesslich erlaubt sein, wenn sie zur Wahrung eines berechtigten Interesses des Unternehmens erforderlich ist, sofern dieses Interesse dasjenige der betroffenen Person überwiegt. Hier ist aber gerade bei bloss wirtschaftlichen Interessen an der Durchführung von Marketingmassnahmen stets eine sorgfältige Prüfung im Einzelfall erforderlich.

2. Grundprinzipien jeder rechtmässigen Datenbearbeitung

Das Vorliegen eines Erlaubnistatbestands führt allerdings alleine noch nicht dazu, dass eine Datenbearbeitung den Vorgaben der DSGVO entspricht. Vielmehr sind insbesondere auch die sog. **Datenverarbeitungsgrundsätze** einzuhalten. Damit sind Grundprinzipien einer rechtmässigen Datenbearbeitung gemeint, die bereits im geltenden EU- und Schweizer Recht vorgesehen sind. Neu sind diese konkretisiert sowie verschärft worden und vor allem ist deren Verletzung neu sanktionsbedroht.

Hervorzuheben sind dabei die folgenden Grundsätze:

- **Zweckbindungsgrundsatz**: Personenbezogene Daten dürfen nur für eindeutig definierte und erkennbare Zwecke erhoben und bearbeitet werden.
- **Transparenzgrundsatz**: Die Datenbearbeitung und die damit verfolgten Zwecke müssen für die betroffene Person ab dem Moment der Erhebung und jederzeit danach nachvollziehbar sein. Diese Transparenz soll u.a. durch die ausgebauten Informationspflichten (siehe dazu weiter unten) sichergestellt werden.
- **Datenminimierung**: Es dürfen nur personenbezogene Daten erhoben werden, die für die Erreichung des festgelegten Verarbeitungszwecks erforderlich sind. Es dürfen keine Daten auf Vorrat erfasst und weiterbearbeitet werden.
- **Speicherbegrenzung**: Personenbezogene Daten dürfen nur so lange gespeichert werden, als es zur Erreichung des festgelegten Verarbeitungszwecks erforderlich ist. Ist der Zweck erfüllt, müssen die Daten gelöscht werden.

3. Umfangreiche neue Pflichten im Umgang mit Daten

Die DSGVO auferlegt den Unternehmen darüber hinaus eine Vielzahl von neuen formellen Pflichten.

Hervorzuheben ist dabei Folgendes:

- **Datenverarbeitungsverzeichnis**: Jedes Unternehmen, welches personenbezogene Daten bearbeitet, muss neu ein Verzeichnis aller relevanten Datenverarbeitungen führen. In diesem Verzeichnis muss für jeden entsprechenden Bearbeitungsprozess eine Reihe von Informationen dokumentiert und detailliert beschrieben werden (bspw. Zweck, Verantwortung, Art der Daten, spezifische Risiken, etc.).
- **Nachweispflicht**: Die DSGVO verlangt explizit, dass Datenbearbeiter jederzeit die Einhaltung der Datenverarbeitungsgrundsätze nachweisen können. Somit besteht eine Dokumentationspflicht aller datenschutzrechtlich relevanten Vorgänge. Dazu dient u.a. das Datenverarbeitungsverzeichnis.
- **Informationspflicht**: Die DSGVO verlangt, dass Unternehmen, die personenbezogene Daten bearbeiten, zum Zeitpunkt der Erhebung der Daten den betroffenen Personen gewisse Informationen betreffend die Datenbearbeitung zur Verfügung stellen. Die Information kann beispielsweise durch eine Datenschutzerklärung für den Onlineshop sichergestellt werden.
- **Datenschutz-Folgeabschätzung**: Bei Datenverarbeitungen, die voraussichtlich ein hohes Risiko für die Betroffenen in sich bergen können, muss eine Abschätzung dieser Folgen durchgeführt und dokumentiert werden. Dies wird insbesondere bei der Verwendung neuer Technologien und dem Einsatz neuartiger Datenverarbeitungsvorgängen zu prüfen sein. Die Datenschutz-Folgeabschätzung setzt sich aus der Beschreibung und Analyse der Datenbearbeitung, der Bestimmung der Risiken und der Erarbeitung eines Massnahmenplans zur Reduktion der erkannten Risiken zusammen.
- **„Data Breach Notifications"**: Verstösse gegen die Vorgaben der DSGVO, insb. der Missbrauch, Verlust oder der Diebstahl von Daten sind unter bestimmten Voraussetzungen der Aufsichtsbehörde und den betroffenen Personen zu melden. Für die Umsetzung dieser Pflicht müssen in vielen Unternehmen dokumentierte interne Prozesse implementiert werden, d.h. es muss bestimmt werden, in welchen Konstellationen Mitarbeiter an welche interne verantwortliche Person Meldung machen müssen.

- **Privacy by Design/ by Default**: Die Datenverarbeitungen sind so auszugestalten, dass die Einhaltung des Datenschutzes und die Ausübungen der Betroffenenrechte (Auskunft, Löschung, Berichtigung) jederzeit sichergestellt ist (Privacy by Design). Zudem muss jede Datenbearbeitung so ausgestaltet sein, dass die datenschutzfreundlichsten Voreinstellungen als Standard hinterlegt sind (Privacy by Default).
- **Bestellung eines Vertreters**: Unternehmen ohne Niederlassung in der EU müssen in der Regel einen Vertreter in der EU bestellen, sofern ihre Datenbearbeitungen der DSGVO unterliegen.

4. Welche Rechte haben die Personen, deren Daten bearbeitet werden („Betroffenenrechte")?

Eine rechtmässige Datenbearbeitung bedingt, dass die Personen, deren Daten bearbeitet werden, jederzeit nachvollziehen können, welche Daten über sie und in welcher Art und Weise bearbeitet werden. Die DSGVO sieht deshalb sog. Betroffenenrechte vor, d.h. formelle Rechtsansprüche gegenüber den Bearbeitern ihrer Daten. Ein Grossteil dieser Rechte bestand zwar im Grundsatz bereits im bisherigen Recht, doch wurden sie verschiedentlich ausgebaut und angepasst.

Eine betroffene Person hat insbesondere folgende Rechte. Diese kann sie jederzeit geltend machen:

- **Auskunftsrecht**: Die Betroffenen können von Unternehmen jederzeit detaillierte Auskunft über die sie betreffenden Datenbearbeitungen verlangen. Um den Auskunftsersuchen der Betroffenen nachzukommen, dienen u.a. das Datenverarbeitungsverzeichnis und die entsprechende Dokumentation der Datenbearbeitungen. Das Auskunftsrecht gilt auch für Arbeitnehmer und Angestellte von Geschäftspartnern.
- **Berichtigungsrecht**: Neben der grundsätzlichen Pflicht des bearbeitenden Unternehmens, Massnahmen zur Sicherstellung der Richtigkeit von Daten zu treffen, können Betroffene jederzeit die unverzügliche Berichtigung unrichtiger Daten fordern.
- **Löschungs- und Widerspruchsrecht**: Betroffene können grundsätzlich unter bestimmten Voraussetzungen der Durchführung einer Datenbearbeitung widersprechen und die Löschung von Daten (sog. Recht auf Vergessen) verlangen.
- **Datenportabilität**: Nach der DSGVO müssen erfasste Daten so bearbeitet werden, dass sie der betroffenen Person jederzeit in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben werden können.

IV. Zentrale Themen für den Online-Handel

Die meisten Mitglieder des VSV führen regelmässig Datenbearbeitungen durch, die vom Anwendungsbereich der DSGVO erfasst sind, insbesondere, wenn sie sich mit ihrem Angebot auch an potentielle Kunden in der EU wenden wollen (siehe dazu oben). Dies ist auch dann der Fall, wenn die Bearbeitung physisch ausschliesslich in der Schweiz durchgeführt wird. Entsprechend müssen diese Datenbearbeitungen im Hinblick auf das Inkrafttreten der DSGVO überprüft und, sofern notwendig, angepasst werden. **Stichtag** für die Umsetzung der entsprechenden Anpassungen ist der **25. Mai 2018**. Nachfolgend werden einige der für die Mitglieder des VSV zentralen Datenschutzthemen beleuchtet, die wesentlichsten Problemstellungen erläutert und mit konkreten Beispielen veranschaulicht.

1. Grundsätze der Datenbearbeitung

a. Transparenz der Datenbearbeitung / Informationspflichten

Der erste Schritt einer jeden Datenbearbeitung ist die Erhebung der Daten. Nach der DSGVO besteht bei jeder Beschaffung von personenbezogenen Daten die Pflicht, umfangreiche Informationen rund um die beabsichtigte Datenbearbeitung aktiv, also unaufgefordert, zur Verfügung zu stellen.

Beispiel:

Werden die Daten im Rahmen des Bestellprozesses im Onlineshop erhoben, ist in der Datenschutzerklärung klar zu stellen, dass die Daten für die Abwicklung der Bestellung bearbeitet werden. Dies gilt umso mehr, wenn die Daten darüber hinaus auch zu Werbezwecken verwendet werden sollen, wie z.B. den Versand des Newsletters.

Die DSGVO unterscheidet bezüglich dem Inhalt einer transparenten Information zwischen Daten, die **direkt von der betroffenen Person, resp. beim Kunden** beschafft wurden und solchen, die **aus dritten Quellen** stammen. In beiden Fällen wurde die Liste der gesetzlich vorgeschriebenen Information stark ausgebaut. Verlangt werden „leicht verständliche" und „präzise" Angaben.

1. Informationspflicht bei der direkten Erhebung von Daten beim Kunden

Im Falle der **Beschaffung der Daten direkt bei der betroffenen Person** schreibt die DSGVO folgende transparent und vorgängig zu erteilende Informationen vor:

1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
2. Kontaktdaten des allfälligen Datenschutzbeauftragten
3. Zwecke und Rechtsgrundlage der Datenbearbeitung
4. ggf. die berechtigten Interessen an einer Datenverarbeitung
5. ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
6. ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
7. weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten
8. Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
10. Widerrufsrecht, sofern die Datenbearbeitung auf einer Einwilligung beruht
11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
12. ggf., ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsschluss erforderlich ist
13. Bestehen einer automatisierten Entscheidungsfindung, einschliesslich Profiling, sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Diese Informationen müssen überall dort **gut sichtbar und zugänglich** sein, wo personenbezogene Informationen beschafft werden. Dies ist insbesondere bei sämtlichen Kontakt- oder Bestellformularen der Fall. Die Unternehmen müssen deshalb namentlich Datenschutzerklärungen erstellen, welche die Pflichtinformationen enthalten, oder bereits vorhandene Datenschutzerklärungen entsprechend überarbeiten. Diese Datenschutzerklärungen müssen schliesslich insbesondere über die Websites einfach und jederzeit auffindbar und zugänglich sein.

Beispiel:

Datenschutzerklärungen auf Websites, über welche Daten erhoben oder gesammelt werden, müssen nicht nur oberhalb der jeweiligen Buttons, wie z.B. „Weiter", „Bestätigen" oder „Absenden" verlinkt sein, sondern auch beim Öffnen einzelner Unterseiten abgerufen werden können. In der Praxis wird das dadurch gelöst, dass die Datenschutzerklärung in einer ständig angezeigten Fusszeile verlinkt wird (sog. Footer). Eine bloss nachträgliche Information, beispielsweise durch Zusendung der Datenschutzerklärung in einem Bestätigungsmail oder den Hinweis/die Verlinkung auf die Datenschutzerklärung nach bereits erfolgter Erhebung der Daten, wäre ungenügend.

2. Informationspflicht bei der Erhebung von Daten aus Drittquellen

Auch bei der **Datenbeschaffung aus Drittquellen** besteht eine Informationspflicht. In diesen Fällen müssen, mit gewissen Abweichungen, dieselben umfangreichen Informationen erteilt werden, wie dies bei der direkten Datenbeschaffung bei der betroffenen Person verlangt wird.

Mit der Beschaffung aus Drittquellen sind Fälle gemeint, in welchen die Daten nicht bei der betroffenen Person, sondern beispielsweise bei Dritten oder aus öffentlich zugänglichen Quellen erhoben werden.

Beispiel:

Bei Online-Händlern wird bei der Wahl der Zahlungsoption „auf Rechnung" in der Regel im Hintergrund eine Bonitätsprüfung vorgenommen. Das Ergebnis der Bonitätsprüfung stammt regelmässig aus einer Drittquelle. Darum muss dies auch in der Datenschutzerklärung transparent gemacht werden. Diese Information muss zudem vor der Durchführung der Bonitätsprüfung erfolgen.

b. Zweckbindung der Datenbearbeitung

In der Regel wollen Online-Händler die erhobenen Daten für mehrere Zwecke nutzen, die sich zudem über die Zeit verändern können. Dies kann zu Konflikten mit dem Grundsatz der Zweckbindung führen. Die betroffene Person muss nämlich zum Zeitpunkt der erstmaligen Datenerhebung über den vollständigen Verwendungszweck informiert sein. Dieser Zweck darf anschliessend grundsätzlich nicht geändert, resp. ausgeweitet werden.

Beispiel:

Werden die Daten im Rahmen des Bestellprozesses im Onlineshop erhoben, ohne Information über weitere Zwecke, dürfen diese grundsätzlich nur für den Zweck der Bestellungsabwicklung verwendet werden. In diesem Fall dürften diese Daten beispielsweise nicht in ein CRM-System und entsprechende Analyse einfliessen.

Durch eine sorgfältige Beschreibung der Zwecke der Datenbearbeitungen in einem Online-Shop und einer entsprechenden Information der betroffenen Person können die Daten selbstverständlich auch weitergehend genutzt werden. Dies setzt aber voraus, dass sich der Online-Händler bereits vor der jeweiligen Bearbeitung der Daten bewusst ist, für welche Zwecke die Daten bearbeitet werden sollen, und dass die betroffene Person entsprechend informiert wurde (siehe dazu auch oben). Die spätere Bearbeitung zu anderen Zwecken ist zwar nicht gänzlich ausgeschlossen, jedoch müssen die Betroffenen vor der Bearbeitung über diese **Zweckänderung** informiert werden und es muss wiederum ein Erlaubnistatbestand (z.B. eine Einwilligung) vorliegen. Dies dürfte in der Praxis kaum ohne Datenverlust, d.h. nicht-aktualisierte Einwilligungen, in beträchtlichem Ausmass möglich sein.

c. Grundsatz der Datensparsamkeit

Gerade im Onlinehandel spielt der Grundsatz der Datensparsamkeit (die DSGVO spricht von Datenminimierung) eine wichtige Rolle. Mit Blick auf die Auslieferung von Bestellungen erheben Online-Händler im Rahmen des Checkout-Prozesses regelmässig eine Vielzahl von persönlichen Angaben direkt bei den betroffenen Personen. Auch zur blossen Kontaktaufnahme über die verbreiteten Standardformulare verlangen Shop-Betreiber mehrere persönliche Angaben.

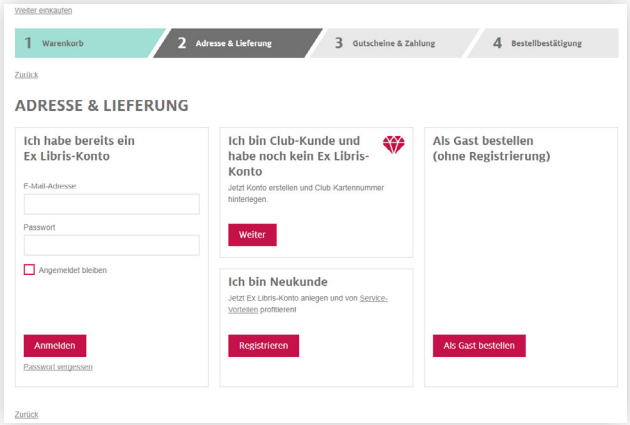
Es gilt jedoch dabei zu beachten, dass immer nur so viele Daten erhoben werden, wie dies zur Verwirklichung des Bearbeitungszwecks auch nötig ist. Der Online-Händler muss sich somit vorab die Frage stellen, ob die verlangten Angaben zur Erreichung der verfolgten Zwecke der Datenbearbeitungen wirklich erforderlich sind. Massstab hierfür sind insbesondere die in der Datenschutzerklärung enthaltenen Informationen über die Bearbeitungszwecke. Sind die Angaben für diese Zwecke nicht erforderlich, muss von der Erhebung der Daten im Sinne des Gebots der Datenminimierung abgesehen werden.

Beispiele:

Für die Abwicklung der Bestellung können von den Kunden die Angabe des Namens, des Vornamens, der Adresse sowie allenfalls Kreditkartenangaben verlangt werden.

Wird für die Abwicklung der Bestellung als Pflichtfeld allerdings zusätzlich die Anzahl Familienmitglieder verlangt, so wäre dem Gebot der Datenminimierung nicht genügend Rechnung getragen.

Ähnliche Fragen stellen sich auch rund um die Eröffnung von **Kundenkontos**. Zur Abwicklung der Bestellung ist die Eröffnung eines Kundenkontos und die damit verbundene dauerhafte Speicherung zusätzlicher Angaben durch den Shop-Betreiber nicht erforderlich. Aus diesem Grund wird allgemein davon ausgegangen, dass den Kunden die Möglichkeit zur Bestellung als Gast, also ohne Registrierung, zur Verfügung gestellt werden muss.



Quelle: www.exlibris.ch/de/bestellung/login/ (besucht am 3.4.2018)

2. Einwilligung als wichtiger Erlaubnistatbestand

Jede Bearbeitung von personenbezogenen Daten muss sich auf einen sog. Erlaubnistatbestand abstützen, andernfalls ist sie nach der DSGVO verboten. Einen sehr wichtigen Erlaubnistatbestand stellt die Einwilligung der betroffenen Person dar. Die Anforderungen an die Gültigkeit einer rechtswirksamen Einwilligung werden mit der DSGVO deutlich erhöht.

> Damit eine Einwilligung gültig ist, muss sie insbesondere gestützt auf **ausreichender vorgängiger Information** und **freiwillig** erfolgen sowie in **unmissverständlicher Form** abgegeben werden.

Die erhöhten Anforderungen gelten auch, wenn Betroffene bereits vor dem Inkrafttreten der DSGVO eine Einwilligung erteilt haben. Mit anderen Worten sind auch **„Alteinwilligungen"** nur gültig, wenn sie die Anforderungen der DSGVO erfüllen. Dies hat eine besondere Bedeutung vor dem Hintergrund der in der Schweiz noch verbreiteten Verwendung von vorangekreuzten Einwilligungserklärungen (siehe dazu weiter unten).

a. Freiwilligkeit und Koppelungsverbot

Eine der zentralsten Anforderungen stellt die Freiwilligkeit der Einwilligung dar. An der Freiwilligkeit kann es fehlen, wenn ein klares Ungleichgewicht zwischen den Leistungen besteht, welche der betroffenen Person unter einem Vertrag zukommen und den Datenbearbeitungen in die im Rahmen des Vertrages eingewilligt wird.

Von besonderer Bedeutung ist die Frage, ob künftig ein sog. **Kopplungsverbot** gilt. Danach wäre es verboten, die Erfüllung eines Vertrags von der Einwilligung in weitere Datenverarbeitungen abhängig zu machen. Gemeint sind damit nicht Datenverarbeitungen, die für die Abwicklung eines Vertrags erforderlich sind, sondern primär die Verwendung von Daten zu Werbezwecken.

Beispiel:

Demnach dürfte ein Online-Händler die Bestellung eines Produkts nicht von der Einwilligung in die Weitergabe der Daten an einen Adresshändler abhängig machen.

Nach aktuellem Stand steht fest, dass solche Kopplungen problematisch sein können. Bis zur Etablierung einer Praxis durch die Aufsichtsbehörden sind solche Praktiken risikobehaftet und sollten entweder unterlassen werden oder es sollte den Betroffenen eine Wahlmöglichkeit zur Verfügung gestellt werden.

b. Vorselektierte Kästchen

Die Problematik des Kopplungsverbots wird weiter dadurch verstärkt, dass Einwilligungen nur dann gültig sind, wenn sie durch eine eindeutige bestätigende Handlung zum Ausdruck gebracht werden.

> Stillschweigen oder Untätigkeit der betroffenen Person genügen daher nicht.

Beispiel:

Im vorher genannten Beispiel würde daher so oder so keine gültige Einwilligung für die Datenweitergabe vorliegen, wenn diese auf einem **vorangewählten Kästchen** basiert. Der Kunde muss die Checkbox vielmehr selber durch einen Klick markieren, damit seine Einwilligung wirksam ist.

Diese Anforderung führt bei vielen Schweizer Unternehmen zu einer Umstellung. Nach schweizerischer Praxis sind solche vorangekreuzten Check-Boxen in der Regel im Moment noch zulässig. Allerdings bilden entsprechend gesammelte Einwilligungen im Anwendungsbereich der DSGVO nach deren Inkrafttreten am 25. Mai 2018 keine gültige Rechtsgrundlage mehr für die weitere Datenbearbeitung.

3. Datenweitergabe an Dritte

a. Vorbemerkung zur Weitergabe von Daten durch Online-Händler

Im Zusammenhang mit der Geschäftstätigkeit von Online-Händlern stellt sich eine ganze Reihe von Fragen bezüglich der Weitergabe von Daten an Dritte. Beispielsweise beinhaltet die Durchführung einer Bonitätsprüfung, die Versendung der Bestellung über einen Dienstleister oder die Nutzung einer Cloud zur Speicherung der Daten bereits eine Datenweitergabe im Sinne der DSGVO und muss somit auch deren Vorgabe entsprechen.

Es besteht deshalb auch hier eine Informationspflicht. Die Weitergabe an sich muss transparent gemacht und unter anderem erklärt werden, zu welchen Zwecken die Weitergabe erfolgt. Zudem muss der Datenübermittler auch hier nachweisen können, dass ein Erlaubnistatbestand (z.B. Einwilligung oder ein berechtigtes Interesse) gegeben ist.

> Vernachlässigt wird dabei vielfach, dass auch das Bestehen einer **theoretischen Möglichkeit eines Zugriffs** auf Daten als Übermittlung gilt.

Beispiel:

Nach dem Abschluss der Bestellung gibt der Webshopbetreiber einem (Partner-) Unternehmen, welches die Waren lagert und für den Versand vorbereitet, über eine entsprechende Schnittstelle Zugriff auf die Bestelldaten um die Lieferung vorzubereiten.

Abgesehen von den datenschutzrechtlichen Fragen im Zusammenhang mit der Weitergabe von Personendaten, sind mit solchen Zugriffseinräumungen erhebliche **Risiken der Datensicherheit** verbunden.

b. Wer gilt als „Dritter"?

Vor diesem Hintergrund ist von besonderer Bedeutung, wer überhaupt als Dritter gilt. Unternehmen ist oftmals nicht bekannt, dass auch Gesellschaften desselben Konzerns oder (rechtlich eigenständige) Mitglieder eines Verbands Dritte sind.

Deshalb sind auch bei der **konzerninternen Übermittlung** von Daten die Vorschriften der DSGVO zu beachten, also wenn einer Tochter- oder Schwestergesellschaft Zugriff auf personenbezogene Daten gewährt werden.

c. Auftragsdatenverarbeitung

Eine besondere Form der Weitergabe erfolgt im Rahmen der sog. Auftragsdatenverarbeitung.

> Gemeint sind damit Fälle, in welchen ein anderes Unternehmen damit beauftragt wird, Daten (bspw. Mitarbeiter- oder Kundendaten) zu Zwecken der Auftraggeberin zu bearbeiten, diese jedoch nicht zu eigenen Zwecken verwenden darf.

Im Unternehmensalltag sind diese Konstellationen generell sehr häufig und bedeutsam.

Beispiele:

Verbreitete Anwendungsfälle ergeben sich beispielsweise beim Rückgriff auf folgende Dienste bzw. Programme:

- SaaS-Lösungen für Email-Marketing (z.B. Mailchimp, Evalenche)
- Google Analytics für Webanalysen
- Cloud-Anbieter für Datenspeicherungen
- Microsoft 365 (Cloud-Lösung)
- Chatlio (Chatfunktionen auf Webseite)
- Bonitätsprüfung im Bestellprozess (z.B. Deltavista)
- Einsatz von Social Monitoring Tools durch Drittdienstleister
- Salesforce / Microsoft Dynamics (CRM-Systeme)
- Hosting der Website
- Versicherungsbroker
- Externe Buchhaltung
- Telefondienst

Zentral ist dabei, dass die DSGVO **explizit den Abschluss eines schriftlichen Vertrags** verlangt, wobei dies auch in einem „elektronischen Format" erfolgen kann. Insbesondere im Online-Kontext genügt daher der Abschluss über eine Website. Im Vertrag muss sich der Auftraggeber Weisungs- und Kontrollrechte einräumen lassen. Mit anderen Worten muss der Beauftragte insbesondere dazu verpflichtet werden, die Daten nur nach den Weisungen des Auftraggebers zu bearbeiten. Wichtiger Inhalt des Vertrags ist auch die Frage, ob der Beauftragte selber auf weitere Dritte (Subunternehmen) zurückgreifen darf oder nicht. Denn nach der DSGVO ist ihm dies nur mit Genehmigung des Auftraggebers gestattet.

Beispiel:

Nutzt ein Online-Händler zur Analyse der Website-Nutzung den Dienst „Google Analytics" muss Google verpflichtet werden, Daten „weisungsgemäss" zu bearbeiten. Hierfür stellt Google eine Vertragsvorlage zur Verfügung, deren Rechtmässigkeit unter der DSGVO allerdings noch nicht abschliessend geklärt ist.

Der Auftraggeber darf Datenbearbeitungen nur an Unternehmen „auslagern", die durch die Implementierung von technischen und organisatorischen Massnahmen (sog. TOM's) die Verarbeitung im Einklang mit der DSGVO sicherstellen können. Diese TOM's muss sich der Auftraggeber dokumentieren lassen.

> Der Auftraggeber bleibt aber in jedem Fall auch beim Einsatz eines Drittens gegenüber den von der Datenverarbeitung betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben.

Allerdings treffen zahlreiche Pflichten der DSGVO zusätzlich auch den Auftragsdatenverarbeiter. Zudem können auch gegen ihn Sanktionen verhängt werden.

4. Bonitätsprüfungen

Für den Onlinehandel ist die Bonitätsprüfung eines der wichtigsten Mittel zur Vermeidung von Zahlungsausfällen. Die Bonitätsprüfung wird in aller Regel durch ein Drittunternehmen im Hintergrund während des Bestellprozesses im Interesse des Online-Händlers durchgeführt. Insofern ist der Anbieter der Bonitätsprüfung aus Sicht des Online-Händlers ein Dritter. Folglich sind die Anforderungen bezüglich der **Auftragsdatenbearbeitung** einzuhalten.

Hinzu kommt, dass die Prüfung regelmässig automatisiert, also ohne „menschliches Zutun" erfolgt. Mit anderen Worten wird automatisiert darüber entschieden, ob mit dem Besteller ein Vertrag geschlossen wird oder nicht. Die DSGVO gewährt den Betroffenen grundsätzlich das Recht solche **„automatisierten Einzelentscheidung"** durch einen Menschen überprüfen zu lassen. Dies gilt jedoch auch nach Ansicht von Datenschützern nicht, wenn der Vorgang zur Reduktion des Risikos von Zahlungsausfällen führt. Eine verhältnismässige Bonitätsprüfung ist somit beim Kauf auf Rechnung auch künftig zulässig, ohne dass eine nachträgliche Überprüfung vorgenommen werden muss. Gleichwohl sind die **weiteren Vorgaben der DSGVO** auch hier zu beachten. So muss vor allem auf die automatisierte Bonitätsprüfung deutlich hingewiesen und in verständlicher Weise über die Grundprinzipien der involvierten Logik informiert werden.

5. Verwendung von von Tracking-/Webanalyse-Tools

Im Rahmen des Marketingkonzepts spielt selbstredend auch die Nutzung der Website bzw. des Onlineshops des Unternehmens eine zentrale Rolle. Zur Auswertung der Website-Besuche wird dabei auf Dienste, wie Google Analytics, zurückgegriffen.

Aus datenschutzrechtlicher Sicht sind in diesem Zusammenhang verschiedene Anforderungen einzuhalten, auf welche bereits an anderer Stelle eingegangen wurde. So erfolgt, wie im Beispiel von Google Analytics, häufig eine Datenübermittlung an einen Dritten, der seinen Sitz in den USA hat.

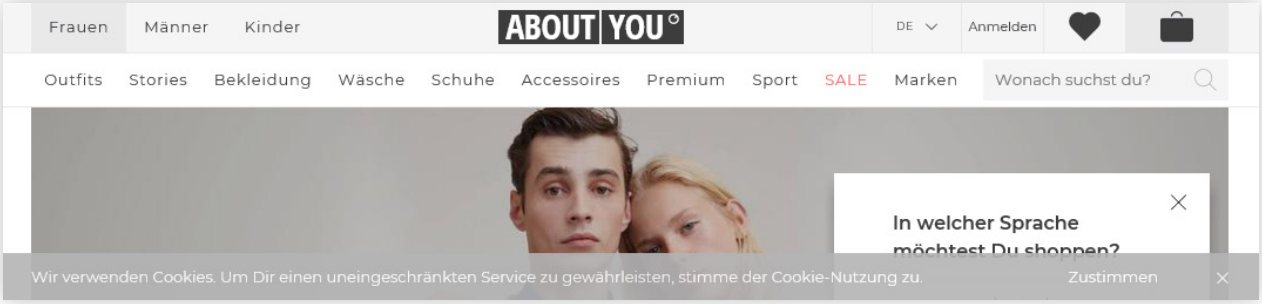
> Deshalb sind die Anforderungen an die Auftragsdatenverarbeitung und die Datenübermittlung in Drittstaaten einzuhalten.

Darüber hinaus müssen der Einsatz solcher Dienste – zur Erfüllung der Informationspflicht – in der Datenschutzerklärung offengelegt und die damit verbundenen Datenverarbeitungen erläutert werden.

Bekanntlich basieren die Analyse-Tools regelmässig auf dem **Einsatz von Cookies** oder vergleichbaren Technologien, durch welche das Klickverhalten der Nutzer über mehrere Seiten nachverfolgt werden kann. Bereits nach geltendem EU-Recht müssen User vor dem Setzen von Cookies hierüber informiert und nach ihrer Einwilligung gefragt werden. In der Praxis wird diese Anforderung derzeit primär über die verbreiteten **Cookie-Banner** umgesetzt, welche beim Einstieg auf eine Website eingeblendet werden.

Beispiel:

Als Beispiel kann ein Mitglied des VSV herangezogen werden, dass auf seiner Webseite derzeit folgenden Banner einblendet:



Quelle: www.aboutyou.ch (besucht am 3.4.2018)

Zu beachten ist jedoch, dass in der EU eine strenge Regelung für Cookies geplant ist, welche ergänzend zur DSGVO zur Anwendung gelangen soll. Der konkrete Inhalt dieser sog. **ePrivacy-Verordnung** steht aktuell noch nicht fest. Allerdings zeichnet sich ab, dass künftig auch die bisherigen Cookie-Banner nicht mehr genügen werden und das Setzen von Cookies oder ähnlichen Technologien nur und erst gestützt auf eine ausdrückliche Einwilligung der User zulässig sein sollen. Die weitere Entwicklung ist deshalb im Auge zu behalten.

6. Datenweitergabe ins Ausland

Besondere Beachtung zu schenken ist stets auch der Frage, in welche Länder Daten übermittelt werden. Namentlich bei Übermittlungen in die USA ist Vorsicht geboten.

> Die USA (wie auch andere Drittländer, insb. China, Russland oder Indien) gelten als Land ohne angemessenes Datenschutzniveau, weshalb eine Datenübermittlung ohne zusätzliche besondere Vorkehrungen nicht erlaubt ist.

Eine solche besondere Vorkehrung für die Übermittlung von personenbezogenen Daten in die USA stellt die Zertifizierung durch das Empfängerunternehmen in den USA im Rahmen des sog. **„Privacy-Shield"-Abkommens** dar. Auch bei einer solchen Zertifizierung sind aber die anderen Pflichten der DSGVO (z.B. die Informationspflichten oder die Pflicht zur Rechtfertigung der Datenweitergabe) selbstredend weiterhin einzuhalten. In vielen Konstellationen wird der Datentransfer in die USA zudem im Rahmen einer Auftragsdatenverarbeitung erfolgen. In diesen Konstellationen muss nicht nur der Datentransfer DSGVO-konform erfolgen, sondern auch die eigentliche Auftragsdatenverarbeitung.

Alternativ zur „Privacy-Shield"-Zertifizierung kommen auch andere zusätzliche besondere Vorkehrungen in Frage. Aktuell gelten z.B. die sog. **EU-Standarddatenschutzklauseln** (sog. „EU Model Contract Clauses") als genügende Massnahme für Datentransfers in die USA, sofern sie im Rahmen der Auftragsdatenverarbeitungs-Verträge vereinbart werden. Entsprechend enthalten die meisten Muster-Auftragsdatenverarbeitungsverträge bereits diejenigen Bestimmungen, welche für datenschutzkonforme Datentransfers in die USA und andere Länder ohne angemessenes Datenschutzniveau notwendig sind.

Beispiel:

Ein Onlineshop, der auf seiner Website den so genannten Remarketing Pixel von Facebook einsetzt, um personalisiertes Marketing in sozialen Netzwerken zu ermöglichen, übermittelt dabei grundsätzlich personenbezogene Daten an Facebook mit Sitz in den USA. Facebook ist zwar ein unter dem „Privacy Shield" zertifiziertes Unternehmen, weshalb keine zusätzlichen Garantien erforderlich sind. Anders als etwa bei Google, ist es allerdings immer noch unklar und deshalb problematisch, wie mit Facebook ein ausreichender Auftragsverarbeitungsvertrag abgeschlossen werden kann.

7. CRM-Systeme

Grosse Herausforderungen bringt das Inkrafttreten der DSGVO auch für die Datenverarbeitungen im Rahmen von Kundenmanagement (CRM) Systemen. Der Sinn und Zweck dieser Systeme besteht unter anderem in der zentralen Speicherung aller relevanten Geschäftsvorgänge mit den einzelnen Kunden.

> Gerade diese Zusammenführung bzw. Verknüpfung der Vielzahl von Daten aus unterschiedlichen Quellen ist aus datenschutzrechtlicher Sicht jedoch problematisch.

a. Transparenz und Rechtmässigkeit

Aufgrund der Informationspflicht und des Transparenzgebots müssen die Kunden auf die Verknüpfung und zentrale Speicherung ihrer Daten vorab aufmerksam gemacht werden. Damit verbunden ist auch die Frage nach der rechtlichen Grundlage für die Bearbeitung. Denn für die Speicherung von Bestelldaten kann zwar der Erlaubnistatbestand des Vertrags in Frage kommen, jedoch wird für die Verknüpfung der Daten und Verarbeitung im Rahmen eines CRM-Systems meist eine Einwilligung des Kunden erforderlich sein. Diese ist jedoch nur wirksam, wenn sie vom Kunden gestützt auf ausreichende Informationen über die Datenverarbeitung vorgängig erteilt wird. Eine klare und vollständige Information der betroffenen Kunden ist deshalb unter beiden Aspekten nicht nur notwendig, sondern auch gesetzlich vorgeschrieben.

Beispiel:

Der Online-Händler muss den Kunden im Zeitpunkt, indem dieser das Bestellformular mit seinen Rechnungs- und Lieferangaben ausfüllt, darüber informieren, dass seine Daten in einer zentralen Datenbank gespeichert und mit anderen Informationen, wie z.B. früherer Bestellungen, dem Bonitätsrating oder abgegebenen Produktbewertungen, verknüpft werden. Gleichzeitig muss der Online-Händler die Einwilligung des Kunden einholen.

Zentral ist dabei, dass auch die von den Kunden erteilten Einwilligungen (inkl. Zeitpunkt sowie Wortlaut der Erklärung und der Informationen) dokumentiert werden und bei Bedarf rasch abrufbar sind.

b. Zweckbindung und Zweckänderung

In diesem Zusammenhang ist auch ein besonderes Augenmerk darauf zu richten, dass die vorhandenen Daten nicht zu neuen Zwecken bearbeitet werden, die durch den ursprünglich angegebenen Zweck nicht mehr gedeckt sind. Dies kann insbesondere bei „**Altdaten**“ problematisch sein. Sollen personenbezogene Daten aus einer Datenbank in eine andere überführt werden, ist deshalb stets zu prüfen, ob hierdurch nicht eine Zweckänderung erfolgt. Ist dies der Fall, muss der betroffene Kunde darüber informiert werden und er muss seine Einwilligung in die Datenverarbeitung zum neuen Zweck erteilen.

Die gleiche Herausforderung stellt sich, wenn aus den vorhandenen Daten neue Erkenntnisse abgeleitet werden sollen. Bei solchen **CRM- oder Big-Data-Analysen** lässt sich im Vornherein teilweise nur schwer definieren, welche konkreten Erkenntnisse letztlich gewonnen werden. Daher ist bei der Formulierung der Informationen, namentlich des Zwecks der Datenverarbeitung, besondere Vorsicht geboten.

Beispiel:

Hat der Online-Händler in seiner Datenschutzerklärung darüber informiert, dass die Daten zum Zweck ausgewertet werden, den Kunden einen bestimmten Scorewert zuzuweisen, damit ihnen personalisierte Werbung zugestellt werden kann, dann darf er die Analyse nicht auch auf die Festsetzung eines individualisierten Preises ausweiten. Unter Umständen gehen jedoch später aus der Analyse auch Erkenntnisse hinsichtlich des Preises hervor, sodass bereits eine Zweckänderung vorliegen würde.

Weitgehend ungeklärt ist auch nach wie vor, wie solche Analysen mit dem Grundsatz der **Datensparsamkeit** in Einklang gebracht werden können. Ist doch gerade die Generierung und Auswertung einer möglichst grossen Zahl von Daten für die Aussagekraft der Analyse-Ergebnisse entscheidend. Die DSGVO verlangt aber jedenfalls, dass bereits bei der Erhebung darüber informiert wird, wie lange Daten gespeichert werden oder, „falls dies nicht möglich ist", welches die Kriterien für die Festlegung der Speicherdauer sind. Die Unternehmen müssen deshalb in jedem Fall auch für das CRM-System ein **Konzept für die Löschung bzw. Aufbewahrung** von personenbezogenen Daten definieren.

c. Zugriffsrechte und Weitergabe der Daten

Für den datenschutzkonformen Einsatz von CRM-Systemen ist die Regelung der Zugriffsrechte besonders wichtig.

> Es muss sichergestellt werden, dass Mitarbeiter nur auf diejenigen Daten zugreifen können, die für die Erfüllung ihrer Aufgabe erforderlich ist (sog. Need-to-know-Prinzip).

Dieses **„Need-to-know-Prinzip"** ist durch ein Berechtigungskonzept umzusetzen, in welchem Zugriffsregeln für einzelne Benutzer oder Benutzergruppen festgelegt werden.

Neben diesem unternehmensinternen Aspekt ergeben sich auch bereits aus der Wahl des jeweiligen CRM-Systems grundlegende Anforderungen. Denn ein Grossteil solcher Systeme basiert auf einer Cloud-Lösung, resp. SaaS-Lösung und die Anbieter oder die Hoster befinden sich im Ausland. In diesem Fall sind wiederum die Vorgaben für die **Übermittlung ins Ausland** sowie die **Auftragsdatenverarbeitung** zu beachten.

8. Online- und Offline-Marketing

Auch das Marketing wird von der EU-DSGVO betroffen sein. Gerade Online-Händler nutzen in der Regel die ganze Palette an möglichen Marketing-Aktivitäten. Besonders wichtig in diesem Zusammenhang ist für Online-Händler die personalisierte Werbung, das E-Mail-Marketing und Gewinnspiele, da sie von den meisten Onlineshops gezielt und effektiv eingesetzt werden.

a. Personalisierte Werbung

Personalisierte Werbung erfolgt in der Regel über auf dem Rechner der betroffenen Person gesetzte Cookies, Analyse Tools (z.B. Google Analytics) oder basierend auf Daten aus dem CRM. Ziel der Werbung ist es den betroffenen Personen nur diejenigen Angebote zuzustellen, welche für sie auch von Interesse sein könnten.

Die personalisierte Werbung ist jedoch auch unter DSGVO nicht unproblematisch und es stellen sich vielschichtige Fragen zur Rechtmässigkeit. Bereits der Umstand, dass für die erfolgreiche Personalisierung der Werbung möglichst viele Daten über einen längeren Zeitraum gesammelt werden sollen, führt zu Konflikten mit dem Prinzip der Datensparsamkeit. Die Daten werden regelmässig zu einem „Profil" zusammengeführt, bspw. in einem Cookie. Die Auswertung der Informationen und die Entscheidung über zu schaltende Anzeigen erfolgt wiederum automatisiert. Deshalb sind die besonderen Vorgaben für solche „automatisierte Einzelentscheidungen" und insbesondere das „**Profiling**" zu beachten. Allerdings greift das hierfür vorgesehene Verbot auch nach Ansicht der Datenschützer noch nicht beim blossen „targeted advertising".

Gleichwohl sind auch hier die allgemeinen Vorgaben zu beachten.

> So ist personalisierte Werbung in der Regel nur dann zulässig, wenn vorab eine gültige **Einwilligung**

der betroffenen Person eingeholt wurde.

Dies setzt voraus, dass transparent und vollständig über die einzelnen Datenbearbeitungen vorab informiert wurde. Die Umsetzung und der Nachweis der Einhaltung dieser Vorgaben können gerade Online-Händlern, die an **Affiliate-Programmen** teilnehmen, Schwierigkeiten bereiten. Denn an den Datenverarbeitungen sind regelmässig mindestens drei Unternehmen beteiligt. Die Hauptverantwortung liegt zwar bei den Betreibern der Werbenetzwerke.

Aber auch die werbenden Unternehmen und die Betreiber von Websites, auf welchen die Anzeigen publiziert werden, nehmen im Rahmen solcher Affiliate-Programmen relevante Datenbearbeitungen vor.

So übertragen beide regelmässig Daten an den Betreiber des Werbenetzwerks und setzen Cookies oder lesen diese aus. Auch hierfür gelten wiederum die Vorgaben der DSGVO, insbesondere die Informationspflicht und das Erfordernis eines Erlaubnistatbestands. Wer an solchen Programmen teilnehmen oder generell auf Online-Marketing-Tools zurückgreifen will, muss deshalb über die zugrundeliegenden Datenbearbeitungen Bescheid wissen, um die Betroffenen überhaupt transparent und vollständig informieren zu können. Hinzu kommt, dass das Verhältnis zu den eingesetzten Dienstleistern vielfach als **Auftragsdatenverarbeitung** zu betrachten ist und die Anbieter ihren **Sitz im Ausland**, insbesondere den USA haben. Die bereits erläuterten Vorgaben müssen deshalb auch hier eingehalten werden.

b. E-Mail-Marketing

Für die Zustellung von Werbe-E-Mails und insbesondere den Versand eines Newsletters ergeben sich weitere Fragestellungen aus dem Zusammenspiel von Datenschutz- und Wettbewerbsrecht. Denn zum einen werden dabei regelmässig personenbezogene Daten bearbeitet und zum anderen sehen die nationalen Gesetze strenge Vorschriften zum Schutz vor „Spam" vor.

Eine Schweizer Besonderheit besteht darin, dass Verstösse gegen den „Spam-Artikel" bereits heute **strafrechtlich sanktioniert** sind.

Vor diesem Hintergrund sollten Unternehmen beim E-Mail-Marketing besonderen Wert auf die Einhaltung der rechtlichen Vorgaben legen.

1. Einwilligung („Opt-in")

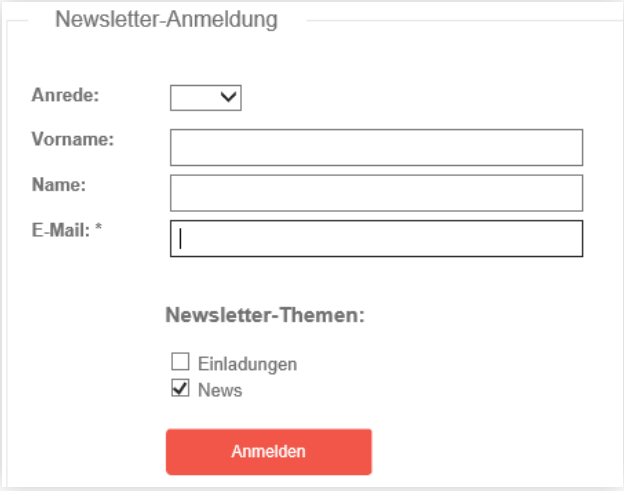
Für die Rechtmässigkeit von Werbe-E-Mails ist regelmässig eine **Einwilligung** des Empfängers erforderlich. Wie bereits ausgeführt, ist eine Einwilligung nur gültig, wenn sie gestützt auf einer hinreichenden Information über die mit dem Versand verbundenen Datenverarbeitungen erfolgt. Diese Informationen sind daher ebenfalls in die **Datenschutzerklärung** aufzunehmen und im Rahmen des Registrierungsprozesses an prominenter Stelle zu platzieren. Weiter stellt sich die Frage, in welcher Form die Einwilligung der Interessenten eingeholt werden kann. Es wurde bereits erläutert, dass **vorangekreuzte Kästchen** nach der DSGVO nicht für eine wirksame Einwilligung genügen. Darüber hinaus ist Unternehmen dringend zu empfehlen, das sog. **„Double Opt-in"-Verfahren** einzusetzen:

Hierfür wird im Rahmen des Anmeldeprozesses zunächst ein erstes „Opt-in" für die Zustellung des Newsletters an die eingegebene E-Mail-Adresse verlangt. In einem zweiten Schritt wird dann unmittelbar danach und bevor der Newsletter erstmals zugestellt wird, ein E-Mail versandt mit der Aufforderung zur

Bestätigung der Anmeldung durch einen Klick auf einen entsprechenden Link (zweites „Opt-In"). Vorteil dieses Verfahrens ist, dass sich die Einwilligung durch das „zweite Opt-in" relativ leicht und gut dokumentiert nachweisen lässt.

Beispiel:

Im Beispiel des VSV-Newsletters würde Schritt 1 dann folgendermassen aussehen:



Schritt 2 im Sinne des Double-Opt-In könnte wie folgt umgesetzt werden:

2. Weitergabe an Dritte und Übermittlung ins Ausland

Für den Versand des Newsletters greifen Unternehmen regelmässig auf Tools von Dritten zurück. Je nach konkreter Ausgestaltung kann dies dazu führen, dass ein **Auftragsdatenverarbeitungsverhältnis** vorliegt. In diesem Fall sind die bereits erläuterten Anforderungen einzuhalten, also namentlich eine Vereinbarung über die Weisungs- und Kontrollrechte abzuschliessen. Hinzu kommt, dass verschiedene Anbieter, wie z.B. MailChimp, ihren Sitz in den USA haben und Daten auf diesen Servern gespeichert werden. Dies hat zur Folge, dass auch die Anforderungen (insb. Informationspflicht und Garantien) für die **Übermittlung ins Ausland** zu beachten sind.

Zusätzliche Vorgaben bestehen auch dann, wenn der Versand des Newsletters selbst grenzüberschreitend erfolgt. Sofern ausländischen Interessenten eine Registrierung offen steht, sind unter Umständen auch die **nationalen Vorschriften anderer Länder** zu beachten. Dies hängt insbesondere davon ab, ob die Website und das Angebot des Newsletters auch auf Kunden in diesen Ländern „ausgerichtet" ist, was relativ rasch der Fall ist. Es gelten somit im Wesentlichen die gleichen Kriterien, wie bei der Frage nach der Anwendbarkeit der DSGVO auf Schweizer Unternehmen ohne EU-Niederlassung (siehe oben).

> In der Konsequenz unterstehen Newsletter von Schweizer Online-Händlern regelmässig auch den Vorschriften ausländischer Rechtsordnungen, insb. des deutschen Rechts.

Im deutschen Recht genügt bereits eine einzige Werbe-Mail ohne Einwilligung um allenfalls als Spammer eine Abmahnung zu erhalten, mit welcher regelmässig Unterlassungsansprüche geltend gemacht und die Erstattung von Anwaltskosten verlangt werden. Bei der Ausgestaltung des Newsletter-Prozesses dürfen deshalb neben der DSGVO auch weitere ausländische Rechtsvorschriften nicht vernachlässigt werden.

c. Gewinnspiele

Gewinnspiele sind für Unternehmen ein unverzichtbares Marketinginstrument und vor allem im Online-Kontext allgegenwärtig. Dies einerseits wegen der Werbewirkung. Andererseits aber auch wegen der Möglichkeit zur Generierung persönlicher Daten von potentiellen Kunden. Diese Daten sollen anschliessend für Marketingzwecke verwendet werden, um den Teilnehmenden beispielsweise einen Newsletter zuzustellen.

Vor diesem Hintergrund ist die Teilnahme an einem Gewinnspiel nach der bisherigen Praxis in der Schweiz stets davon abhängig, dass die Teilnehmer eine Einwilligung in die Nutzung ihrer Daten zu Werbezwecken erteilen. Diese Praxis führt zu einem grundlegenden Konflikt mit den Anforderungen der DSGVO an gültige Einwilligungen, welche allerdings noch nicht restlos geklärt sind.

Konkret stellt sich die Frage, ob bzw. inwiefern künftig ein sog. **Koppelungsverbot** (siehe oben)gilt. Danach wäre es verboten, die Erfüllung eines Vertrags von der Einwilligung in weitere Datenverarbeitungen abhängig zu machen, die für die Vertragserfüllung nicht erforderlich sind. Neben der glückspielrechtlichen Regulierung, die grundsätzlich einen geldwerten Einsatz verbietet, wäre danach auch die Verknüpfung der Teilnahme mit der Werbe-Einwilligung unzulässig.

Beispiel:

Zur Einhaltung des Kopplungsverbots muss die Teilnahme an einem Gewinnspiel auch möglich sein, wenn der Interessierte die Checkbox zur Einwilligung in die Zustellung eines Newsletters nicht anwählt.

9. Social-Media

Der Grossteil der Unternehmen ergänzt sein Marketing-Konzept auch mit einer Präsenz auf den einschlägigen Social Media Plattformen. Auf diesen Plattformen äussern sich tausende Nutzer täglich über Produkte und Anbieter. Für viele Unternehmen ist es daher gängige Praxis, neben den klassischen Medien auch Social Media zu beobachten und zu analysieren und die Funktionalitäten der einschlägigen Plattformen in den eigenen Onlineshop einzubeziehen. Dabei wird eine Vielzahl von personenbezogenen Daten bearbeitet, sodass das Inkrafttreten der DSGVO auch für die Durchführung von Social Media Aktivitäten zahlreiche Herausforderungen mit sich bringen wird.

a. Plug-Ins

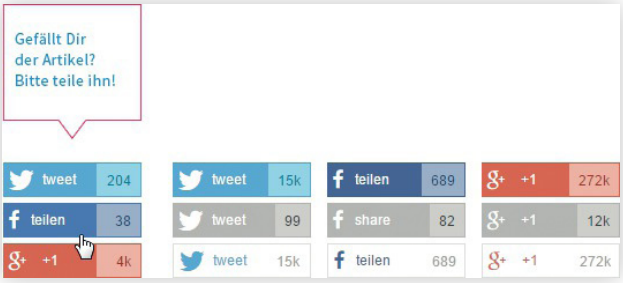
Die meisten Online-Händler verwenden in ihrem Onlineshop sog. Social Plug-Ins (z.B. den Facebook „Like"-Button). Die Verwendung dieser Social Plug-Ins ist aus datenschutzrechtlicher Sicht problematisch. Sofern nicht spezifische Massnahmen getroffen werden, kommunizieren diese Plug-Ins in der Regel mit der darin verlinkten Social Media Plattform im Hintergrund. Dabei werden, ohne dass der Benutzer etwas davon weiss, Daten an die Social Media Plattform gesendet und zwar auch dann, wenn der Benutzer kein entsprechendes Profil auf dieser Plattform hat. Mit anderen Worten werden die Daten an die Social Media Plattform übermittelt, ohne dass die betroffene Person entsprechend informiert wurde und ohne dass sie ihre Einwilligung hierfür erteilt hat.

Eine Möglichkeit zur Reduzierung der rechtlichen Risiken besteht im Einsatz der sog. 2-Klick-Lösung oder der Weiterentwicklung davon, dem sog. „Shariff"-Plugin.

Bei der **2-Klick-Lösung** werden die Social Plug-Ins erst dann aktiviert und die Daten erst an die Social Media Plattform übermittelt, wenn auf die entsprechende Schaltfläche geklickt wird. Insofern kann durch entsprechende Ausgestaltung der Website und namentlich klare Informationen in der Datenschutzerklärung eine „Einwilligung" des Nutzers vor der Übermittlung von Daten eingeholt werden.

Quelle: www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html (besucht am: 3.4.2018)

Bei **„Shariff"** ist demgegenüber nur ein Klick erforderlich und Informationen der Websitebesucher wie die IP-Adresse werden erst nach dem Klick auf den Button an die Social Media Plattform übertragen.



Quelle: www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html (besucht am: 3.4.2018)

Von Seiten der Datenschützer wurde die Weiterentwicklung zwar begrüsst, jedoch bestehen **weiterhin Risiken**, die selbst mit ausführlichen Informationen in der Datenschutzerklärung nicht gänzlich reduziert werden können. Das ist unter anderem darauf zurückzuführen, dass die DSGVO hohe Anforderungen an die gültige Einwilligung stellt und die Einwilligung auch beweissicher protokolliert und dokumentiert werden muss.

b. Social-Media-Monitoring

Sowohl im Schweizer wie bspw. auch im deutschen Recht bestanden bisher Sondervorschriften für die Datenverarbeitung von öffentlich zugänglich gemachten Daten. Vergleichbare Regelungen sind in der DSGVO nicht mehr vorhanden, weshalb sich die Rechtslage auch für das Social-Media-Monitoring deutlich verschärft. Die bereits nach bisherigem Recht problematischen Praktiken sind deshalb mit erheblichen Risiken behaftet.

Besondere Herausforderungen stellen sich bereits bei der Erfüllung der **Informationspflicht**. Diese greift auch dann, wenn Daten nicht bei der betroffenen Person selbst erhoben werden.

> Auf den Plattformen stellt sich allerdings die Frage, wie diese Informationen den Betroffenen in hinreichender Form erteilt werden können.

Zumindest in Bezug auf Daten, die ein Nutzer auf dem Profil eines Unternehmens (z.B. durch das Verfassen eines Posts) hinterlässt, ist die Platzierung in einer gesonderten Rubrik auf dem Profil denkbar. Anders als bspw. bei Kontaktformularen auf einer Website können diese Informationen allerdings in der Regel nicht unmittelbar dort verlinkt werden, wo der Nutzer seinen Post anbringt. Deshalb ist nach aktuellem Stand fraglich, ob die Aufsichtsbehörden diese Praxis genügen lassen.

Quelle: https:/de-de.facebook.com/pg/Nestle/about/?ref=page_internal (besucht am: 3.4.2018)

Beispiel:

Würde daher Nestlé auf seinem Facebook-Profil unter der Rubrik „Info" Informationen zum Datenschutz einbinden, erscheint es fraglich, ob diese genügend transparent sind.

Ausgehend davon müssten die Pflicht-Informationen nachträglich jedem einzelnen Nutzer zur Kenntnis gebracht werden. Dies gilt umso mehr bei der Erhebung von Daten, die Nutzer in anderen öffentlich zugänglichen Bereichen veröffentlicht haben. In diesen Fällen stellt sich allerdings ohnehin die Frage, ob sich der Online-Händler auf einen **Erlaubnistatbestand** berufen könnte. In der Regel wird ein solcher nicht gegeben sein. Was die Sammlung von Daten, in nicht-öffentlichen Bereichen betrifft, wird diese, wie bereits nach geltendem Recht, stets unzulässig sein.

Beispiele:

Hinterlässt ein Nutzer auf dem öffentlichen Facebook-Profil von Nestlé einen Post mit einer Frage zu einem aktuellen Produkt, darf dieser beantwortet und die ersuchte Leistung grundsätzlich erbracht werden. Unzulässig wäre aber die Einbindung der Daten in das CRM-System, weil hierfür eine informierte Einwilligung des Nutzers erforderlich wäre.

Postet ein Nutzer auf seinem nicht-öffentlichen Facebook-Profil ein Foto eines Nestlé-Produkts und Bemerkungen dazu, darf der Online-Händler darauf weder antworten noch die Daten anderweitig weiterverarbeiten. Denn auch hierfür wäre stets eine informierte Einwilligung erforderlich.

Checkliste: In sechs Schritten zur Compliance

Um die Anforderungen der DSGVO umzusetzen, sind folgende Schritte entscheidend:

Schritt 1: Sensibilisierung

In einem ersten Schritt geht es darum, das Management und die Mitarbeiter für das Thema des Datenschutzes und die mit Verstössen gegen Datenschutzvorgaben verbundenen Risiken zu sensibilisieren. Hierzu bieten sich insbesondere entsprechende Workshops an. Besonders wichtig ist es, die Entscheidungsträger für das Datenschutz-Compliance-Projekt zu gewinnen. Denn schlussendlich ist das Thema Datenschutz Chefsache und muss „Top-Down" in das gesamte Unternehmen einfliessen.

Schritt 2: Überblick über alle Datenverarbeitungen – Erstellen eines Verzeichnisses

Um den datenschutzrechtlichen Anforderungen zu genügen, muss zuallererst ein Überblick über sämtliche im Unternehmen bestehenden Datenverarbeitungen verschafft werden. Gestützt darauf ist sodann das sog. Verarbeitungsverzeichnis entsprechend den konkreten Vorgaben der DSGVO zu erstellen. Die Erfassung aller Datenbearbeitungen ist der Ausgangspunkt und die Basis für alle weiteren Schritte auf dem Weg zur datenschutzrechtlichen Compliance.

Schritt 3: Identifikation von Schwachstellen und Handlungsbedarf

Basierend auf dem Verzeichnis der Datenverarbeitungen ist der Ist-Zustand mit dem angestrebten Soll-Zustand zu vergleichen. Dabei geht es darum, festzustellen, in welchen Bereichen die Vorgaben der DSGVO im unternehmensinternen Datenschutz (noch) nicht eingehalten werden, und entsprechenden Anpassungsbedarf zu identifizieren.

Schritt 4: Fokussierung auf wichtige Massnahmen

Sind die bestehenden Lücken und entsprechender Anpassungsbedarf bekannt, ist eine Priorisierung der einzelnen Massnahmen vorzunehmen. Dabei sollte der Fokus vorab auf diejenigen Massnahmen gerichtet werden, welche einerseits sanktionsbedroht sind und andererseits effizient umgesetzt werden können.

Schritt 5: Beizug von externen Beratern / Anwälten

Grundsätzlich muss ein grosser Teil der Arbeit zur datenschutzrechtlichen Compliance im Unternehmen selbst erfolgen. Sofern intern das Know-how und/oder die Ressourcen fehlen, ist der Beizug externer Berater, wie z.B. Anwälte, in Erwägung zu ziehen. Diese Berater helfen dabei nichts zu vergessen. Zudem kann durch sie ein pragmatischer und umsetzbarer Ansatz gefunden werden, der trotzdem zielführen ist und die Compliance sicherstellt.

Schritt 6: Prozesse zur Beibehaltung der Compliance definieren

Schlussendlich muss sichergestellt werden, dass die Vorgaben der DSGVO auch dauerhaft erfüllt werden. Dazu bedarf es unternehmensinterner Prozesse, die sicherstellen, dass neue Risiken rechtzeitig erkannt und die Beurteilung der Erfüllung der datenschutzrechtlichen Voraussetzungen bei allen neuen Datenbearbeitungen stets mit einfliessen.

Weitere Informationen zum Thema auf unserem Blog **mll-news.com**.

Haben Sie Fragen? Wir beraten Sie gerne.

Lukas Bühlmann, LL.M.
lukas.buehlmann@mll-legal.com
T +41 44 396 91 91

Meyerlustenberger Lachenal AG
Rechtsanwälte – Attorneys at Law
Schiffbaustrasse 2 | Postfach 1765 | CH-8031 Zürich
www.mll-legal.com | www.mll-news.com

Patrick Kessler
info@vsv.ch
T +41 58 310 07 17

Verband des Schweizerischen Versandhandels VSV
Bahnhofplatz 1 | 3011 Bern | Postfach | 3000 Bern
www.vsv-versandhandel.ch